Crypto-Covid: Privacy challenges in BlockChain and Contact Tracing

Silvia Ghilezan[1, 2] Simona Kašterović[1] Tamara Stefanović[1]

[1]Faculty of Technical Sciences, University of Novi Sad
[2]Mathematical Institute SASA, Belgrade, Serbia

September 2022

Initial methods for privacy preservation

1. k-anonimity
2. l-diversity
3. t-closeness

k-anonimity

- An individual cannot be distinguished from at least k-1 other individuals whose information also appear in the record.

Advantages: prevents linking the released data to other information sources (background information).

Shortcomings: vulnerability to Homogeneity Attack and Background Knowledge Attack.

l-diversity

- Promotes intra-group heterogeneity of sensitive attributes by at least l different values.

Advantages: control the level of protection by modifying parameter l.

Shortcomings: Data utility loss, vulnerability to Skewness attack and Similarity attack.

t-closeness

- The distance between the distribution of a sensitive attribute in a class and the distribution of the attribute in the whole table is no more than a threshold t.

Advantages: it ensures attribute disclosure.

Shortcomings: it does not deal with identity disclosure and problem to find better distance measure between distributions.

Advanced lines of privacy research

1. Differential Privacy
2. Contextual Integrity
3. Inverse Privacy

Differential Privacy

- Incorporates random noise so that everything an adversary receives is noisy and imprecise.

- Tools
  - Static: Fuzz, DFuzz, Fuzzi, LightDP, Duet, HOARe2.
  - Dynamic: PINQ, SmartNoise, Diffprivlib, ϵktelo, DDuo.

Contextual Integrity

- Considers privacy from the perspective of information flow.
- Captures the idea that people act as individuals in certain roles in distinctive social context.

Inverse Privacy

- Inversely private data is the data that some party has access to but the individual itself does not.

Privacy and BlockChain

Privacy Protection of BlockChain (*ongoing research*)

- Identity privacy
  - mechanisms: mixing services, ring signature, and zero-knowledge proof.
- Transaction privacy
  - mechanisms: non-interactive zero-knowledge proof and homomorphic encryption.

Privacy-preserving Approaches Based on BlockChain (*ongoing survey*)

BubbleAntiCovid19 - *BAC19*[1]

Covid Pandemics

Goal: Slow down the spreading of SARS-CoV-2 virus.

Means: **Contact tracing**.

- Manual contact tracing does not give satisfactory results.
- Countries are developing DCT Apps - digital contact tracing applications.

[1] S. Ghilezan, Luigi Liquori, Bojan Marinković, S. Kašterović, Zoran Ognjanović, T. Stefanović Federating Digital Contact Tracing using Structured Overlay Networks, submitted

DCT Apps

They work on the principle of **automatic data exchange** with nearby devices.

