The
University
Of
Sheffield.

Towards User-centric Privacy-preserving Techniques for Cloud-assisted IoT Applications

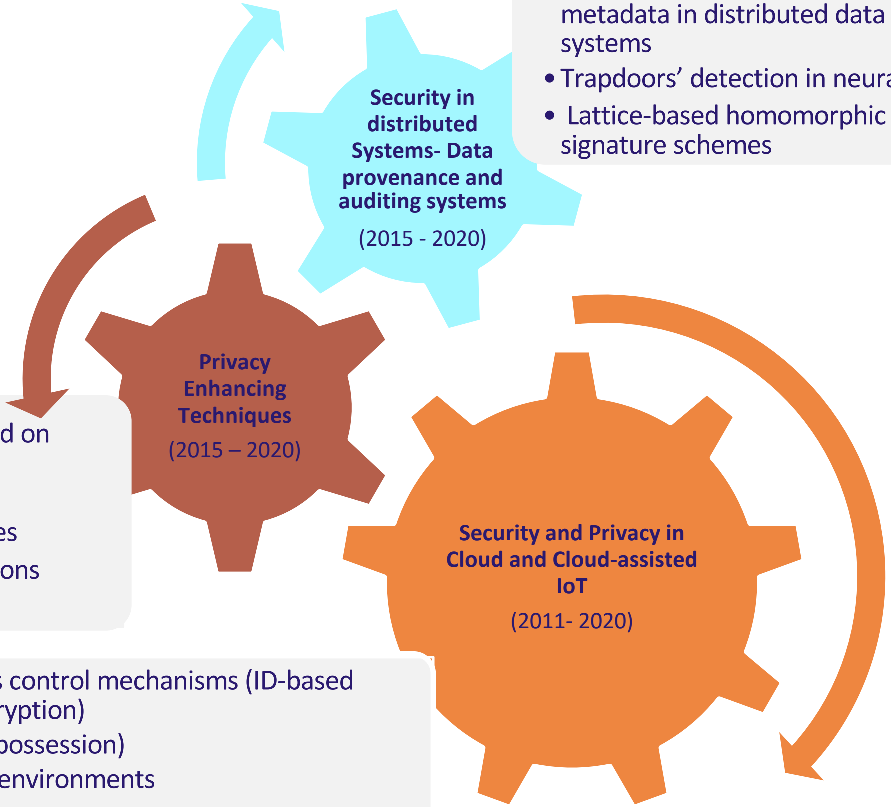
Nesrine Kaaniche
n.kaaniche@sheffield.ac.uk

Security of Advanced Systems Research Group
Department of Computer Science

June 9th, 2020

A little bit about me!

- ○ **Lecturer in Cybersecurity ,** Department of Computer Science, Affiliated with the Security of Advanced Systems group, University of Sheffield, UK
- ○ **Associate Member** of the Chair Values and Policies of Personal Information, Institute Mines Telecom, France



Security in distributed Systems- Data provenance and auditing systems

(2015 - 2020)

- Applications/Design of attribute based cryptographic techniques
- **Visiting researcher (Stanford Research Institute (SRI) International) :** Integrity of metadata in distributed data provenance systems
- Trapdoors' detection in neural networks
- Lattice-based homomorphic encryption and signature schemes

Privacy Enhancing Techniques

(2015 – 2020)

- Anonymous certification scheme, based on attribute based signatures
- Blockchain-based applications
- Privacy-preserving personalised services
- Informed consent in e-Health Applications

Security and Privacy in Cloud and Cloud-assisted IoT

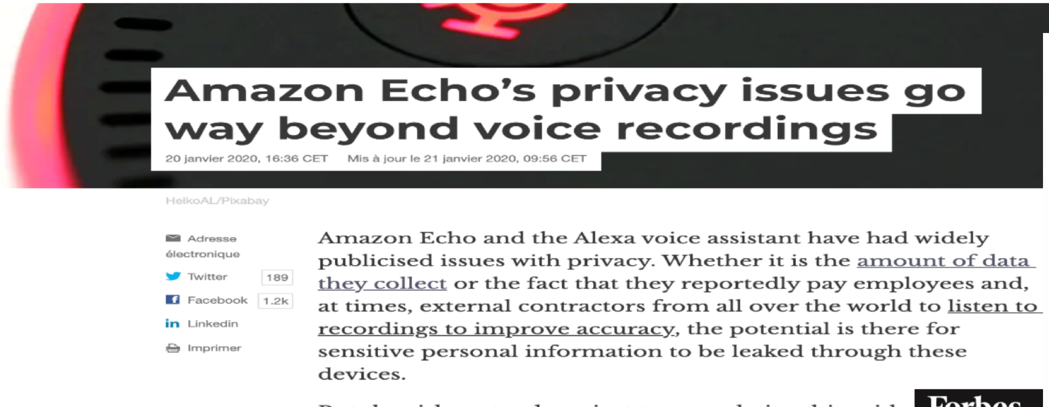
(2011- 2020)

- Data confidentiality and access control mechanisms (ID-based encryption, homomorphic encryption)
- Data integrity (proofs of data possession)
- Authenticated search in cloud environments
- Formal validation, experimentation

Outline

- General Context
- Privacy Preserving Cooperative Computation
- Privacy Preserving Fine grained Access Control to Outsourced Data
- Interdisciplinary Discussion
- Conclusions

Who possess our data? What they know about us? How they are using our data?



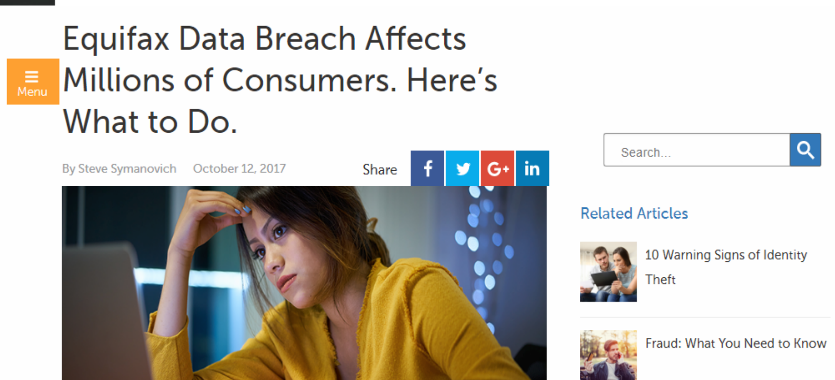
Amazon Echo's privacy issues go way beyond voice recordings

20 janvier 2020, 16:36 CET Mis à jour le 21 janvier 2020, 09:56 CET

HeikoAL/Pixabay

- Adresse électronique
- Twitter 189
- Facebook 1.2k
- Linkedin
- Imprimer

Amazon Echo and the Alexa voice assistant have had widely publicised issues with privacy. Whether it is the amount of data they collect or the fact that they reportedly pay employees and, at times, external contractors from all over the world to listen to recordings to improve accuracy, the potential is there for sensitive personal information to be leaked through these devices.



≡ Menu

Equifax Data Breach Affects Millions of Consumers. Here's What to Do.

By Steve Symanovich October 12, 2017

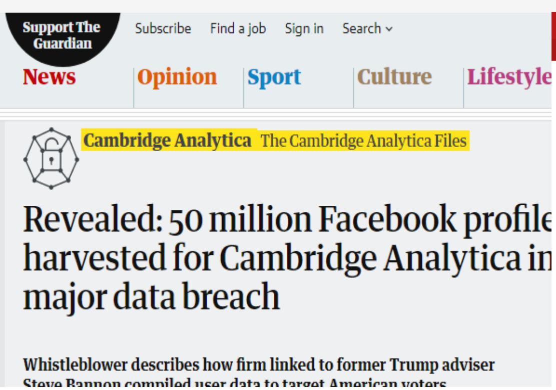
Share f t G+ in

Search...

Related Articles

10 Warning Signs of Identity Theft

Fraud: What You Need to Know



Support The Guardian

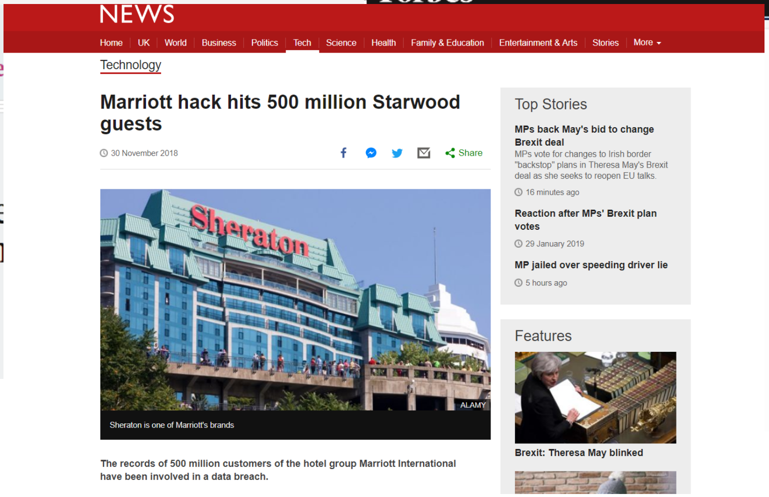
Subscribe Find a job Sign in Search

News Opinion Sport Culture Lifestyle

Cambridge Analytica The Cambridge Analytica Files

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach

Whistleblower describes how firm linked to former Trump adviser Steve Bannon compiled user data to target American voters



NEWS

Home | UK | World | Business | Politics | Tech | Science | Health | Family & Education | Entertainment & Arts | Stories | More

Technology

Marriott hack hits 500 million Starwood guests

30 November 2018

Share

ALAMY

Sheraton is one of Marriott's brands

The records of 500 million customers of the hotel group Marriott International have been involved in a data breach.

Top Stories

MPs back May's bid to change Brexit deal

MPs vote for changes to Irish border "backstop" plans in Theresa May's Brexit deal as she seeks to reopen EU talks.

16 minutes ago

Reaction after MPs' Brexit plan votes

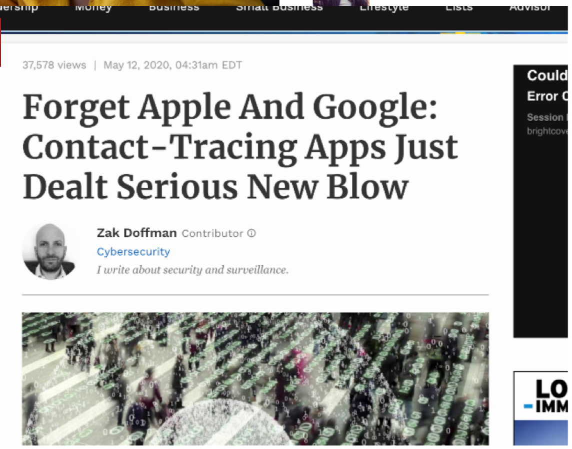
29 January 2019

MP jailed over speeding driver lie

5 hours ago

Features

Brexit: Theresa May blinked



Forbes

Billionaires Innovation Leadership Money Business Small Business Lifestyle Lists Advisor

37,578 views | May 12, 2020, 04:31am EDT

Forget Apple And Google: Contact-Tracing Apps Just Dealt Serious New Blow

Zak Doffman Contributor

Cybersecurity

I write about security and surveillance.

Privacy as a Security Property?

Confidentiality

Keep your secrets, well, secret

Control

Who? And How can use your personal information?

Beyond Technology/Engineering:

A lot of aspects related to sociology, law, psychology, economics, *etc*. ..

