AR-CLOUD COMPUTING: SECURITY & PRIVACY

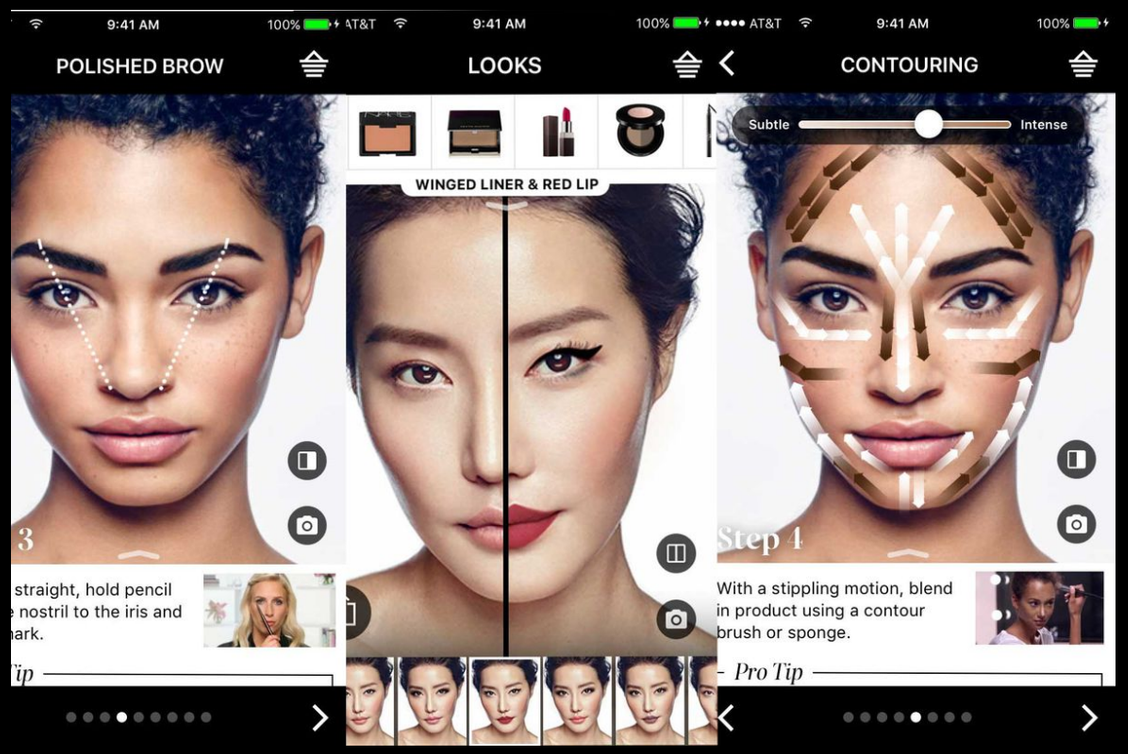
-ARVIND PONNARASSERY JAYAN

SCOPE

- To understand the bleeding edge technology “Augmented Reality Cloud” system.
- Suggest possible design architecture and benefits of this service.
- Discuss pertinent security concerns and issues with the system.
- Suggest possible solutions to the security issues and privacy risks.

AUGMENTED REALITY

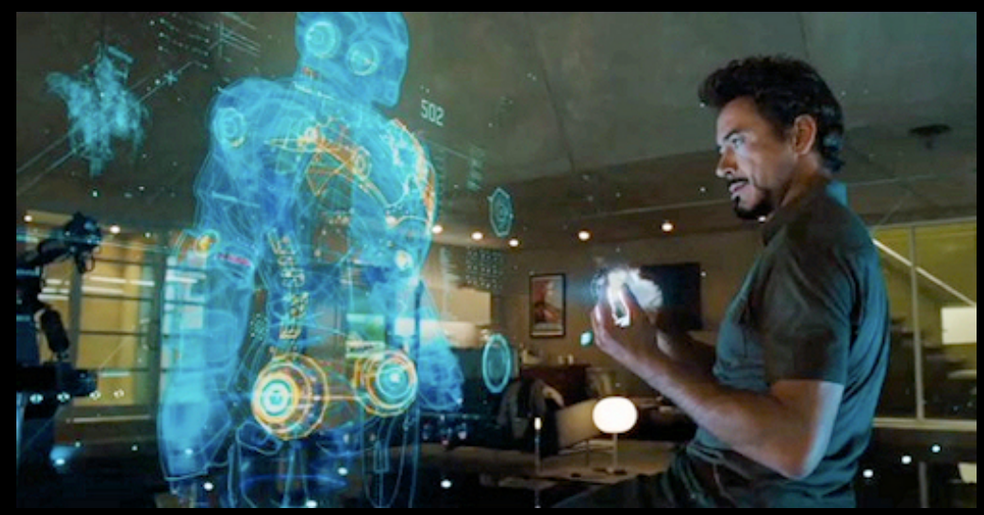
- Augmented reality is the technology that expands our physical world, by adding layers of digital information onto it.
- Unlike the virtual reality where a whole artificial environment is created to replace the real one, augmented reality appears in the direct view of the physical real-world environment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



