AR-CLOUD COMPUTING: SECURITY & PRIVACY

- Arvind Ponnarassery Jayan
(aponnar1)

Abstract

Loss of privacy and sensitive data is one of the prominent security concerns of this age. With the boom of cloud computing, new attack surfaces has been brought forth for malicious users to exploit. This will be more of an issue for the upcoming technology Augmented Reality Cloud, as it involves several real time data being used in transmission and storage using the cloud computing infrastructure. This write up attempts to realize the issues that this new upcoming technology could bring forth and attempts to provide solutions and mitigations to the same.

1 Introduction

NIST (National Institute of Standards and Technology) defines Cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". There are three main types of cloud computing services built upon the same conceptual framework of remote infrastructure powered by servers housed in a data center, and they are:

1. Infrastructure as a Service (IaaS)

   The consumer is provided with the fundamental computing resources including storage and network where they are able to deploy and run arbitrary software. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications.

2. Platform as a Service (PaaS)

   The consumer can deploy consumer-created or acquired applications onto the cloud infrastructure, and does not manage or control the underlying cloud infrastructure.

3. Software as a Service (SaaS)

   The consumer can the application provided that is running on the cloud infrastructure. The consumer does not deploy application nor manage or control the underlying cloud infrastructure.

The basis of the end-to-end AR Cloud service delivery is cloud resources which are commonly offered through an IaaS model. AR-Cloud brings together significant advances in cloud computing and interactive quality networking to provide high-quality experiences. AR-cloud is a bleeding edge technology, that is yet to be deployed and experienced full-fledged. With each new technology comes with its own set of security issues and this paper tries to identify and address the same.

[9, 10]

2 Literature Review

2.1 Augmented Reality

Augmented reality is the technology that expands our physical world, by adding layers of digital information onto it. Unlike the virtual reality where a whole artificial environment is created to replace the real one, augmented reality appears in the direct view of the physical real-world environment with superimposed computer-generated images, sounds, videos and graphics. [1]

2.2 Augmented Reality Cloud

Augmented Reality has already seeped into the various technology, from games to street directions, from industrial heads-up displays to virtual gamescapes to workspace information. These new augmented, virtual, and extended realities should be aware, data-rich, contextual and interactive. The enabling technology for this is augmented reality cloud. Simply put AR Cloud is a huge shared library of maps, accessible on connected devices through a SDK. The AR Cloud is designed with the assumption that multiple devices and sessions relocalizing with the same location ID also share the same map and the same coordinate system, allowing them to interact together through multiplayer and persistence. Different applications include scenarios like neurosurgeons using an AR projection of a 3-D brain to aid in surgeries, AR projecting views of ancient civilizations over todays ruins bringing the past to life, to see and verify information about cargo containers to speed up loading times. [2, 3, 4]

2.3 AR-Cloud Architecture

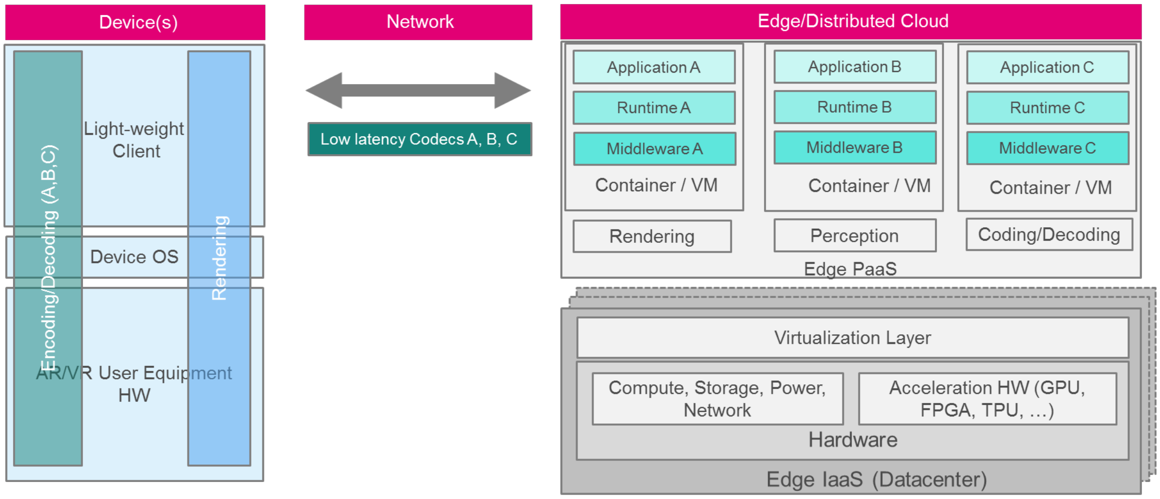

Figure 1: Possible AR-Cloud architecture

The lightweight client function in the terminal device provides the minimum set of capabilities that need to be present for rendering the AR experience, with all additional functionality moved to the Cloud. As there is still a significant amount of data exchanged between the cloud-based processing functions and the users terminal, the use of low latency coding techniques are required even if these come with less than optimal compression factors.