Privacy Enhancing Technologies

Mitigate privacy threats

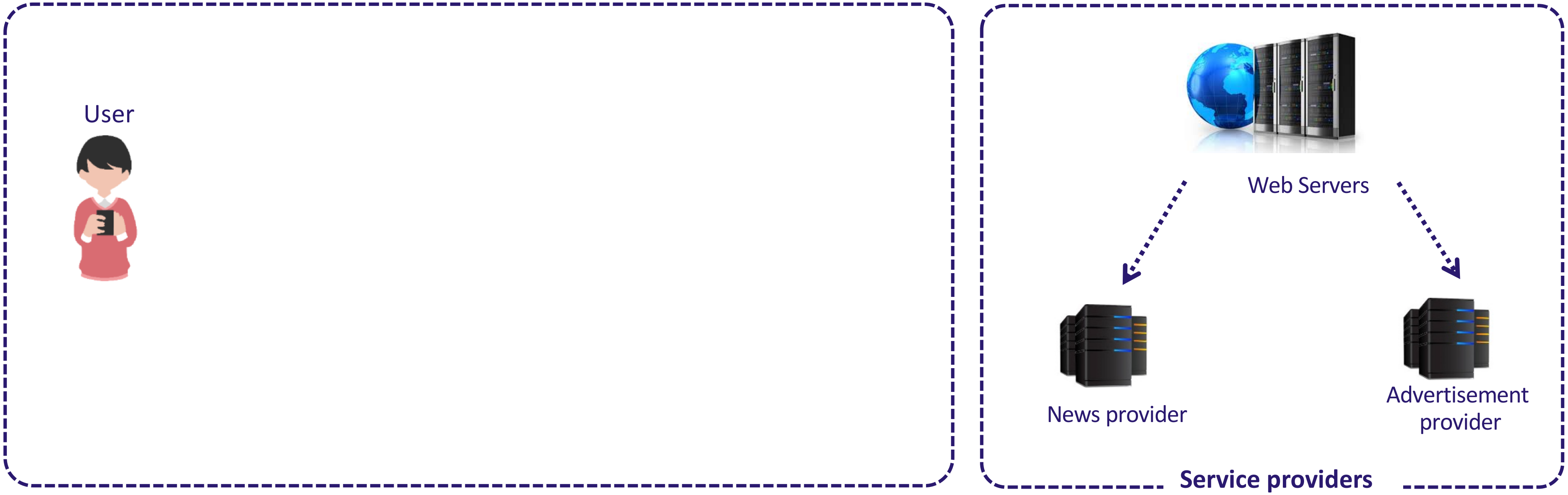
Increase privacy of users, groups, organizations

Enable scenarios impossible w/o strong privacy guarantees

Privacy Preserving Cooperative Computation

Personalisation vs Privacy -Web Search Engines

Web Search Engine: Privacy Challenges



User

Web Servers

News provider

Advertisement provider

Service providers

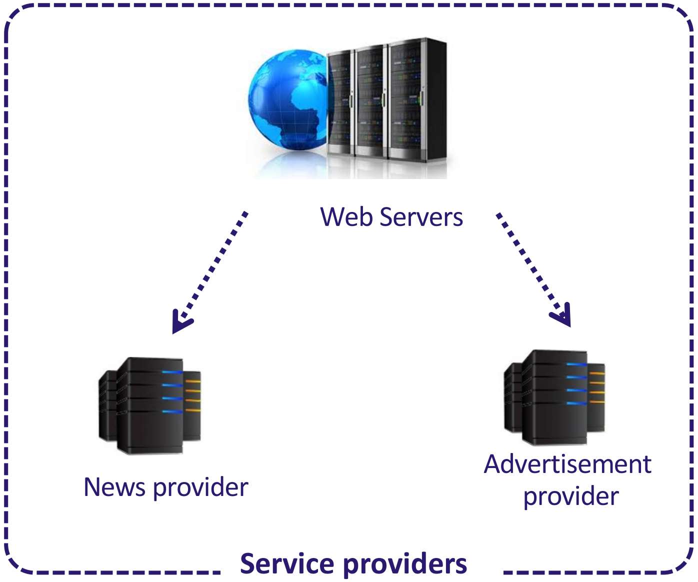
The service provider is a search engine, interacting with an advertising and news agency.

Ads and news are also categorized and annotated by keywords.

Web Search Engine: Privacy Challenges

❌ **Need for privacy preserving matching techniques**

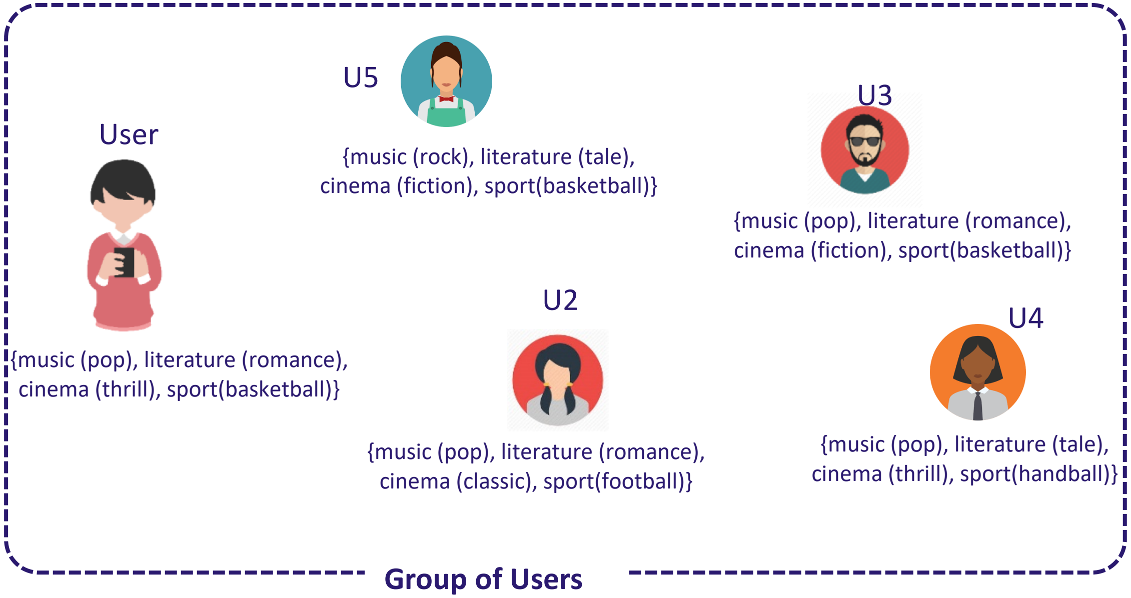
Need for privacy preserving search techniques



The service provider is a search engine, interacting with an advertising and news agency.

Ads and news are also categorized and annotated by keywords.

Privacy-preserving WSE: a collaborative approach



User

{music (pop), literature (romance), cinema (thrill), sport(basketball)}

U5

{music (rock), literature (tale), cinema (fiction), sport(basketball)}

U3

{music (pop), literature (romance), cinema (fiction), sport(basketball)}

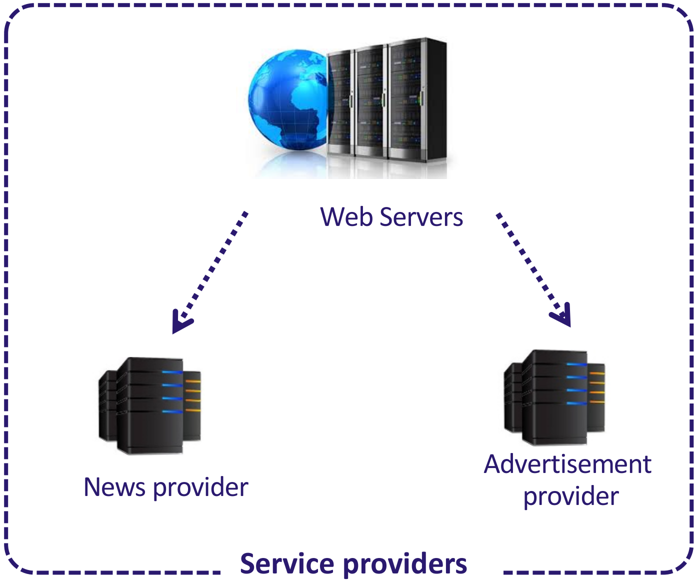
U2

{music (pop), literature (romance), cinema (classic), sport(football)}

U4

{music (pop), literature (tale), cinema (thrill), sport(handball)}

Group of Users



Web Servers

News provider

Advertisement provider

Service providers

Each client belongs to a group of users, sharing the same interests ➔ each client obtains a characterizing profile, encompassing several categories.

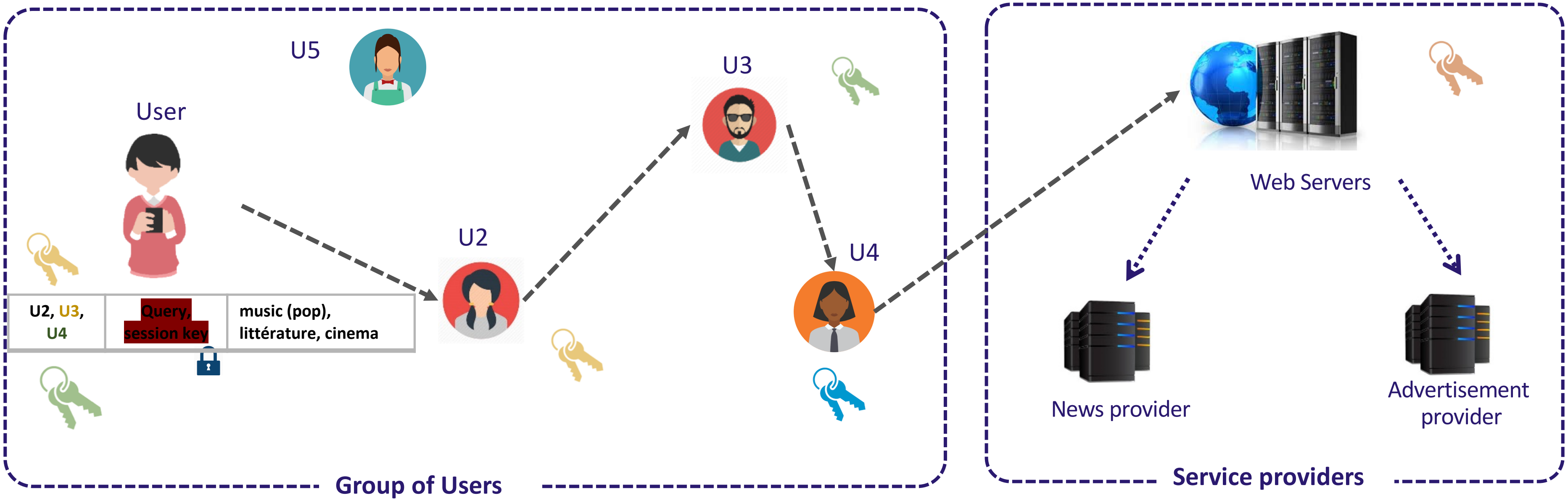
The service provider is a search engine, interacting with an advertising and news agency.
Ads and news are also categorized and annotated by keywords.