AUGMENTED REALITY CLOUD

- Augmented Reality Cloud aims in persistent AR experiences in the real world across time, space, devices as well as shared and collaborated among different users.

- AR-Cloud is described as "the single most important software infrastructure in computing, far more valuable than Facebook's social graph or Google's PageRank index", by Matt Miesnieks Co-founder & CEO of 6d.ai



AR vs AR-CLOUD

- AR application still have not passed the novelty phase and is not widely utilized by the society in general.

- 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.

- Examples: neurosurgeons using an AR projection of a 3-D brain to aid in surgeries, AR projecting views of ancient civilizations over today’s ruins bringing the past to life, to see and verify information about cargo containers to speed up loading times.

CURRENT AR-CLOUD

- The basis of the end-to-end AR Cloud service delivery is cloud resources which are commonly offered through an IaaS model.
- Combines significant advances in cloud computing and interactive quality networking (5G) to provide high-quality experiences.
- A new technology and is yet to be deployed and experienced full-fledged.

AR-CLOUD ARCHITECURE

The architecture diagram must essentially include:

1.The End Point Devices

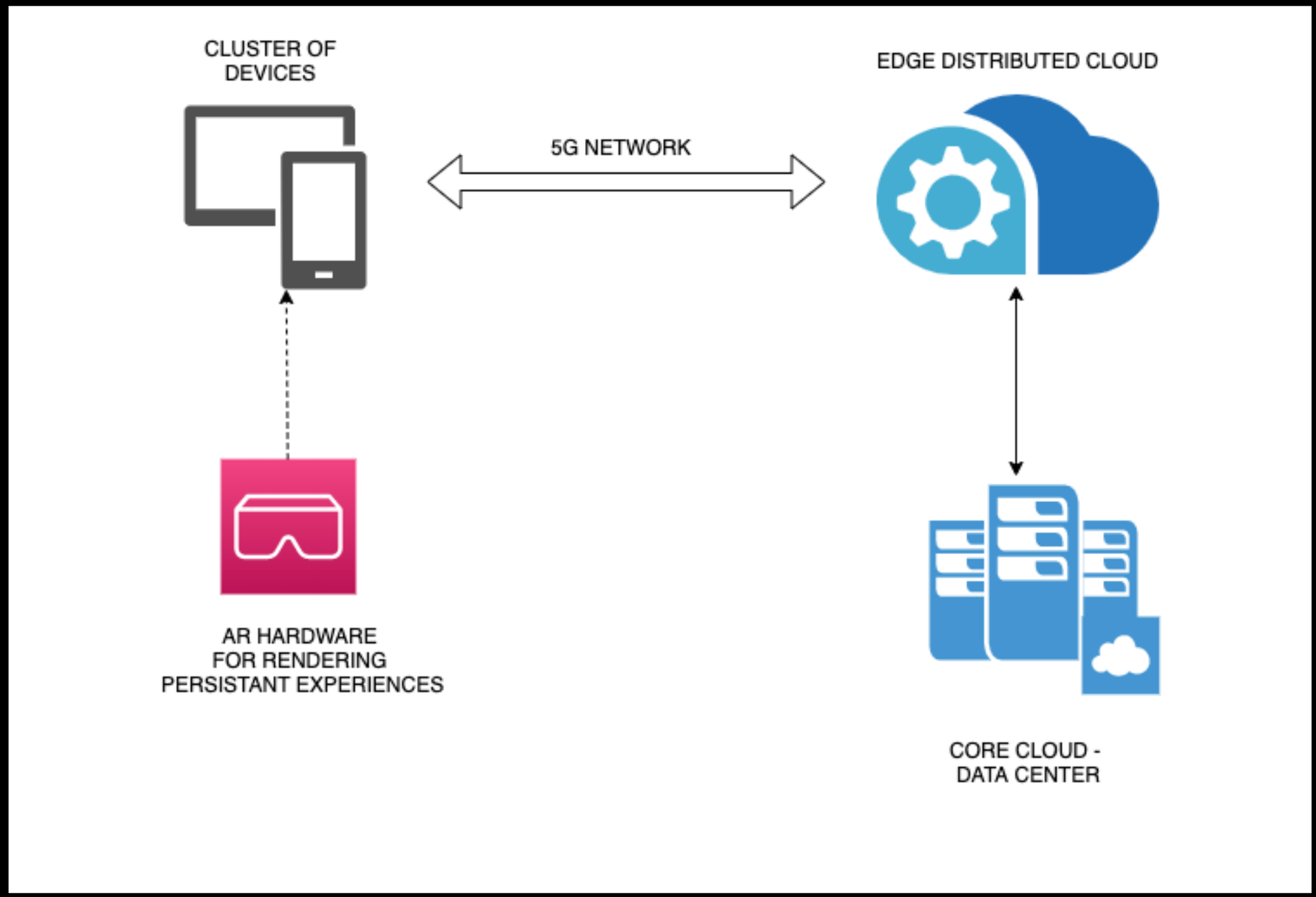
2.The Network Channel

3.The Edge Cloud

4.The Core Cloud

5.The Cloud Infrastructure Service

AR-CLOUD ARCHITECURE



Possible Architecture for an AR-Cloud

ATTACK SURFACE

- The attack surface based on the architecture will be familiar to everyone. But is still covered in brief for a complete picture.

- The main difference that this technology will bring about and to be considered as one of the biggest potential security risk will be focused in more detail.

ATTACK SURFACE - 1

END POINT DEVICES

- 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.

ATTACK SURFACE - 2

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 using TLS and IPsec.

ATTACK SURFACE - 3

EDGE CLOUD

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.

ATTACK SURFACE - 4

DATA CENTERS

- 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.

- In 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.

> 3-D SYSTEMS

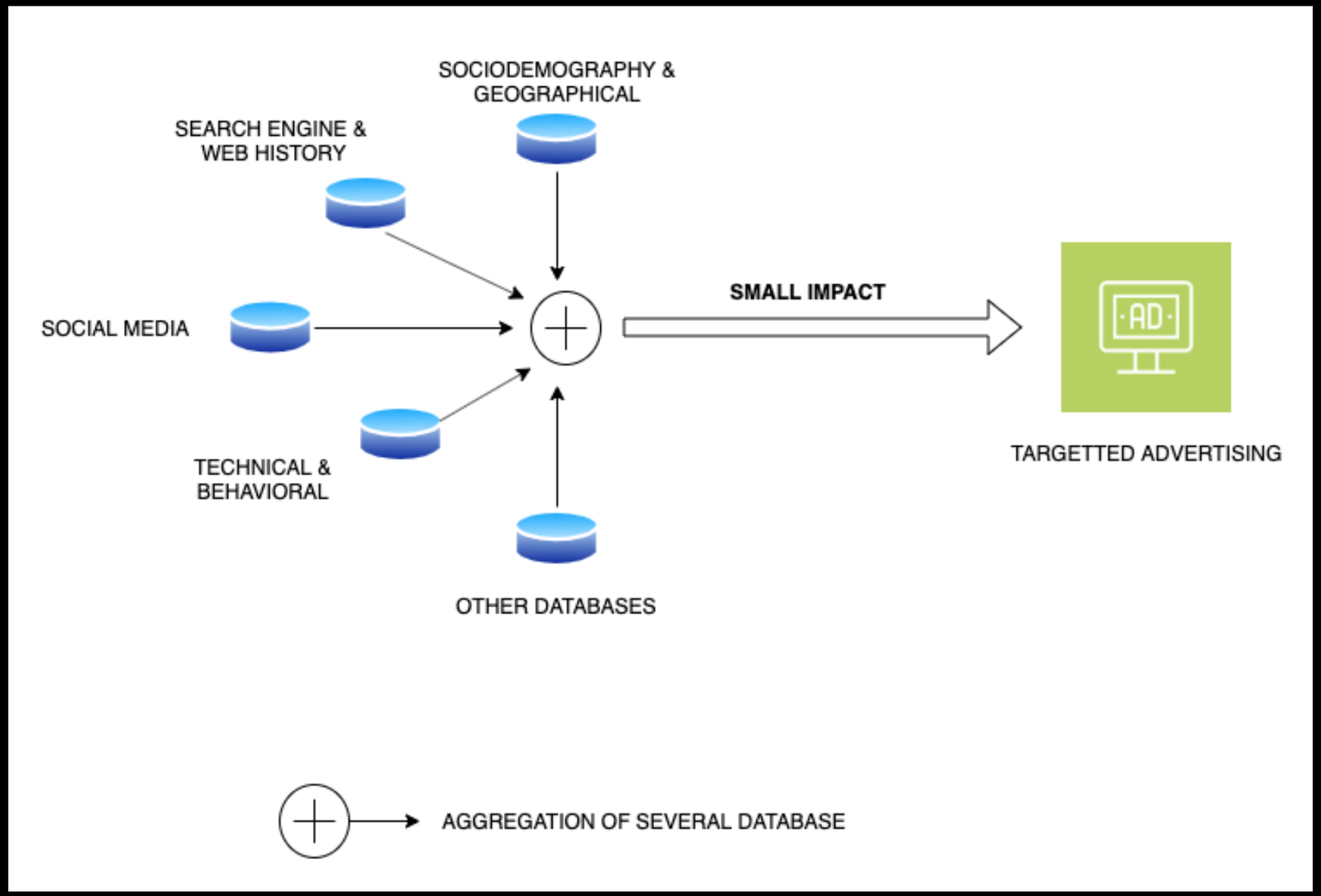
- The security requirements required for this more than 3-D digital system is closely similar to a 2-D digital system.