The edge node mainly completes the user plane function and the edge computing platform function; The edge computing platform is responsible for providing deployment and governance of AR related media and vision capability services.

The central node mainly completes the control plane function and management plane function of the 5G network: specifically, control plane signalling, service flow processing, policy scheduling and capability opening, and network operation and maintenance, node management and slice management. [10]

2.4 AR applications VS AR-Cloud

AR applications and software development kits provided are just the tip of the iceberg, they still have not passed the novelty phase and is not widely utilized by the society in general. Examples of Augmented Reality applications like the “Pokemon Go” and “Harry Potter: Wizards Unite” developed by Niantic was highly successful and broke several records in the first month of release. There are several other applications like Directions in Google maps, IKEA Mobile App, Disney coloring book, L’Oreal Makeup App and Weather Channel Studio Effects that uses Augmented Reality, but these applications do not fully utilize the AR cloud infrastructure. [8]

AR-cloud aims in persistent AR experiences in the real world across time, space and devices. This means that an AR experience that was created by a user can be interacted over a long time and as well as shared and collaborated among other users. AR cloud is like a real time spatial map of the world. The sharing of images or videos with AR components is not the essence of AR cloud, it is more than that. Google has been in the forefront in technology due to its powerful method of organizing the world’s information and making it universally accessible. But at this point of era, we need information in the “now” and AR-Cloud promises this.

2.5 Cloud Computing Security Risks

Cloud computing services has brought up a lot of attack surfaces, considering them will help in identifying possible attack vectors for the AR-Cloud system. The different surfaces that are to be considered includes:

1. Data Security and Availability:

   In the field of cloud computing, the data is provided precedence, since the model is to enable ubiquitous and convenient manner of sharing data. But this comes with threats like insufficient encryption and hashing algorithms used for securing the data itself. Also the data should be available on demand.

2. Data Access and Segregation:

   This concern arises due to the multi users storing and using their data at the same cloud infrastructure. The leakage of data from one user to another user is to be considered.

3. Network Security:

   Exposure of network and traffic flow by not creating a secure channel for communication is prominent. The channel can be secured using cryptographic methods, but the channel is as secure as the end points.

4. Physical security:

   There needs to be attention towards the security of infrastructure and also the disaster management plan.

5. Software security:

   The developers need to be concerned of programming flaws, software interruptions and modifications.

[11]

3 Background And Motivation

AR-Cloud is described as “the single most important software infrastructure in computing, far more valuable than Facebooks social graph or Googles PageRank index”, by Matt Miesnieks Co-founder & CEO of 6d.ai (the company mission is to build a 6D Reality Platform). The software development kit provided currently, such as the ARKit by Apple and ARCore by Google only provides a simple range of AR tools, but an AR-cloud focuses on the connecting people through the augmented reality and also to understand and connect “things” in the real world and for this it uses a strong cloud infrastructure.

AR-Cloud will cause a fundamental shift in the way information is organized. The AR Cloud is a shared memory of the physical world and will enable users to have shared experiences which not only includes videos and messages, it will also allow people to collaborate, play, design, study, or team up to problem solve anything in the real world. AR-Cloud promises not only multi-user engagement but also in the persistence of information in the real world. [5]

Problem Statement: Now the worlds largest companies and organizations are racing to create the required AR Cloud infrastructure, to build and fuel these systems. This is where we will face unprecedented challenges and risks to privacy and individuals rights and freedom if we do not actively and mindfully seek to address the possible issues. AR-Cloud is a cloud infrastructure, by understanding how it uses cloud computing and it’s features and functionality, we can realize the possible security issues and privacy risk for this infrastructure and try to address them. [6]

4 Summary Of Findings

To understand the probable threats to AR-Cloud system, we can use the AR-Cloud to understand the possible attack surfaces. By observing the architecture we can understand that there are several attack surfaces such as:

1. The End Point Device:

   The data that is being collected by the end point device includes from everything you see, hear to what you use.

Hence the applications, software and the end point devices should be secure and various attacks vectors and security measure to consider include:

- Web application attacks:

  Attacks like injection attacks, XSS, CSRF and other web application attacks should be considered while creating a web application, so that the information will not get leaked or modified.

- Hardware integrity:

  The end point applications should be made safe from hardware issues like compromised OS or firmware.

- Software protection:

  Application should be isolated, no other application should access the data consumed by the AR application. The application should be secure from tampering.

2. The Network Channel:

   The communication channel between the software and cloud should be secure from spoofing, sniffing and DoS attacks. Encrypting the channel can prevent a lot of network attacks, like TLS and IPsec.

3. The Edge Cloud:

   The edge cloud has all the functions that uses the data and renders the AR media. Processing data at the edge can reduce that the data exposed to the cloud but also increases the attack surfaces. The edges should be protected from leaking confidential information.The main points of attacks on the edge node can be prevented by securing the firmware and distribution of load.