- Collaboration with Qwant, France – https://github.com/QwantResearch/masq-app/

- **Kaaniche** N., Masmoudi S, Znina S., Laurent M. and Demir L., Privacy Preserving Cooperative Computation for Personalized Web Search Applications, 35th ACM SAC 2020

Privacy-preserving WSE: a collaborative approach

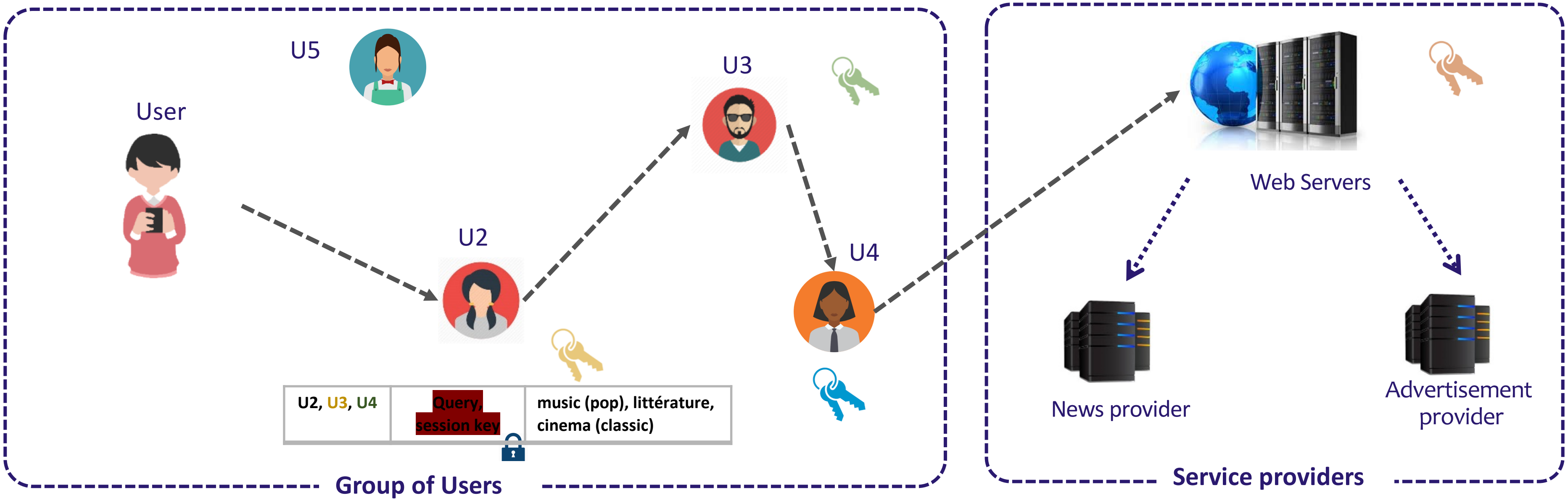
Query’s submission process



U2, U3, U4	Query, session key	music (pop), littérature, cinema

Privacy-preserving WSE: a collaborative approach

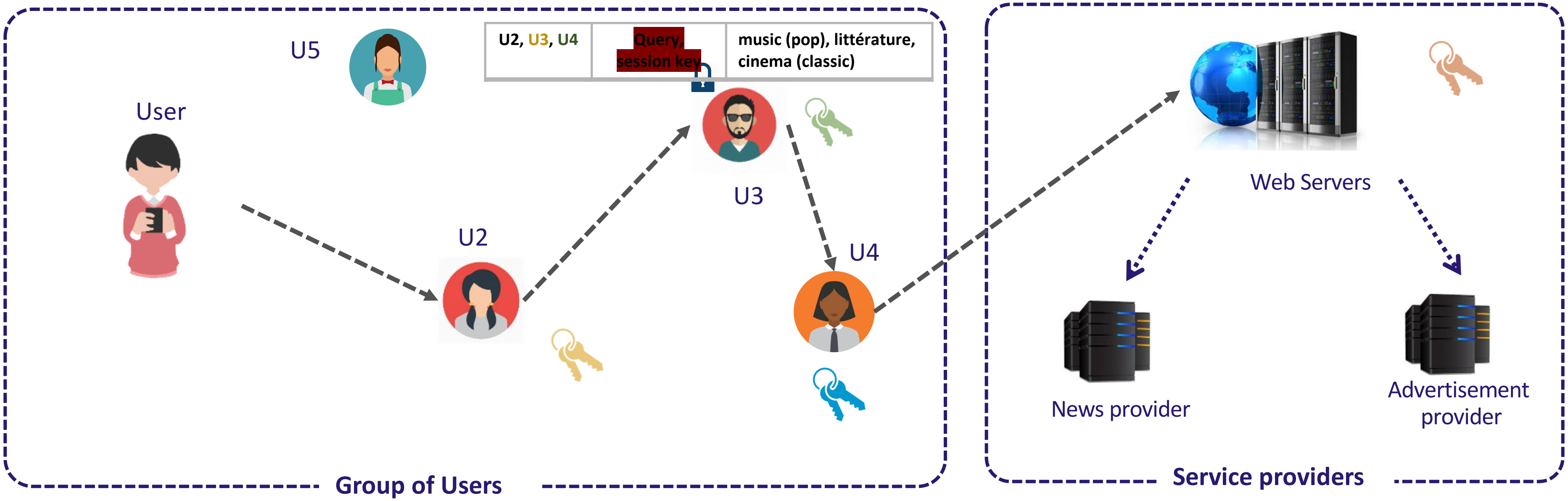
Query’s submission process



U2, U3, U4	Query, session key	music (pop), littérature, cinema (classic)

Privacy-preserving WSE: a collaborative approach

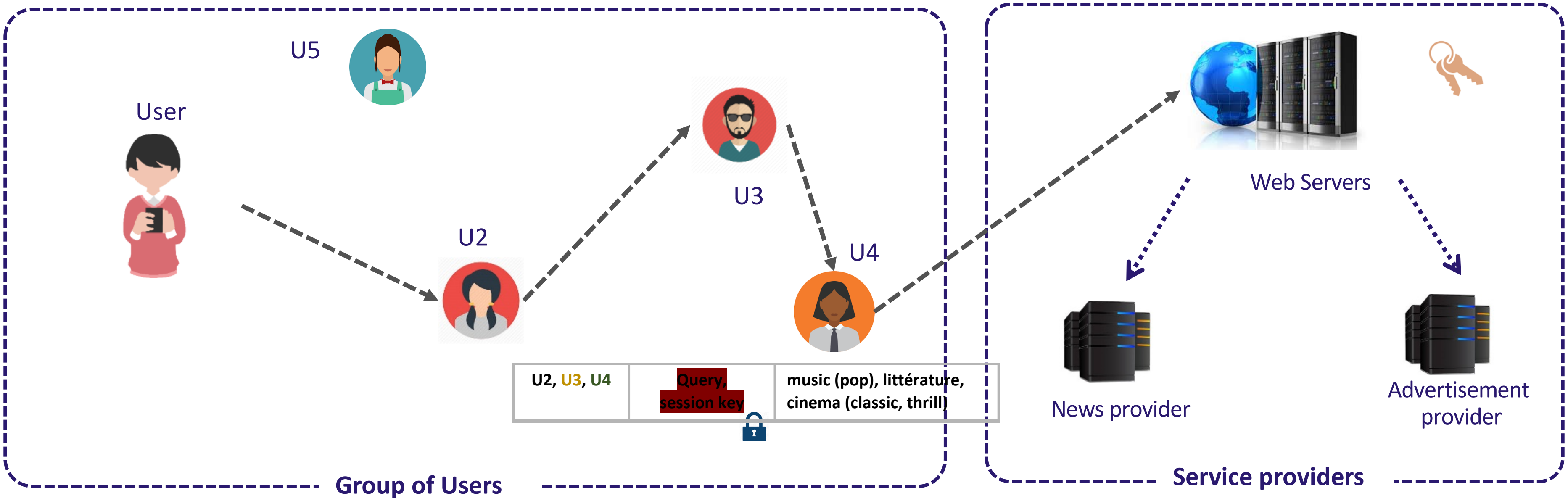
Query's submission process



U2, U3, U4	Query, session key	music (pop), littérature, cinema (classic)

Privacy-preserving WSE: a collaborative approach

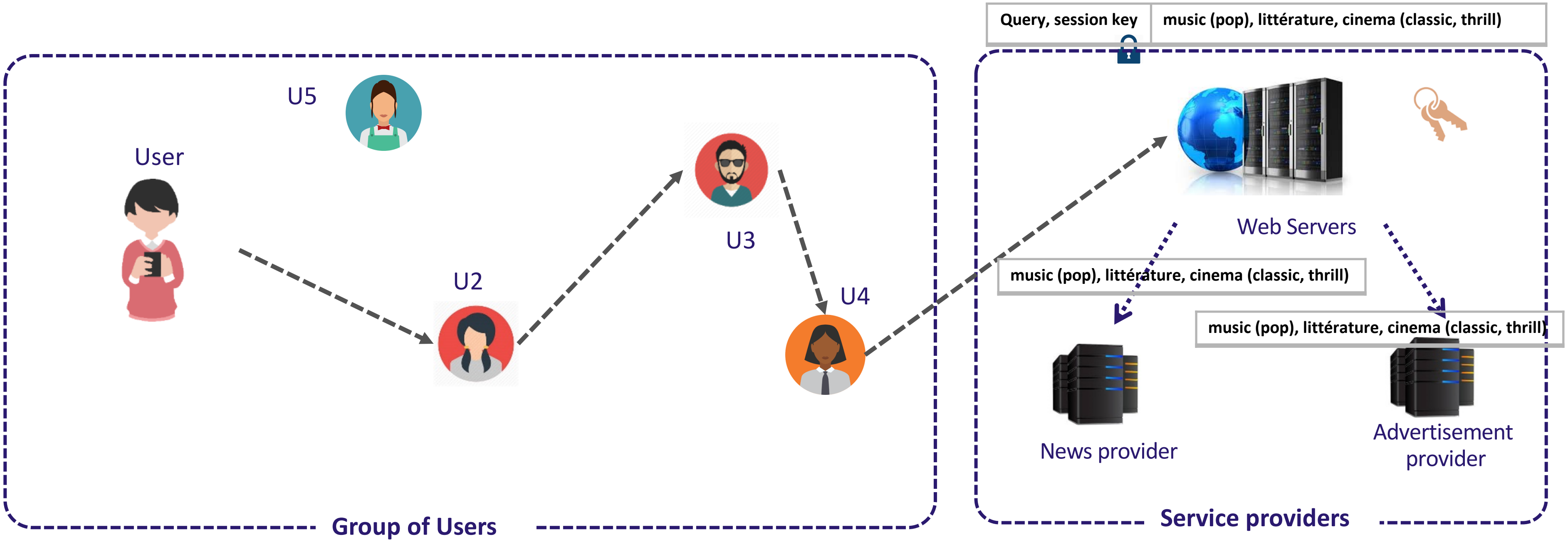
Query's submission process



U2, U3, U4	Query, session key	music (pop), littérature, cinema (classic, thrill)

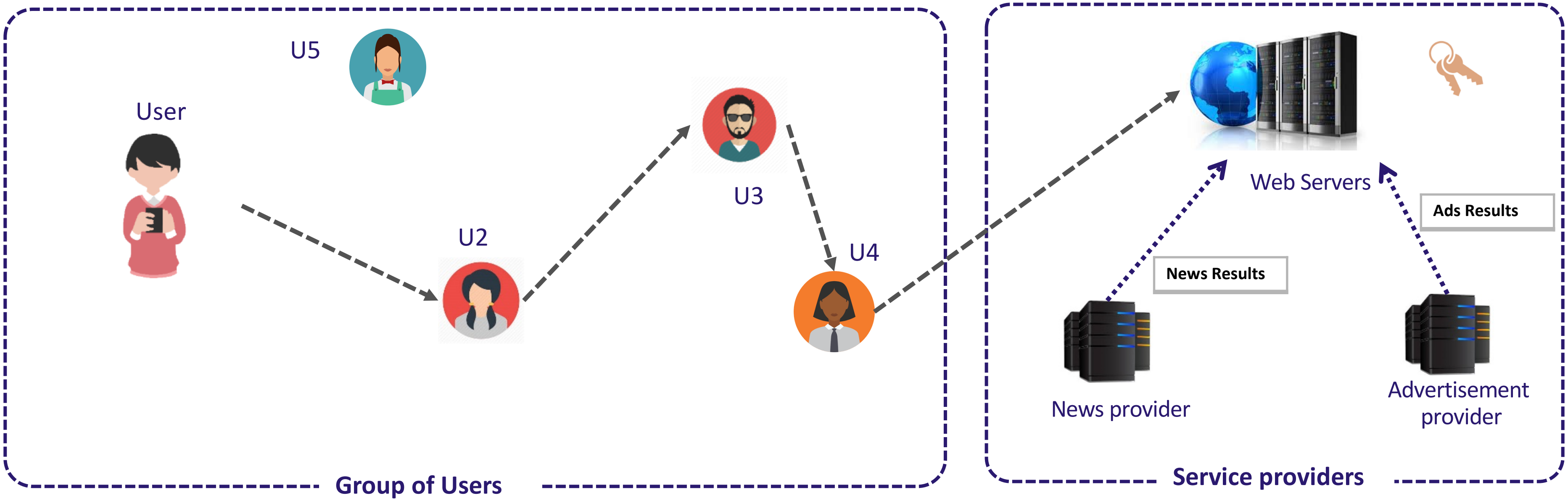
Privacy-preserving WSE: a collaborative approach