- Because similar architecture will be used for most of the services.

- The main difference is the “DATA” that is analyzed by the AR-Cloud system.

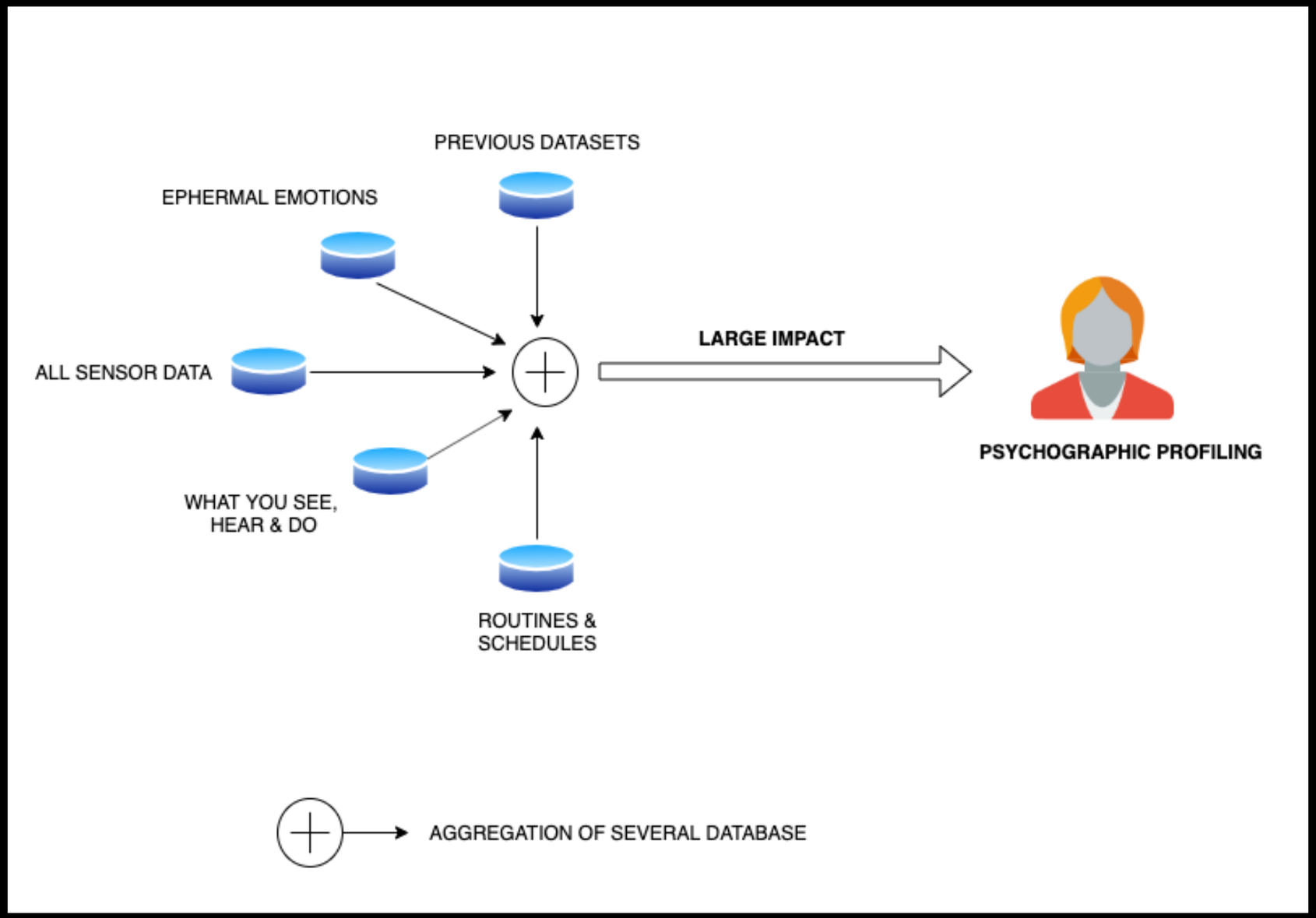
- DATA can include biometric data, what we see, what we respond to, galvanic skin response, facial expressions, emotions (brain waves), etc.