4. The Cloud Infrastructure Service:

   The cloud infrastructure stores all data that is processed by the edge nodes and contains the large repository of all the public and private information of the digital space around the world. The data that is now stored in cluster of data centers are a new attack surface for the attackers to collect sensitive information in bulk. While considering the cloud infrastructure, there are several possible attacks including malware injections, abuse of cloud services, denial of service, insider attacks and side channel attacks. The cloud services should be protected through encryption, intrusion detections, strong authentication, etc.

We realize that this 3-D (or more than 3-D) digital systems have similar weaknesses like that of 2-D digital systems. But the biggest difference is the information that is being collected, analyzed, processed, transported and stored by these 3-D AR-Cloud systems. For the development of this platform, there should be an aggregation of highly specific and real time data for the re-construction of multi-dimensional maps of public and private spaces. This requires routine capture of the same spaces, followed by processing, analyzing and sharing with others. AR cloud should uses sensor data to store identity, location, physical context, and behaviors of users in public and sensitive areas, and collecting, analyzing, transmitting and storing of this information. The various types of data collected related to the user by this technology can include biometric data, what we see, what we respond to, galvanic skin response, facial expressions and emotions (brain waves). It is found that the now using a person's brain wave with the help of Natural Language Processing and AI it is possible to read their thoughts. This shows the tremendous implication if the personal and private data that is used by the system got leaked. To address the issue of loss of privacy we have to consider various angles to address this issue.

Legally a lot of changes are to be brought out for the deployment of the AR-Cloud technology, since the the property that belongs to AR-Cloud infrastructure is not physical but digital and cannot be easily prevented from trespassing. There should be a change in legal guidelines of the owning of property in terms of a digital space

The several ephemeral emotions and responses collected can be analyzed to generate a psychographic profile of an individual. The responses and emotions that the user is being associated can be misleading or corrupt, which could lead to a misleading profile for the user. The main implication of leaking of data is to predicting what the individual is going to do, or at an extreme condition, control the action that they will do. In some levels there is no way to hide the data from the company that is processing it. But the many possible methods for preventing the reconstruction using the private data. The main methods include:

- Decentralized Architectures:

  A implementation of a decentralized architecture can be, which employs a distributed hash table (DHT) to store and retrieve data objects created by their owners.A users profile is a root object, which contains references to other objects, such as contact information, a wall, photo albums, etc. Each object is encrypted to provide confidentiality. The primary advantage of our architecture is its modularity, i.e., the data objects, the cryptographic mechanisms, and the DHT are three separate components, interacting with each other through well- defined interfaces. The modular design provides us with the capability of using any type of DHT or cryptographic scheme.

  This provides the user to provide a fine granular access control and consent mechanism. This architecture preserves user relationship privacy.

- Homomorphic Encryption:

  This method is to preserve privacy using privacy-protecting cryptographic methods. Homomorphic encryption is to ensure sufficient information is available to achieve certain goals.

  The technology required for this method is still not there yet, as lots of computation power is required for such an encryption. Hence wide-scale adaptation of this encryption method is not popular, since it takes a lot of time. Also the privacy is only maintained as long as the data is encrypted.

- Differential Privacy:

  Differential privacy is a meaningful and mathematically rigorous definition of privacy useful for quantifying and bounding privacy loss. A differential privacy requires the probability distribution on the published results of an analysis to be "essentially the same", independent of whether any individual opts in to or opts out of the data set.

Google's RAPPOR or Randomized Aggregatable Privacy-Preserving Ordinal Response is used to ensure anonymity for those participating in crowd-sourced statistics with a strong privacy guarantee.

We can follow these procedure to ensure anonymization of the users to prevent reconstruction of the data to associate to an individual. [7, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21]

5 Conclusion

AR-Cloud is considered to the next technology that will bring the greatest digital revolution, and understanding the threats that it will face to the parties involved is crucial. The paper identifies the threats, possible vulnerabilities and privacy risks associated to this bleeding edge technology and attempts to secure the system.

References

[1] What is Augmented Reality

[2] AR is the future OS

[3] Building AR cloud

[4] AR-Cloud by 6d.ai

[5] ARkit and AR-cloud

[6] The search engine of AR

[7] Privacy manifesto for AR cloud

[8] AR applications

[9] NIST defines cloud computing

[10] AR-Cloud whitepaper

[11] Kumar Patel, Antonina Alabisi, "Cloud Computing Security Risks: Identification and Assessment", Journal of New Business Ideas & Trends. Sep2019, Vol. 17 Issue 2, p11-19. 9p.

[12] AR Cloud Symposium - Privacy & Security Panel

[13] Paul Hyman, Society "Augmented-Reality Glasses Bring Cloud Security into Sharp focus"

[14] Network layer security

[15] OWASP top 10

[16] Edge Nodes Security

[17] Cloud computing cyber attacks

[18] Decentralized Architectures

[19] Garcia F.D., Jacobs B. (2011) Privacy-Friendly Energy-Metering via Homomorphic Encryption. In: Cuellar J., Lopez J., Barthe G., Pretschner A. (eds) Security and Trust Management. STM 2010. Lecture Notes in Computer Science, vol 6710. Springer, Berlin, Heidelberg

[20] Differential Privacy

[21] Google's RAPPOR