Query's submission process


Query, session key
music (pop), littérature, cinema (classic, thrill)
U5
User
U3
U2
U4
Web Servers
music (pop), littérature, cinema (classic, thrill)
music (pop), littérature, cinema (classic, thrill)
News provider
Advertisement provider
Group of Users
Service providers

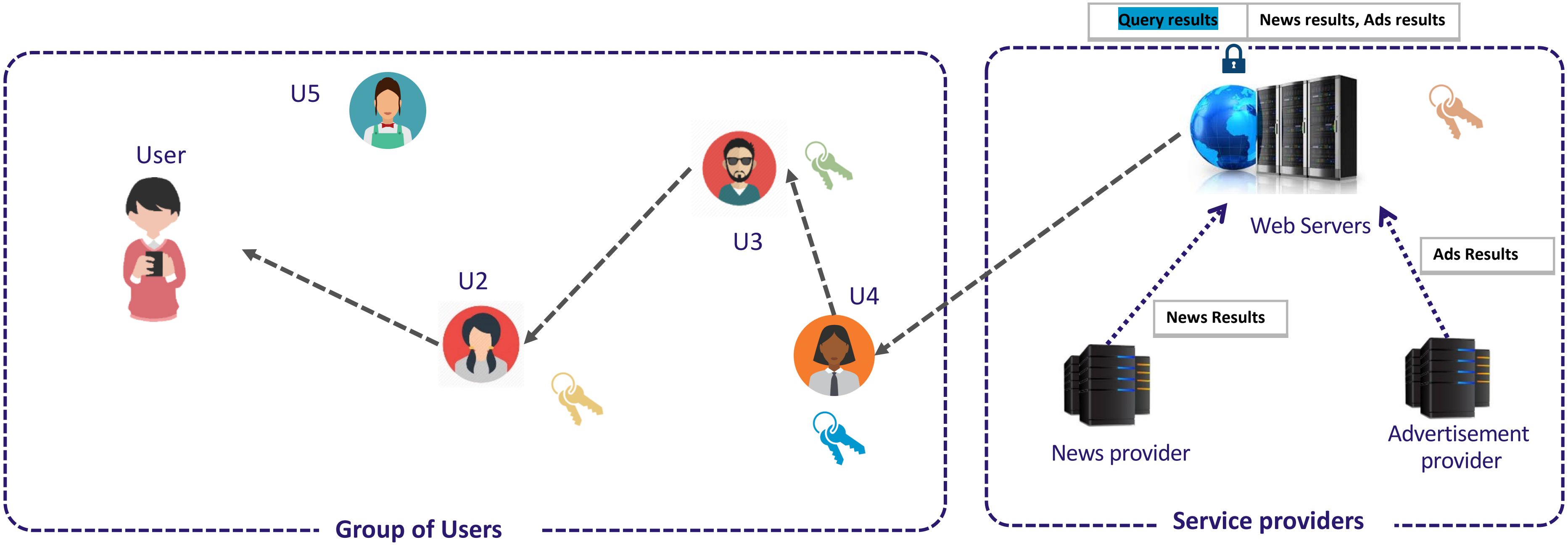
Privacy-preserving WSE: a collaborative approach

Query's response process



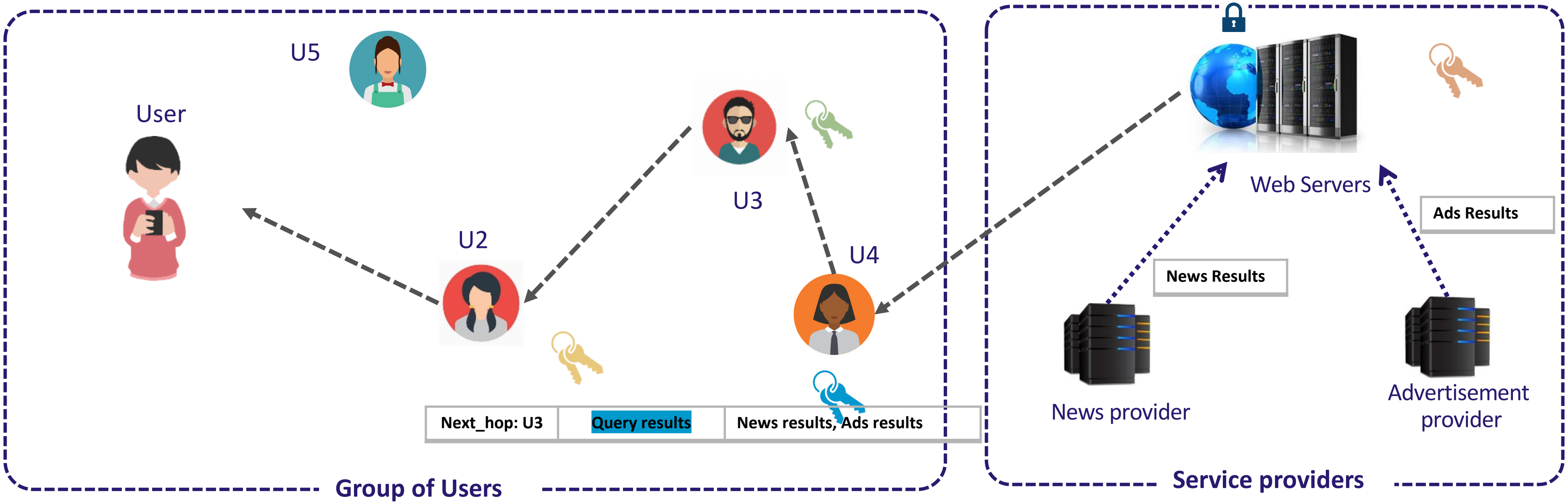
Privacy-preserving WSE: a collaborative approach

Query's response process



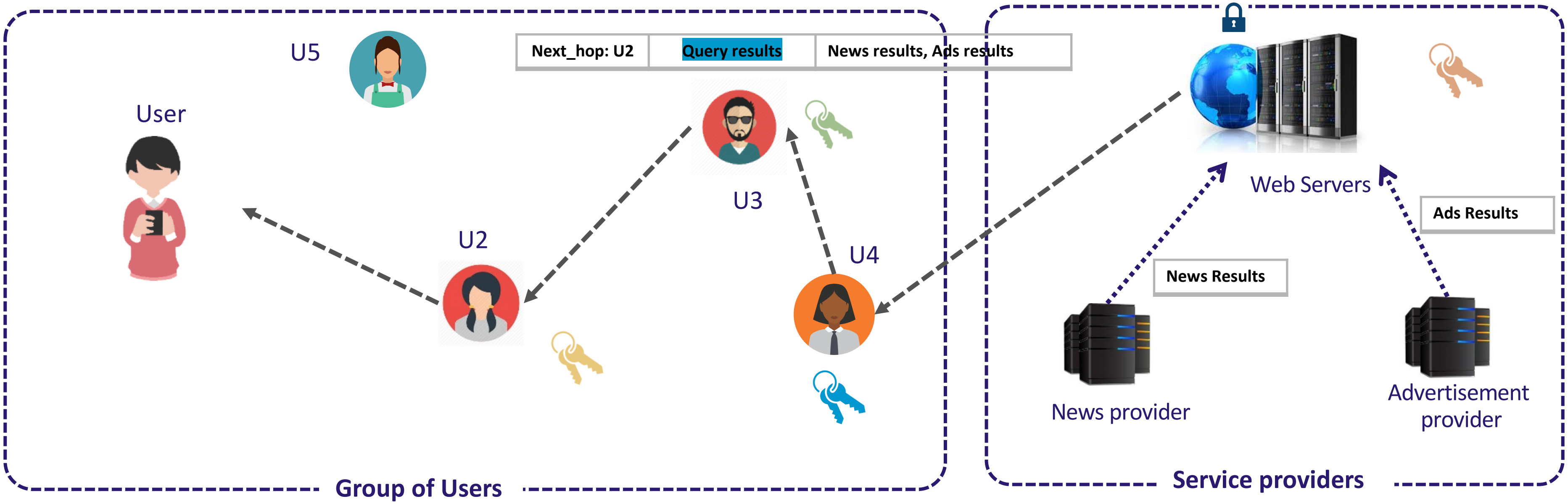
Privacy-preserving WSE: a collaborative approach

Query's response process



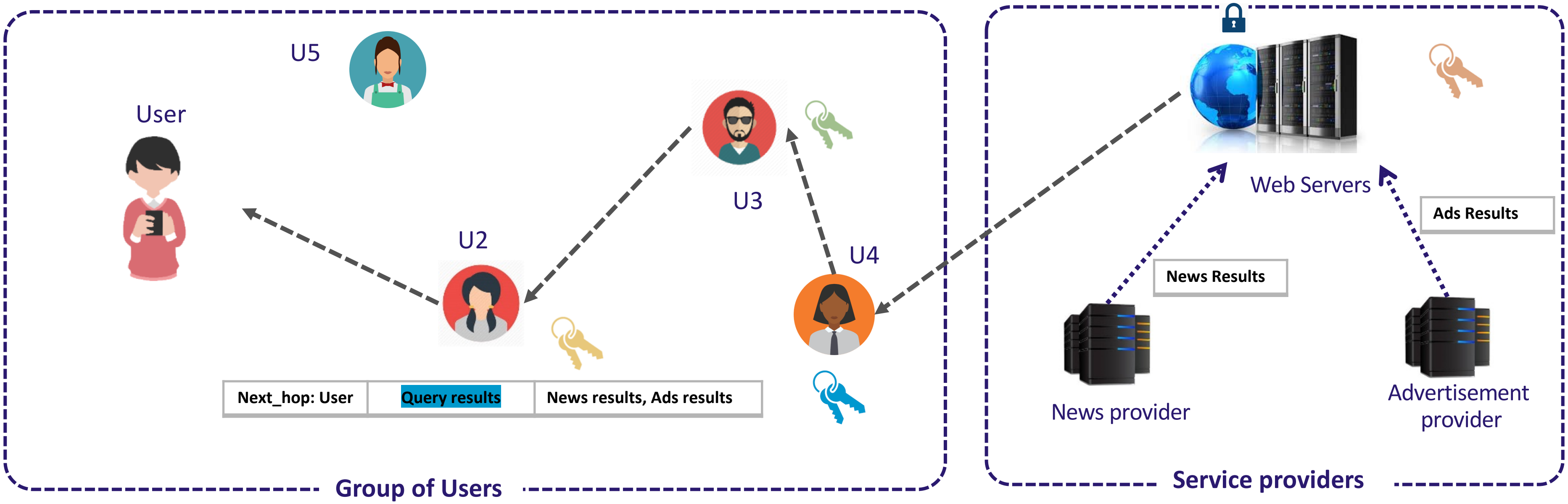
Privacy-preserving WSE: a collaborative approach