NOW - THEY KNOW WHAT YOU LIKE



- Aggregation of datasets can lead to a small scale influences through targeted advertisements.
- Mass influence using strategic communication and data analysis.

LATER - THEY KNOW YOU



- Psychographic profiling to estimate your actions and at an extreme case, control your actions.
- Miss association of user actions and responses generating a misleading profile.

PRIVACY PROTECTION SCHEMES

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.

Significant Privacy Preserving Methods (in development):

1. Decentralized Architectures
2. Homomorphic Encryption
3. Differential Privacy

DECENTRALIZED ARCHITECTURE

- A user’s 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.

- This provides the user to provide a fine granular access control and consent mechanism.

- This architecture preserves user relationship privacy.

DECENTRALIZED ARCHITECTURE

Access Policies associated to an object:

- The policies are either attribute-based, identity-based, or a combination of both types.

- The Read, Write, Append policies are defined by the owner at the time of object creation and are stored in the object metadata.

- These policies are enforced through the use of cryptography.

DECENTRALIZED ARCHITECTURE

Cryptographic Protection:

- Each user becomes a key authority, issuing different encryption keys to social contacts based on their attributes

- The message is encrypted with a randomly chosen symmetric encryption key, which is in turn encrypted with Attribute Based Encryption.

DECENTRALIZED ARCHITECTURE

Distributed Hash Table

- DHT creates a scalable key-value store with an efficient lookup mechanism to locate nodes that store a given object.

- A user’s profile will be the root object, which contains references to other objects, such as contact information, a wall, photo albums, etc.

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.

- Wide-scale adaptation of this encryption method is not popular, since it is resource intensive.

- Also the privacy is only maintained as long as the data is encrypted.

DIFFERENTIAL PRIVACY

- 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.

- Differential Privacy technology to help discover the usage patterns of a large number of users without compromising individual privacy.