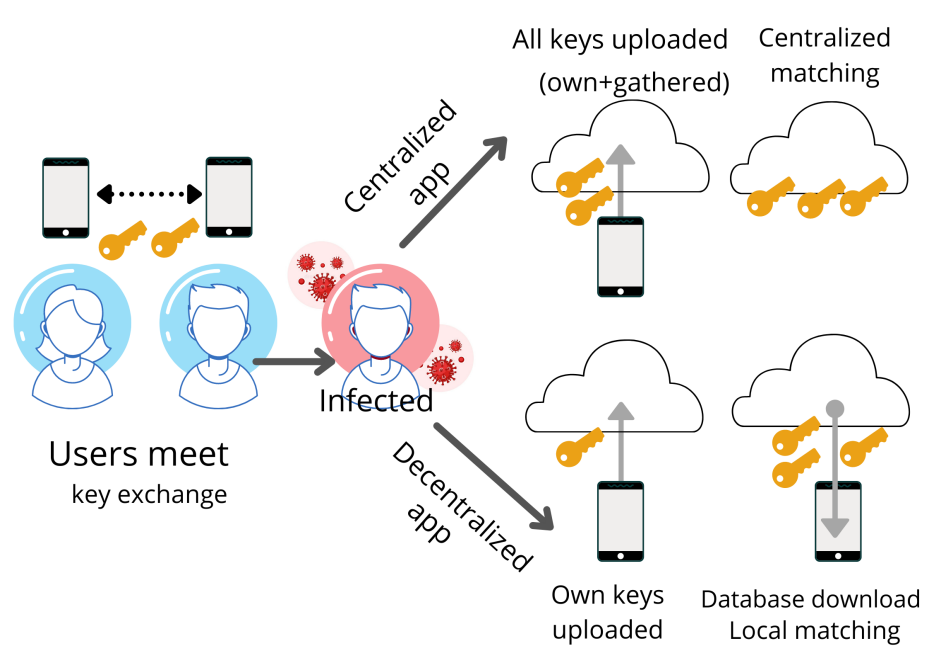

Figure: Digital Contact Tracing

DCT Apps Classification

- **System Architecture:** Centralized, Hybrid, Decentralized.
- **Contact Tracing Technology:** GPS, BlueTooth.

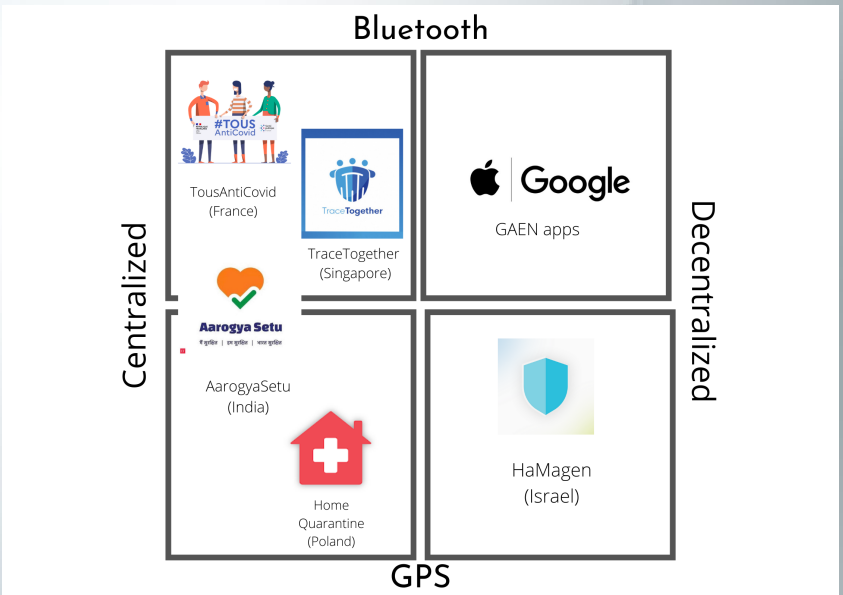

Figure: DCT Apps Classification

Problem with DCT Apps

Example: Alice is using centralized DCT System A, while Bob is using centralized DCT System B. Both of them are traveling together side by side with negative RT-PCR tests. However, Bob developed symptoms of Covid-19 after couple of days and was confirmed as positive.

NO INTEROPERABILITY!

Solution: BubbleAntiCovid19 - *BAC19*

The model is based on the well-known model of Structured Overlay Network protocols like **Chord** and **Synapse**.

The basic idea: all contacts of one person should be stored in one overlay network and the contact between persons could be seen as “the synapse nodes”.

BubbleAntiCovid19 Architecture

BAC19 consits of:

- **Gateways** for communication with original systems;
- **Networks for each person/device** of his/her first contacts (black circles);
- **Red network** for connecting all infected persons (red circle);
- **Amber network** for connecting all the first contacts of infected persons (orange circle).