Query's response process



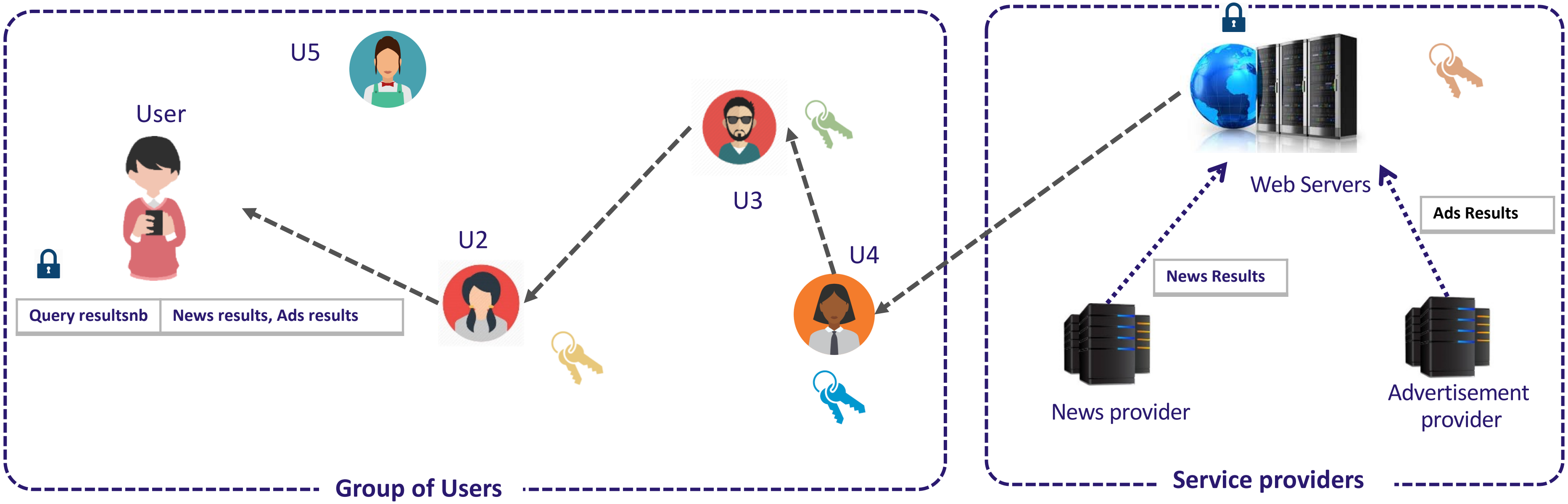
Privacy-preserving WSE: a collaborative approach

Query's response process



Privacy-preserving WSE: a collaborative approach

Query's response process



- Collaboration with Qwant, France – https://github.com/QwantResearch/masq-app/

- **Kaaniche** N., Masmoudi S, Znina S., Laurent M. and Demir L., Privacy Preserving Cooperative Computation for Personalized Web Search Applications, 35th ACM SAC 2020

Privacy-preserving WSE and beyond?

(+) Better outreach for WSE-side applications based on aggregated profiles

(+) User-empowerment: control of disclosed personal data

(-) Collaboration between users: Computation overhead

⇒ *Ongoing research: Perturbation at the client side*

(*) Personalization vs Privacy trade-offs

⇒ *Ongoing research: Reliance on ML algorithms to enhance privacy based on a GAN-inspired approach*

Privacy Preserving Fine grained Access Control to Outsourced Data

Access Control in the Cloud: Challenges?

Access Control List (ACL):

- Save users identities in ACL
- Check ACL to authorise users
- Managed by a trusted party

Role Based Access Control (RBAC):

- Identify users by roles
- Users’ roles match data roles
- Managed by a trusted party

Attribute-Based Access Control (ABAC):

- Identify users by attributes
- Users’ attributes match data roles
- Managed by a trusted party

!

- **Reliance on the cloud server**
- **Confidentiality against SP**
- **Privacy**

Encrypted Access Control in the Cloud

•**Selective En**

▪ Encrypting
outsourcing.
▪ Achieving f
based on effe

!

- **Key ma**
- **Confid**
- **Privacy**

•**Attribute Based Encryption**

• Both users' private keys and ciphertexts are associated with a set of attributes or a structure over attributes.

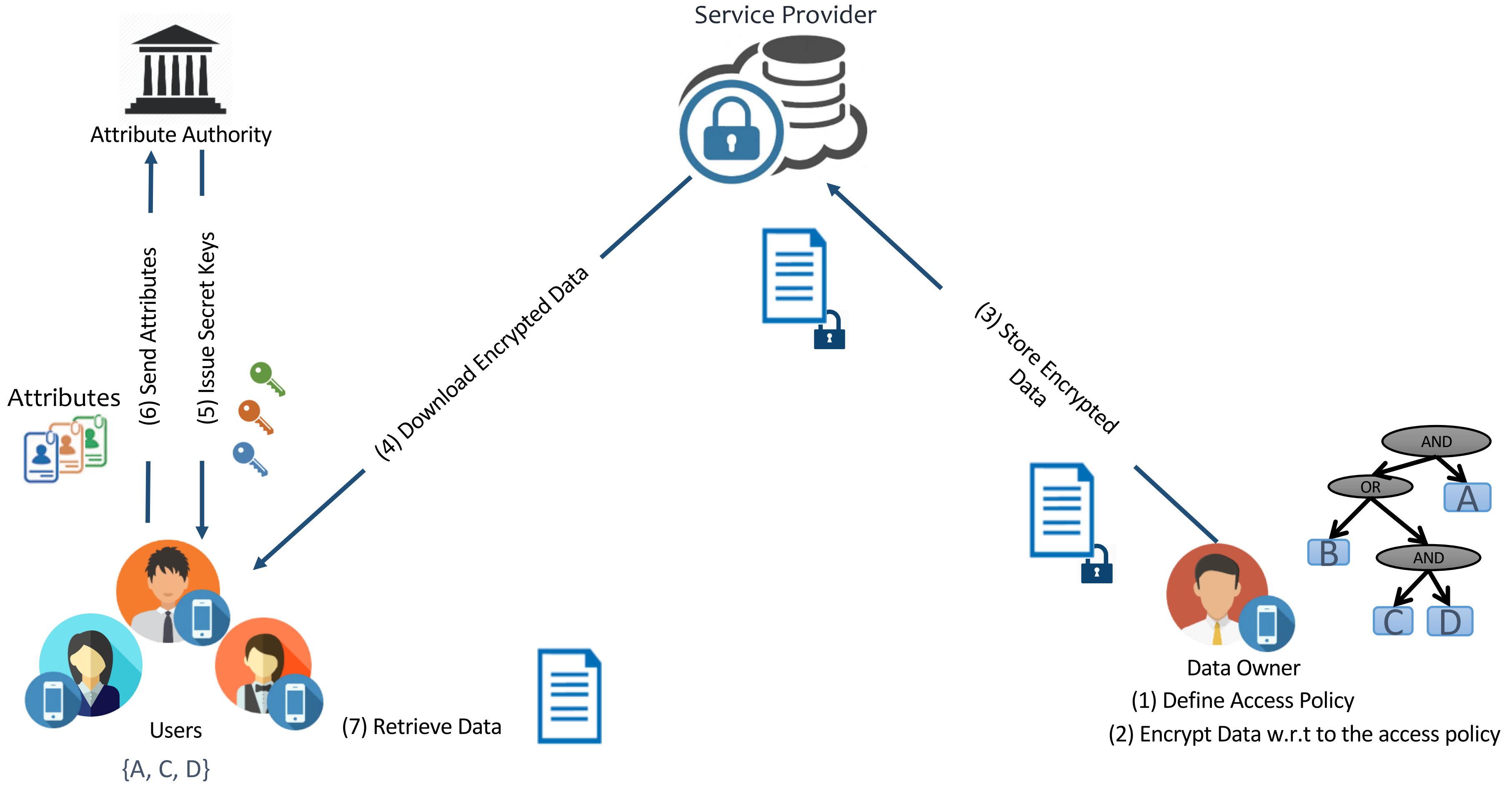
• User is able to decrypt a ciphertext if there is a match between his private key and the ciphertext

!

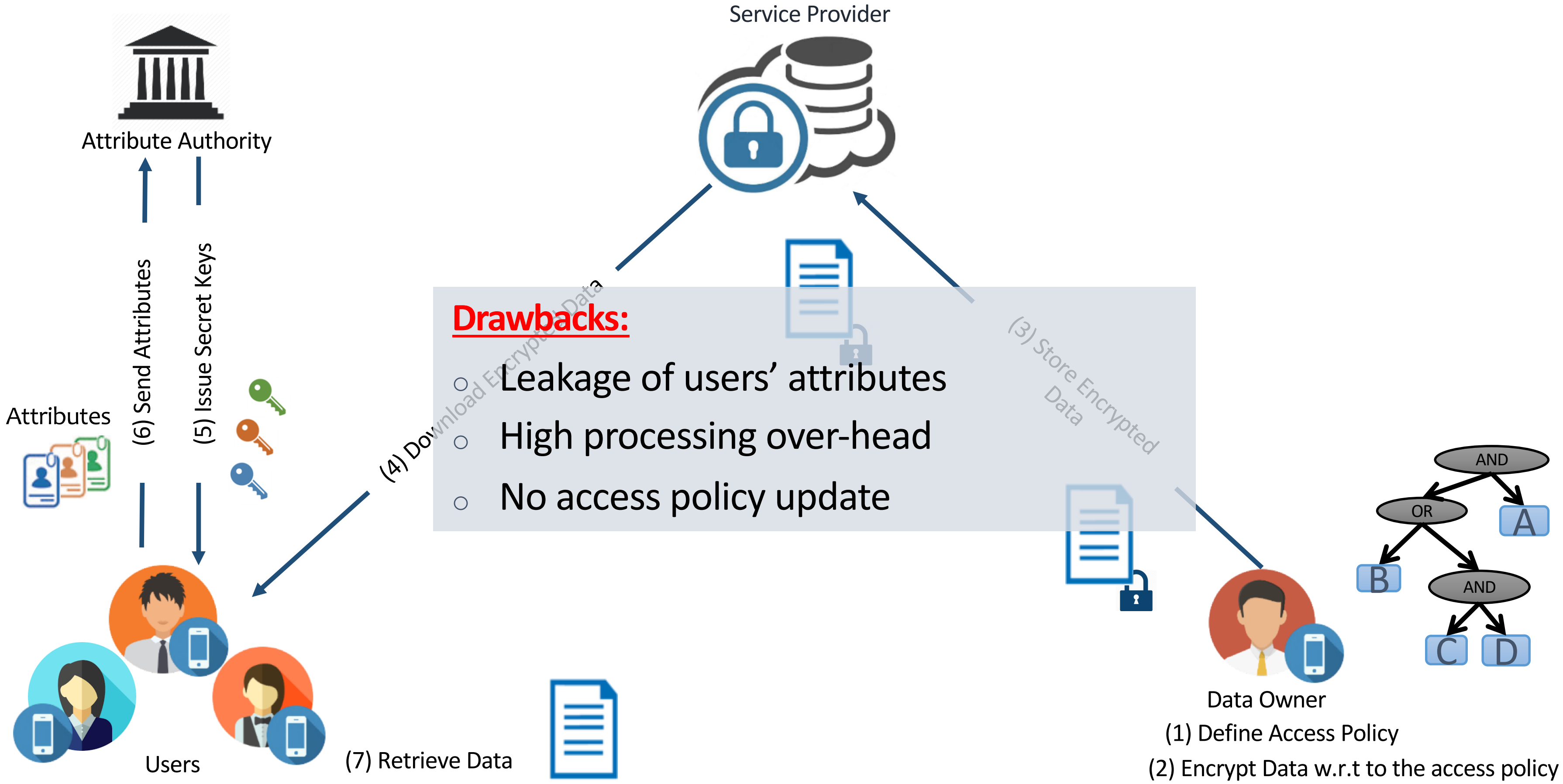
- Easier key management system
- Flexibility in specifying different access rights
- Confidentiality