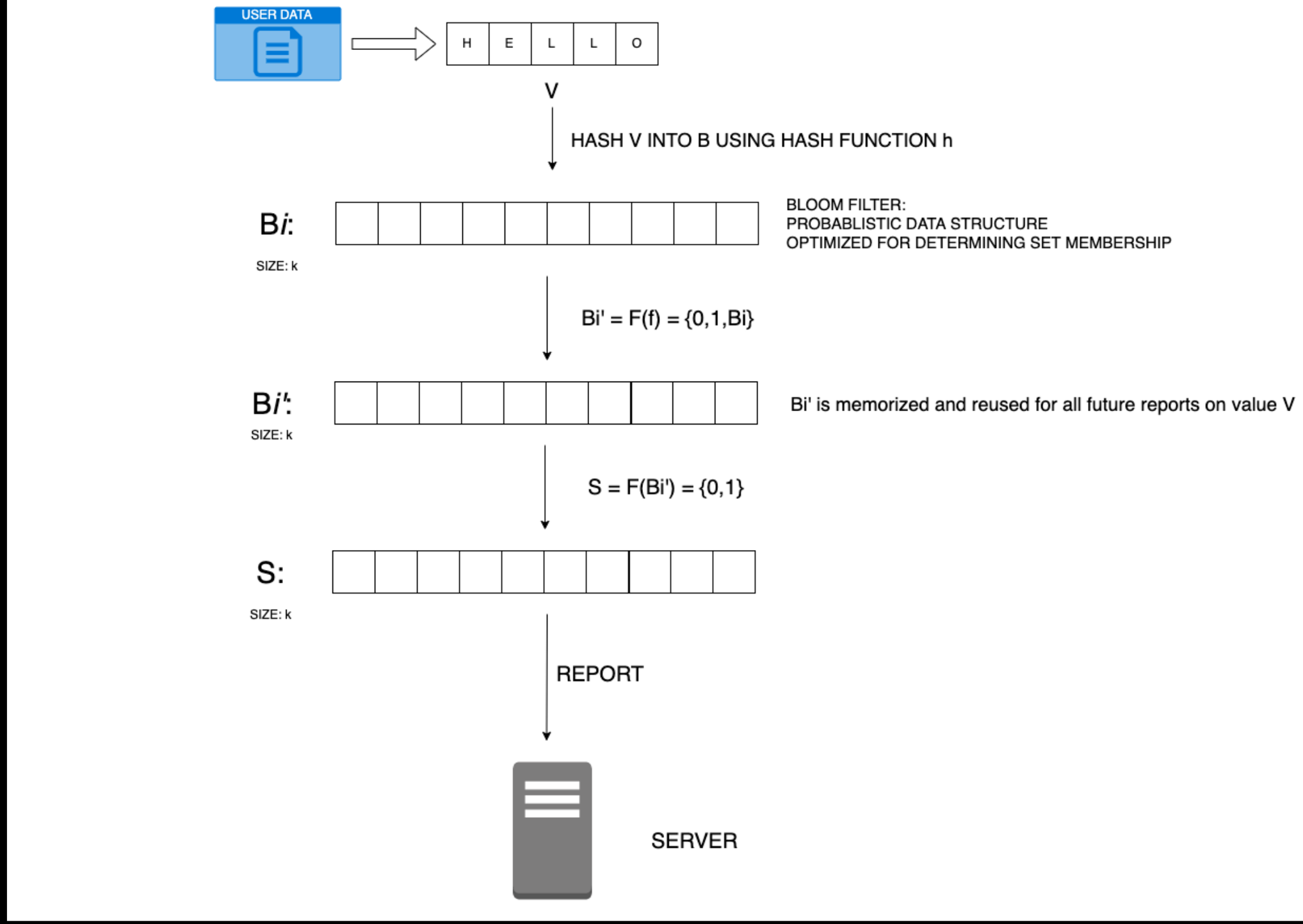
- To obscure an individual’s identity, Differential Privacy adds mathematical noise to a small sample of the individual’s usage pattern.

GOOGLE'S RAPPOR

- On a high level, RAPPOR achieves this by having each client machine report a "noisy" representation of the true value "v" by submitting a k-sized bit array to a server. This representation of v is selected in order to reveal a specific amount of information about v in order to limit the information the server learns from the k-sized bit array.

- Importantly the server does not learn the true value v with confidence even when an infinite number of reports are submitted by the client.

GOOGLE'S RAPPOR



CONCLUSION

- AR-Cloud is considered to be the next technology that will bring the greatest digital revolution.
- Realized possible AR-Cloud architectures and security and privacy threats to the parties involved.
- Considered possible research solutions for preserving privacy.

REFERENCES

- https://arxiv.org/pdf/1111.5377.pdf
- https://secml.github.io/class4/
- https://www.forbes.com/sites/johnkoetsier/2019/02/21/augmented-reality-is-the-operating-system-of-the-future-ar-cloud-is-how-we-get-there/%23469bc9c425fb
- https://developer.6d.ai/user/dashboard/?view=ar_cloud_guide
- https://medium.com/openarcloud/privacy-manifesto-for-ar-cloud-solutions-9507543f50b6
- https://thinkmobiles.com/blog/what-is-augmented-reality/
- https://medium.com/scape-technologies/building-the-ar-cloud-part-one-72a7c5cd9697

THANK YOU