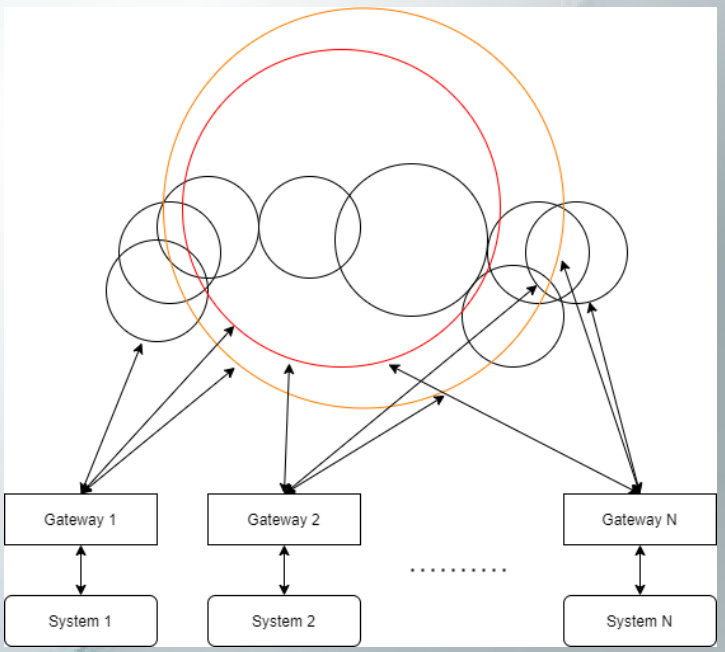

Figure: *BAC19* Architecture

Changes in the Search Procedure

```
FindSuccesor=
For Given key
  if member_of(key, id(Me), successor(id(Me))) then
    Respond With successor(id(Me))
  else
    Forward Query To Closes Predecessor From finger(id(Me))
  endif
```

Figure: Original Search Procedure in Chord

```
FindSuccessor =
For Given key
//successor(id(Me)) is responsible for key
if member_of(key, id(Me), successor(id(Me))) then
 | Respond With successor(id(Me))
else
 | //Me forwards query to its successor
 | Forward Query To successor(id(Me))
end
```

Figure: Search Procedure in *BAC19*

BAC19 **Simulation**

Purpose of the simulation: show that the retrieving procedure of *BAC19* is fully exhaustive.

We have analyzed the results for two types of simulations:

- fixed network size (number of nodes) and variable percentage of infected nodes;
- variable network size and fixed percentage of infected nodes.

Results: The success rate of the retrieving procedures is constantly 1, and it does not depend on the network size or the percentage of infected nodes.