A WORLD TOP 100 UNIVERSITY

Attribute Based Encryption (ABE)



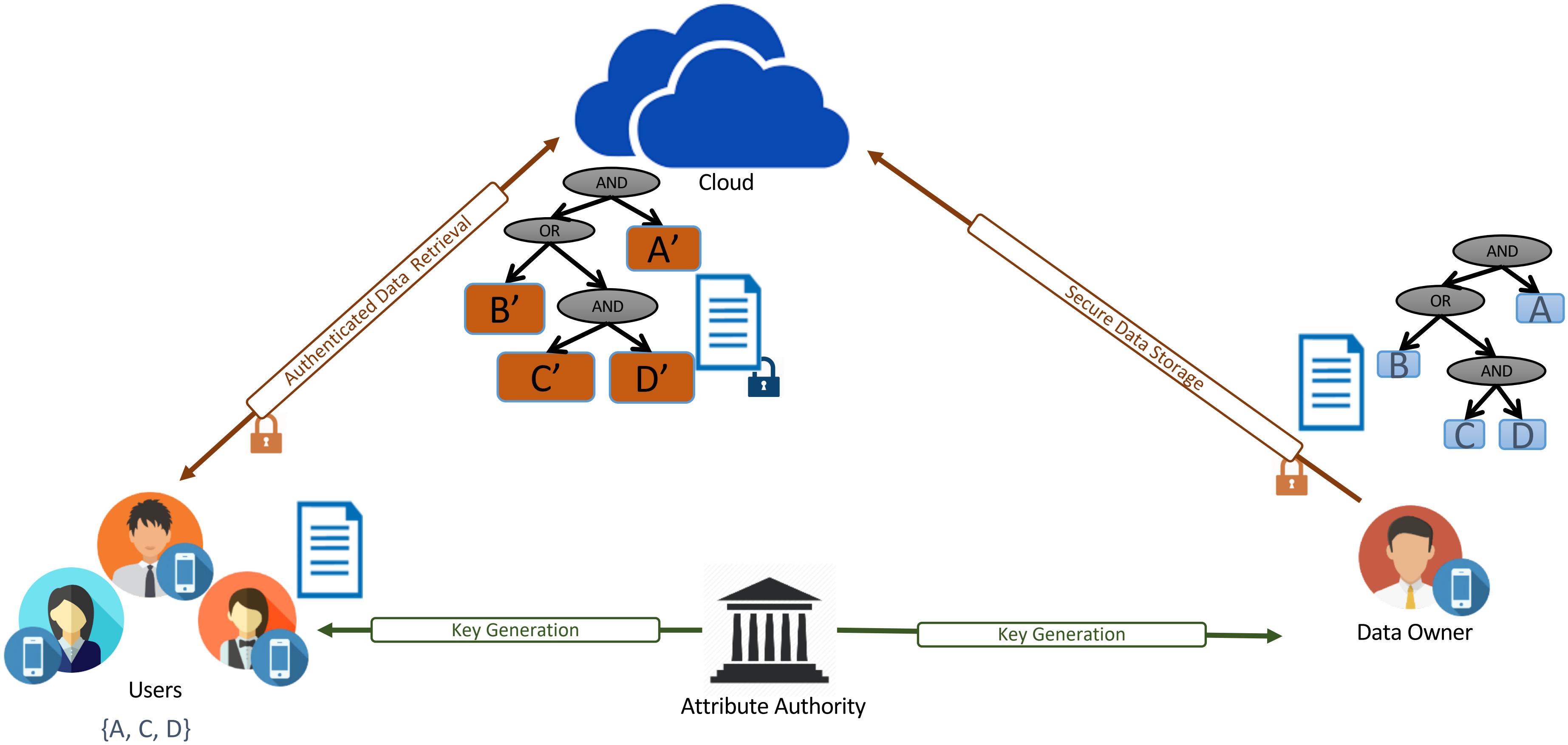
Attribute Based Encryption



Drawbacks:

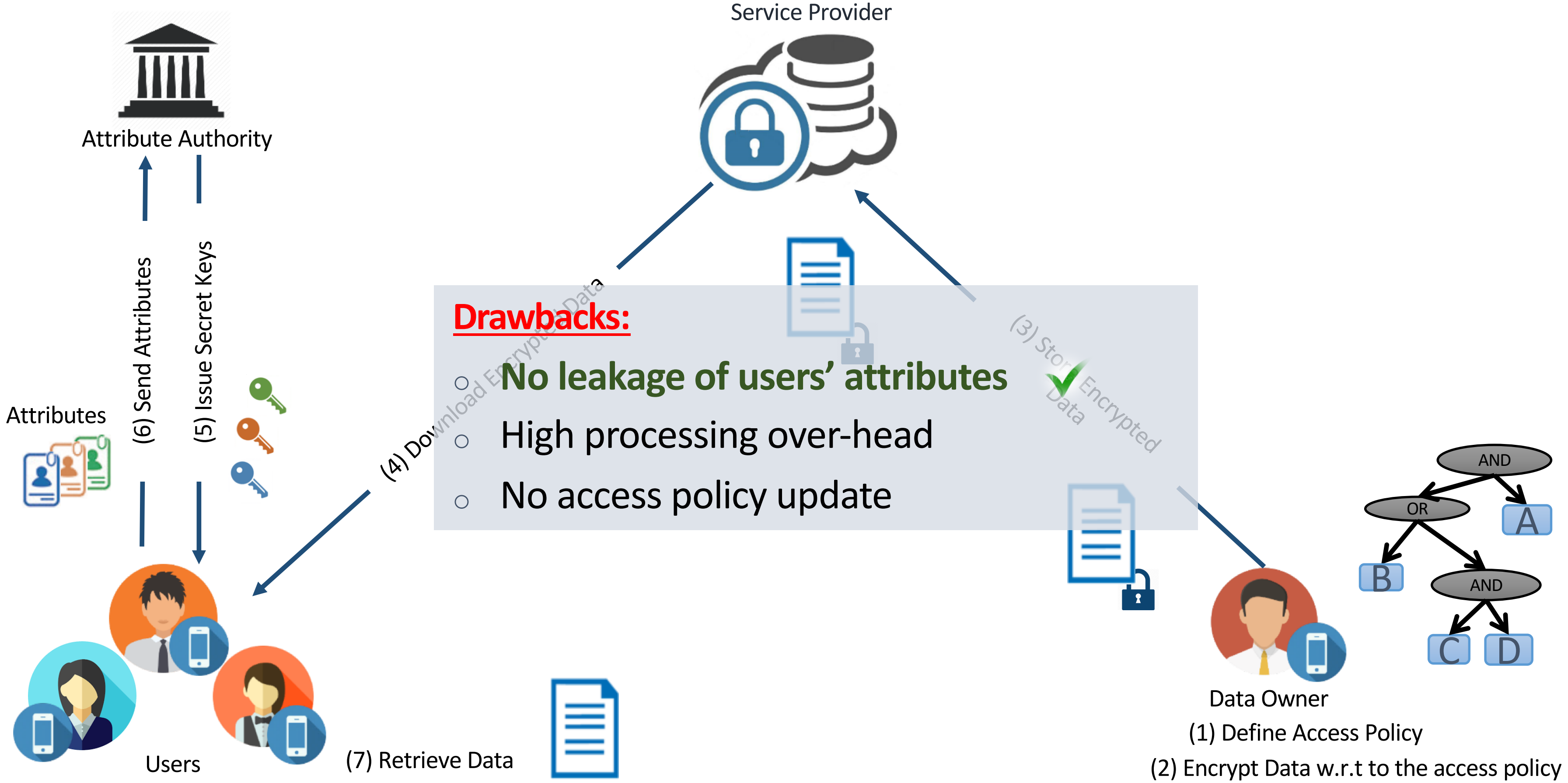
- Leakage of users’ attributes
- High processing over-head
- No access policy update

Attribute Based Encryption: Hidden Access Policy



- Belguith S, **Kaaniche N.,** Laurent, M, Jemai, A. , Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT, Computer Networks

Attribute Based Encryption

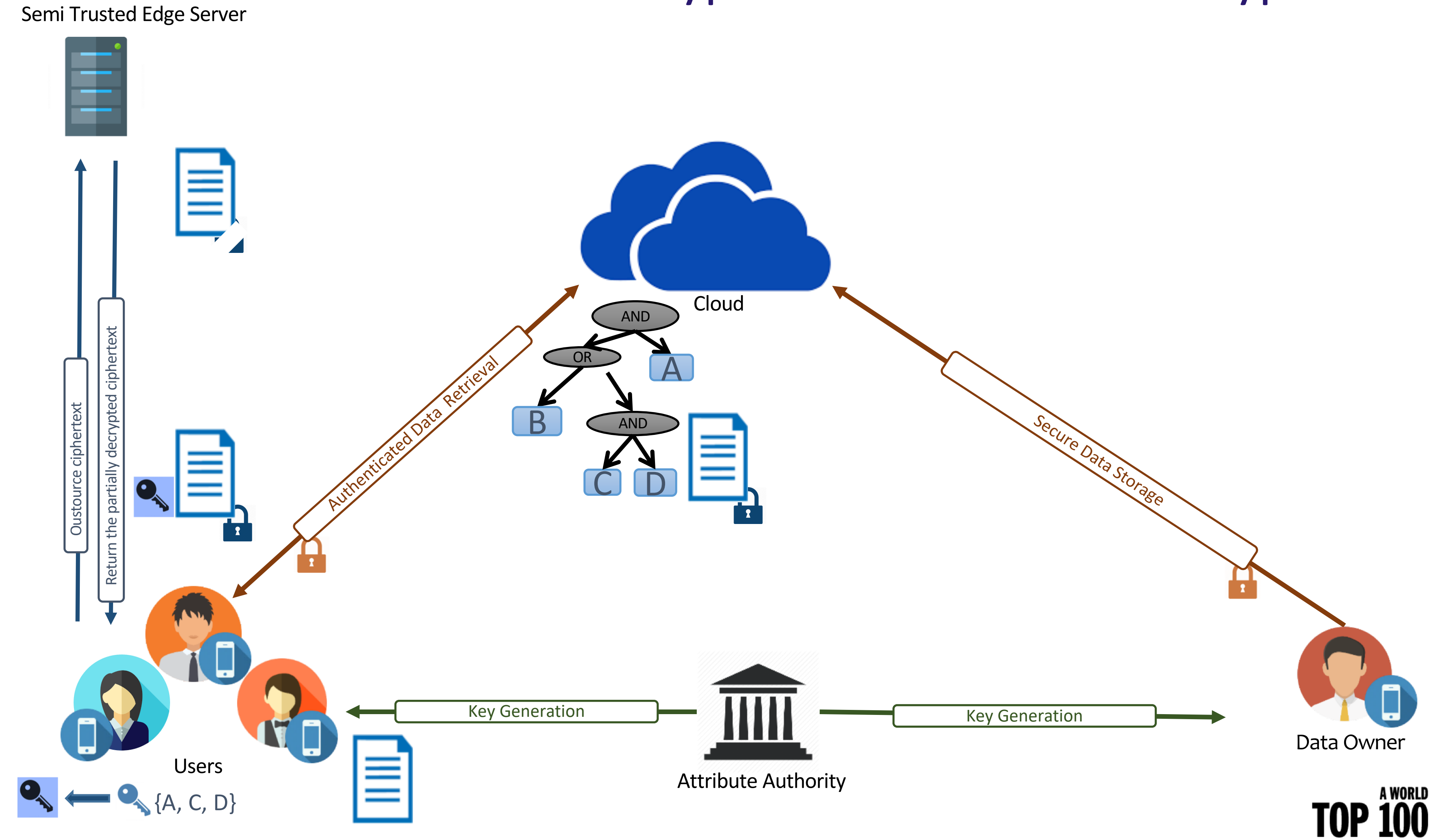


Drawbacks:

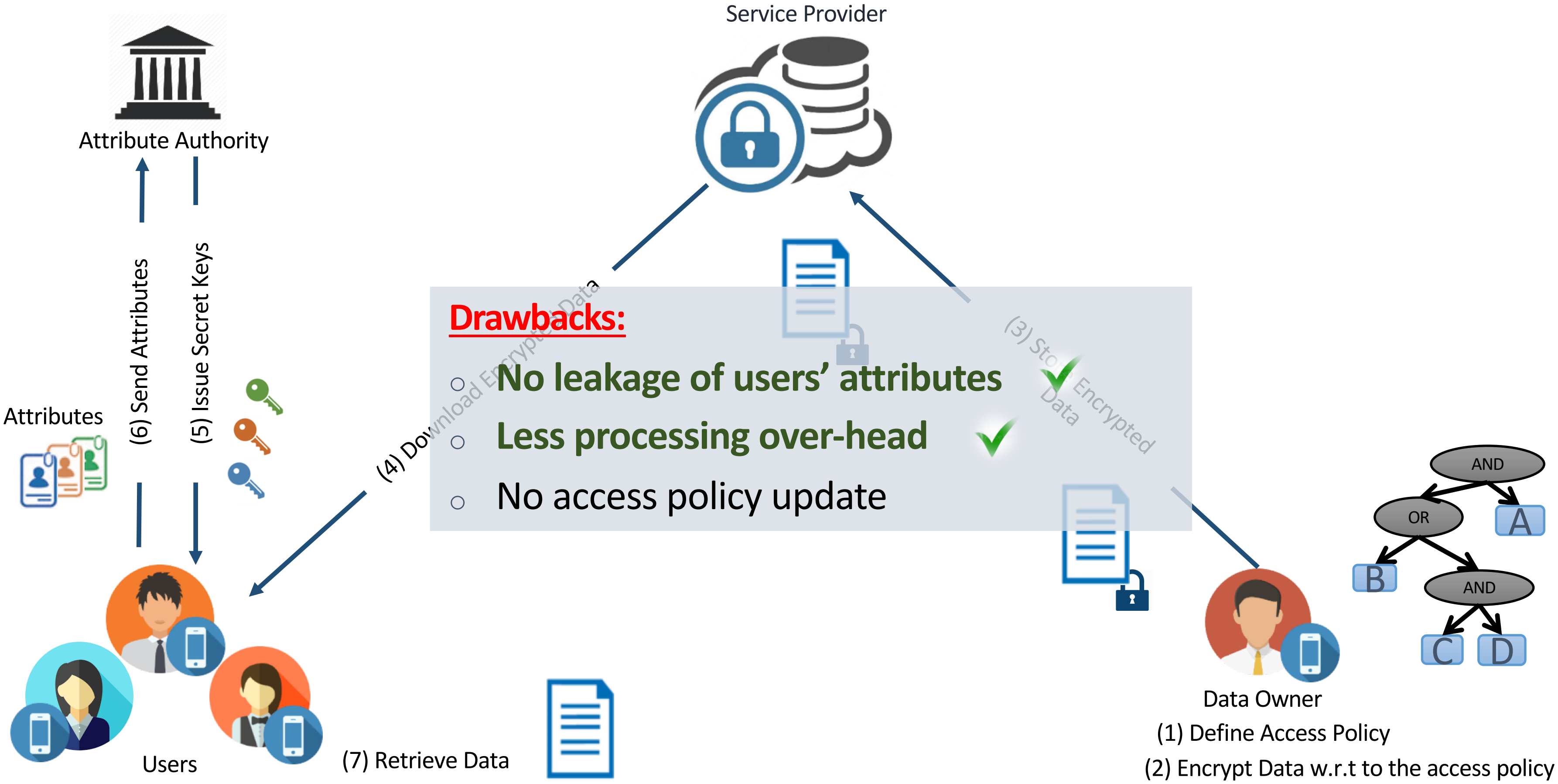
- ○ **No leakage of users' attributes** ✓
- ○ High processing over-head
- ○ No access policy update

- Belguith S, **Kaaniche N.,** Laurent, M, Jemai, A. , Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT, Computer Networks

Attribute Based Encryption: Outsourced Decryption



Attribute based Encryption

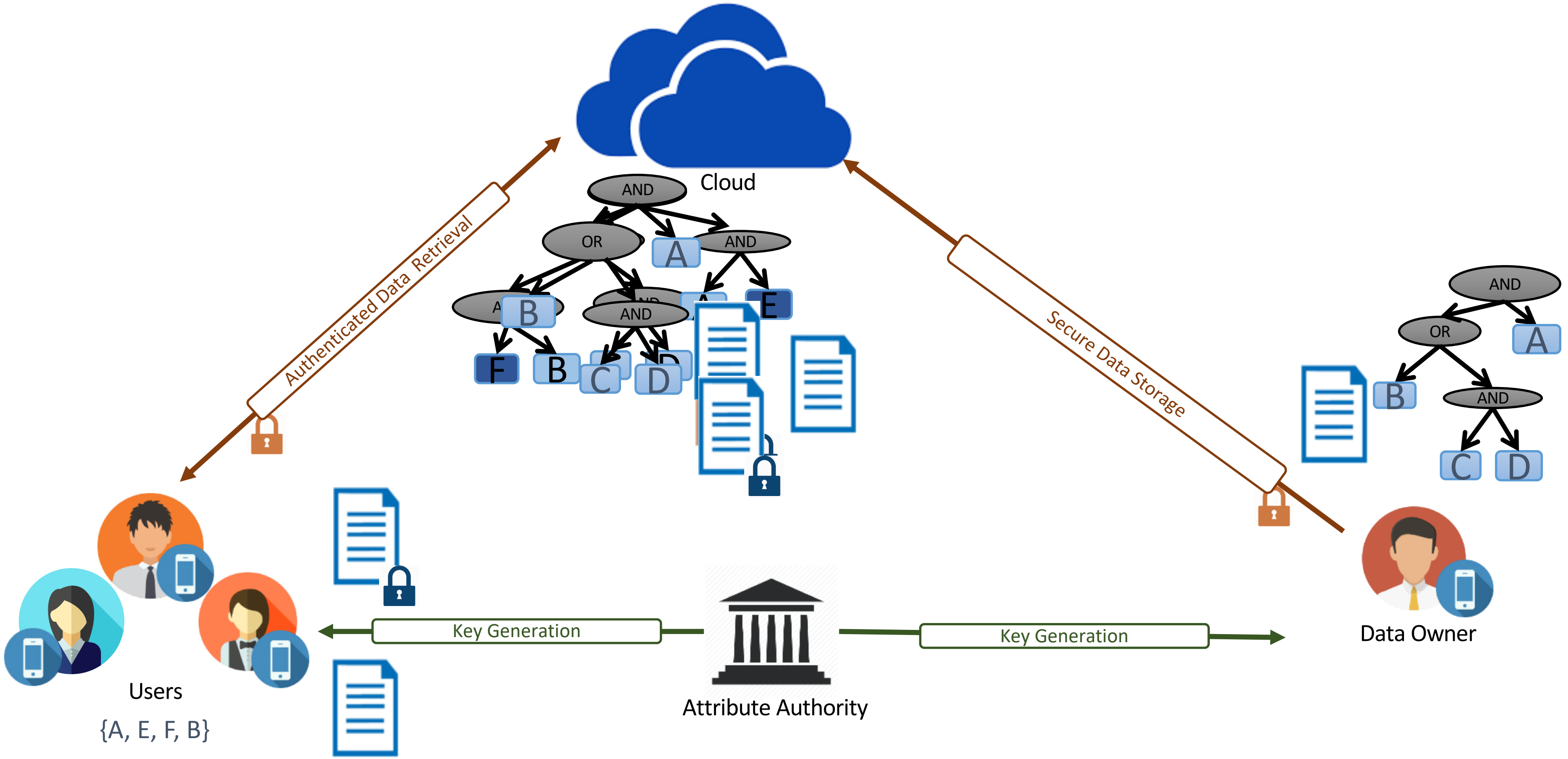


Drawbacks:

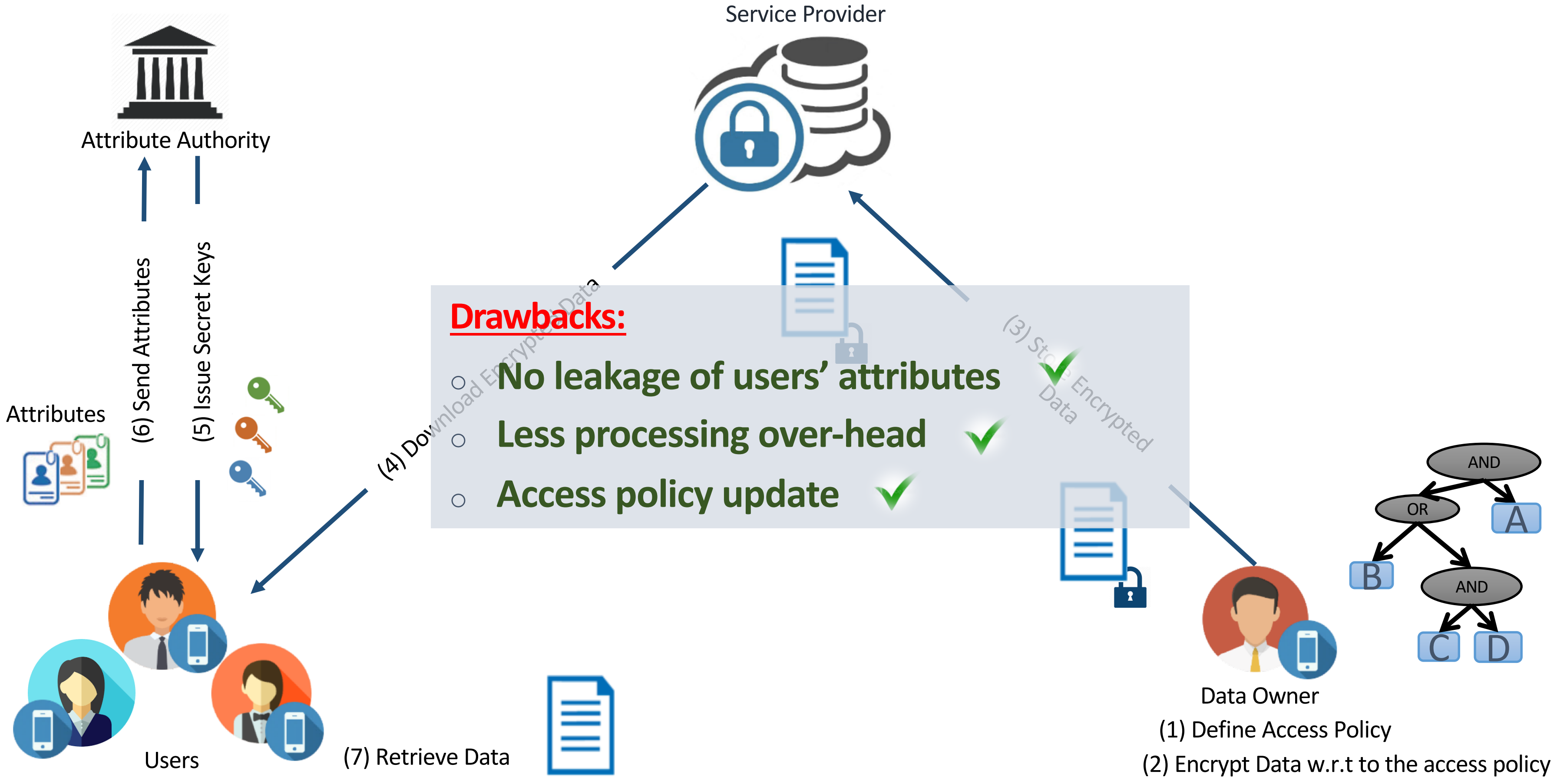
- ○ No leakage of users' attributes ✓
- ○ Less processing over-head ✓
- ○ No access policy update