BAC19 **Simulation**

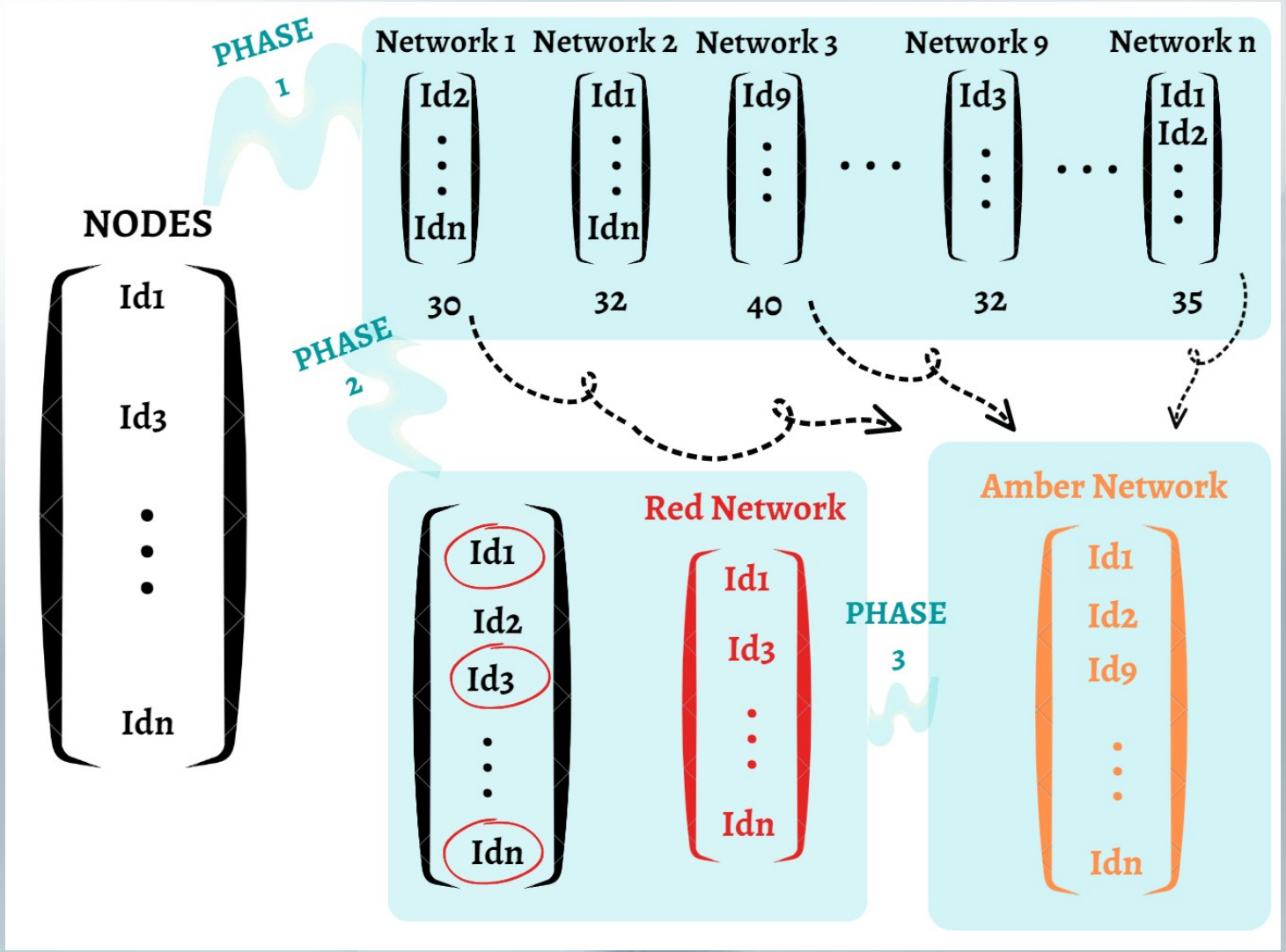

Figure: Simulation Ilustration

BubbleAntiCovid19 Advantages

- Interoperability - “Alice and Bob problem” solved.
- Does not store any personal information.
- Supports manual entry of contacts.
- No new highly complicated calculations.
- Simulation in Python.

References


S. Ghilezan, S. Kašterović, T. Stefanović
A report describing models for privacy management
AI4TrustBC WP1 deliverable D1.5.


S. Ghilezan, S. Kašterović, T. Stefanović
A report on comparative analysis of differential privacy, contextual privacy and inverse privacy
AI4TrustBC WP1 deliverable D1.6.


S. Ghilezan, S. Kašterović, T. Stefanović
An environment for privacy management based on trustworthy BC technology
AI4TrustBC WP1 deliverable D1.7.


S. Ghilezan, S. Kašterović, T. Stefanović
A report on the comparative analysis of existing tools for privacy management
AI4TrustBC WP1 deliverable D1.8.


S. Ghilezan, L. Liquori, B. Marinković, S. Kašterović, Z. Ognjanović, T. Stefanović
Federating Digital Contact Tracing using Structured Overlay Networks
(submitted).


Matematičke osnove privatnosti podataka
predmet na Master studijama Matematika u tehnici, od 2022. god.
Fakultet tehničkih nauka.


“Data is the pollution problem of the information age, and protecting privacy is the environmental challenge.”
Bruce Schneier