- Belguith S, **Kaaniche N.,** Hammoudeh, M,, Dargahi, T. , PROUD: verifiable privacy-preserving outsourced attribute based signcryption supporting access policy update for cloud assisted IoT applications, Future Generation Computer Networks

Attribute-based Encryption : Access Policy Update



Attribute Based Encryption



Drawbacks:

○ No leakage of users' attributes ✓

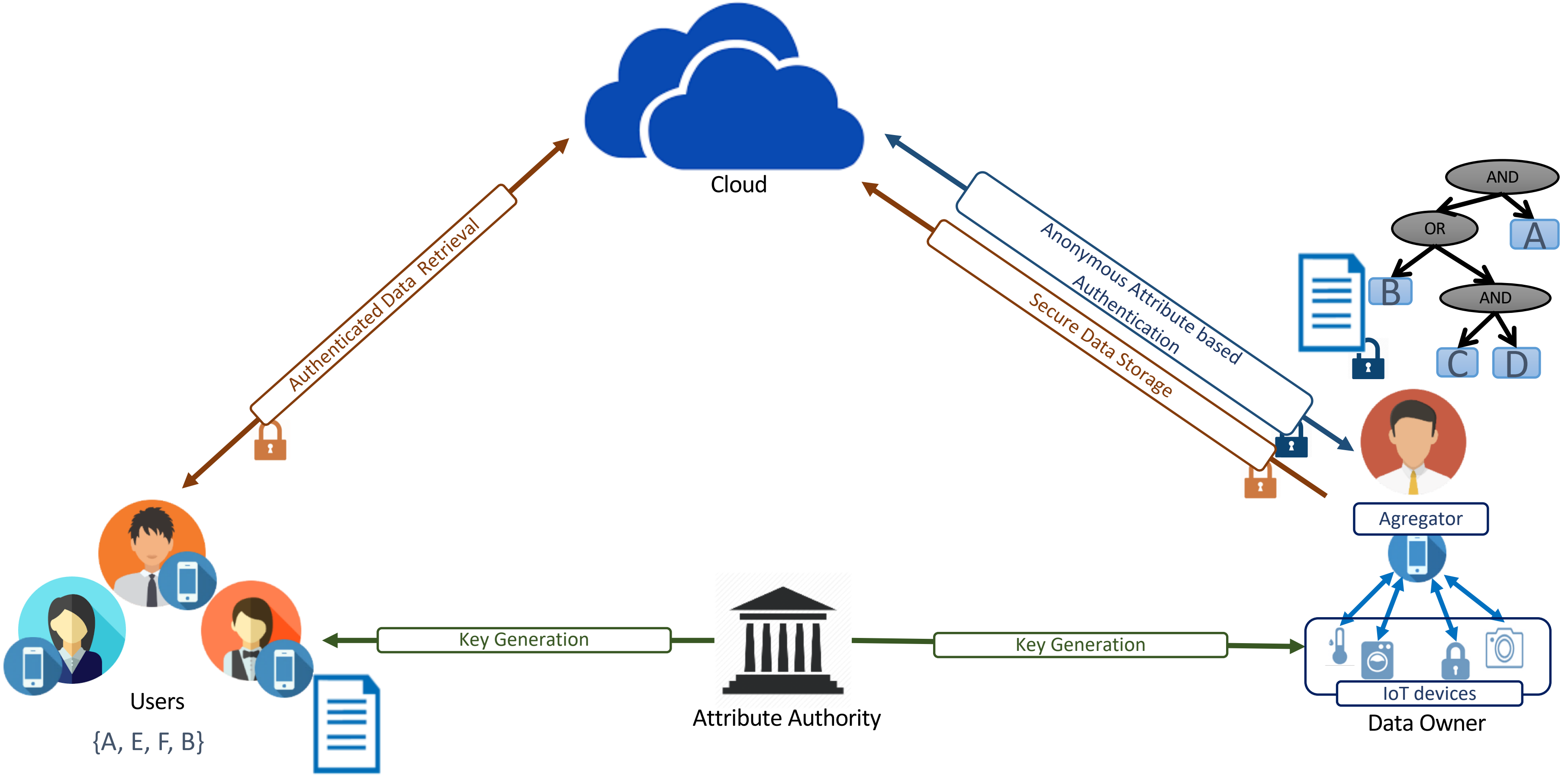
○ Less processing over-head ✓

○ Access policy update ✓

- Belguith S, **Kaaniche N.,** Hammoudeh, M,, Dargahi, T. , PROUD: verifiable privacy-preserving outsourced attribute based signcryption supporting access policy update for cloud assisted IoT applications, Future Generation Computer Networks

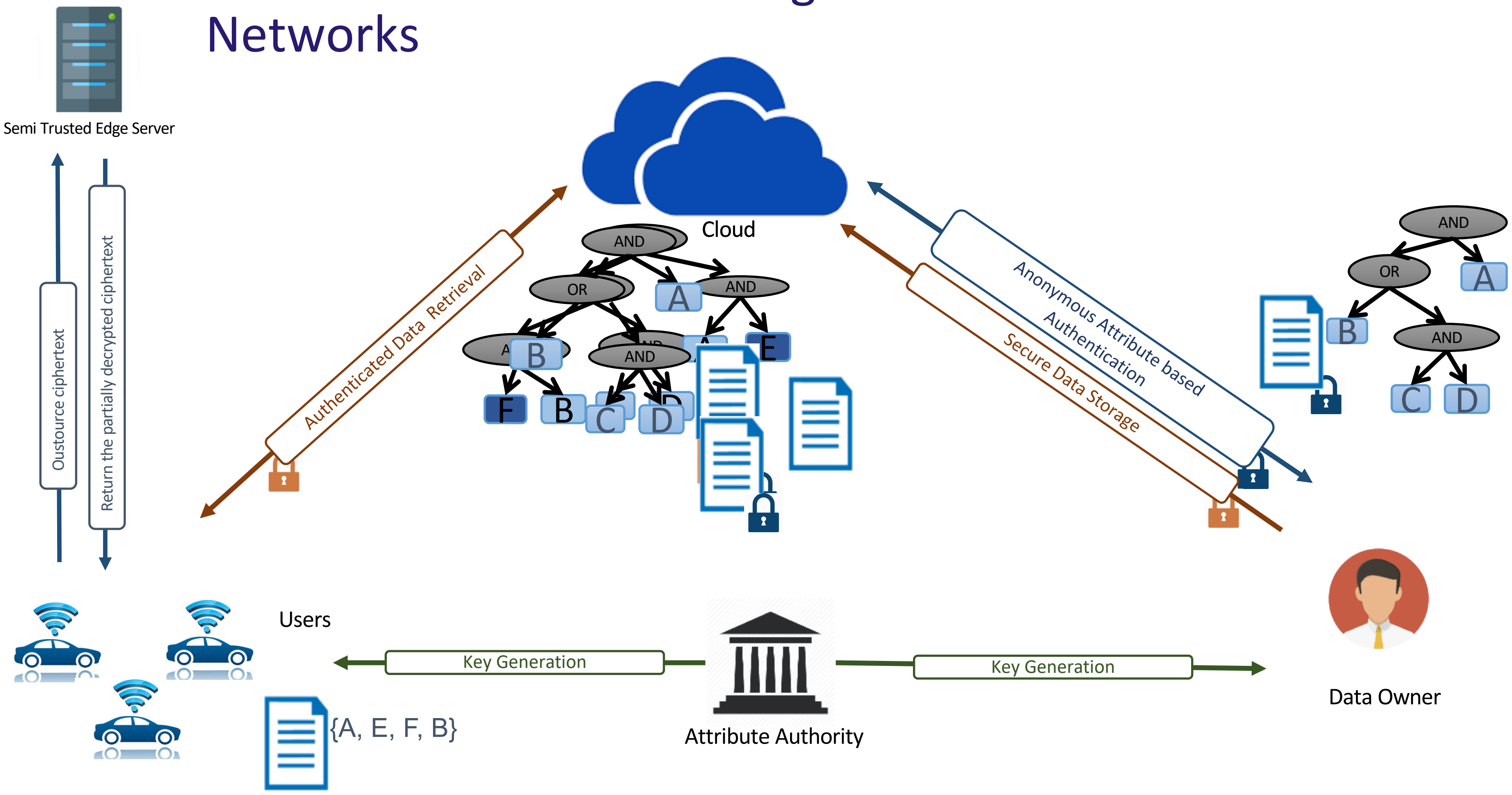
Encrypted Fine-grained Access: Real World Applications

Data Aggregation in Cloud-assisted IoTs: Smart Home Use Case



- Belguith S, **Kaaniche N.,** Mohamed, M, Russello G, T. , Coop-daab: Cooperative attribute based data aggregation for internet of things applications, OTM Conference

Authenticated Data sharing in Cloud-assisted Vehicular Networks



- Belguith S, **Kaaniche N.,** Hammoudeh, M, Dargahi, T. , PROUD: verifiable privacy-preserving outsourced attribute based signcryption supporting access policy update for cloud assisted IoT applications, Future Generation Computer Networks

Interdisciplinary Discussion & Research Directions

Technical Challenges

- Privacy preserving auditing tools
  - Transparency and auditing concerns have been addressed by a minority of works ➔ Need to address these requirements which have been emphasized by recent regulations.
  - *<u>Examples of recent works:</u> Intel-SGX provenance systems, informed consent for e-health applications, transactional privacy in blockchain-based systems*

- Privacy preserving data collection techniques
  - Massive collection of sensitive data, by AI-based systems, in emerging pervasive applications ➔ Need for privacy preserving data collection processes,
  - *<u>Research directions:</u> privacy-enhancing cryptographic methods (i.e., homomorphic encryption on encrypted users' data) to meet an agreement between privacy, efficiency and quality of experience.*

- Privacy sensitive processing for ubiquitous environments
  - Need for lightweight security/privacy solutions adapted to resource-constrained devices (mobile devices).
  - *<u>Examples of recent solutions:</u> Intel-SGX based solutions for pervasive/ubiquitous applications.*

Legal, Social & Economic Challenges

- Legal challenges
  - Several regulations and laws regarding data protection
  - *Research directions: translations laws/texts into efficient technical solutions, namely for users' consent collection and data transfers between several service providers*
- Social and economic challenges
  - User-experience is the main pillar to define the perimeter of private information and the utility over the adoptions of PETs
  - Several mediated cases: Kodak cameras, Google glasses, LG-TV..
  - Trade-off between protection strategies and economic activities
  - *Recent works: user empowerment approaches, the impact of data collection abuse practices on consumers' attitudes…*

Conclusions

Conclusions

- Several **user-centric privacy-preserving solutions** based on attribute-based cryptographic techniques have introduced, while pointing out their applications in distributed systems, i.e., clouds, cloud-assisted IoTs, e-assessment platforms …

- Several solutions at the server-side have been proposed, namely cooperative proofs of possession of outsourced data in cloud-of-clouds environments, authorized keyword search over outsourced encrypted data for multi-owner, multi-user settings, privacy preserving auditing systems, pseudonyms systems and privacy-enhancement for lifelogging personal assistants.

- Ongoing works and several collaborations are actually set-up with different universities and research labs: SRI International, USA; University of Salford, UK; University of NewCastle, AUS; and University of Auckland, NZ to investigate emerging privacy-preserving techniques.

Thank you for your attention!

Nesrine Kaaniche

n.kaaniche@sheffield.ac.uk