Secure Publication Subscription Framework for Reliable Information Dissemination

Shugo Yoshimura, Kouki Inoue, Dirceu Cavendish, Hiroshi Koide

Shugo Yoshimura
Graduate School of Information Science and Electrical Engineering, Kyushu University
yoshimura.shugo.822@s.kyushu-u.ac.jp

Shugo Yoshimura

Received B.E. and M.E. degrees from Kyushu University, Fukuoka, Japan in 2021, 2023 respectively.
His research interests include Java Virtual Machine, Moving Target Defense, Cybersecurity.

Table of Contents

- Introduction
- Secure Publication/subscription
  1. Components
  2. Reputation Algorithm
- Experiment
  1. Experimental methods
  2. Scenario 1 : 100% trusted publisher
  3. Scenario 2 : untrusted publisher
- Conclusion and Future work

Table of Contents

- Introduction
- Secure Publication/subscription
  1. Components
  2. Reputation Algorithm
- Experiment
  1. Experimental methods
  2. Scenario 1 : 100% trusted publisher
  3. Scenario 2 : untrusted publisher
- Conclusion and Future work

Introduction

- In recent years, Internet technologies have made great progress, with the population of Internet users increasing rapidly.
- Thanks to services like blogs and social media, anyone can get a large amount of information easily.

There is a lot of unreliable information on the internet.

(Fake News)

Introduction

Example of Fake News

April 14, 2016
Immediately after the Kumamoto earthquake, fake news spread on Twitter that a lion had escaped from the zoo.

It was actually a photo from South Africa.

(https://www.japantimes.co.jp/news/2017/03/23/national/kanagawa-man-tweeted-lion-scare-2016-kumamoto-quakes-avoids-charges/)

Images used for the fake news

Introduction

To solve this problem, we suggest a new framework for publishers and subscribers.

This framework allows providing the publisher's reputation score that increases or decreases as a result of the reliability of the published information.

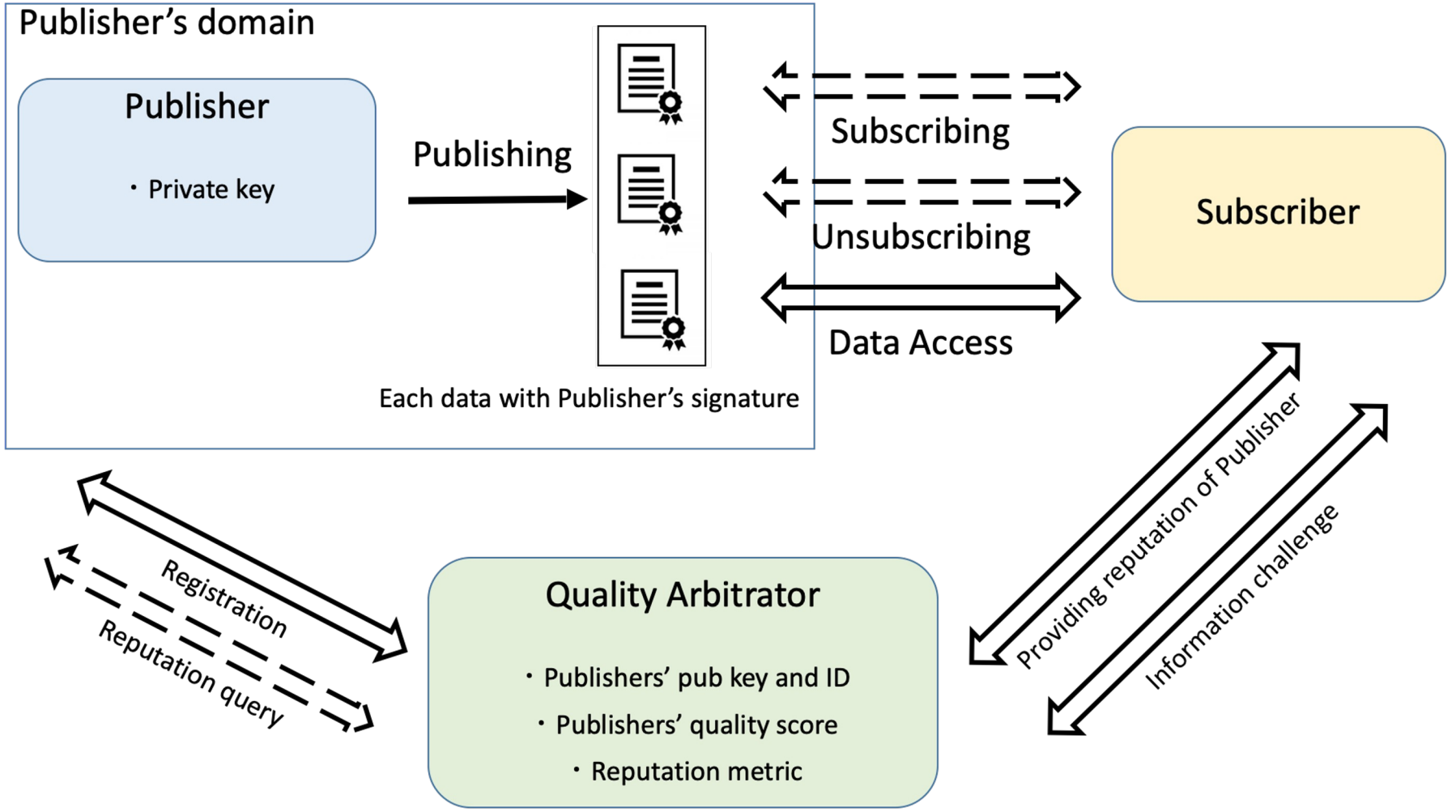
By using it, subscribers can easily confirm the reliability of information and distinguish between true or false information.

Table of Contents

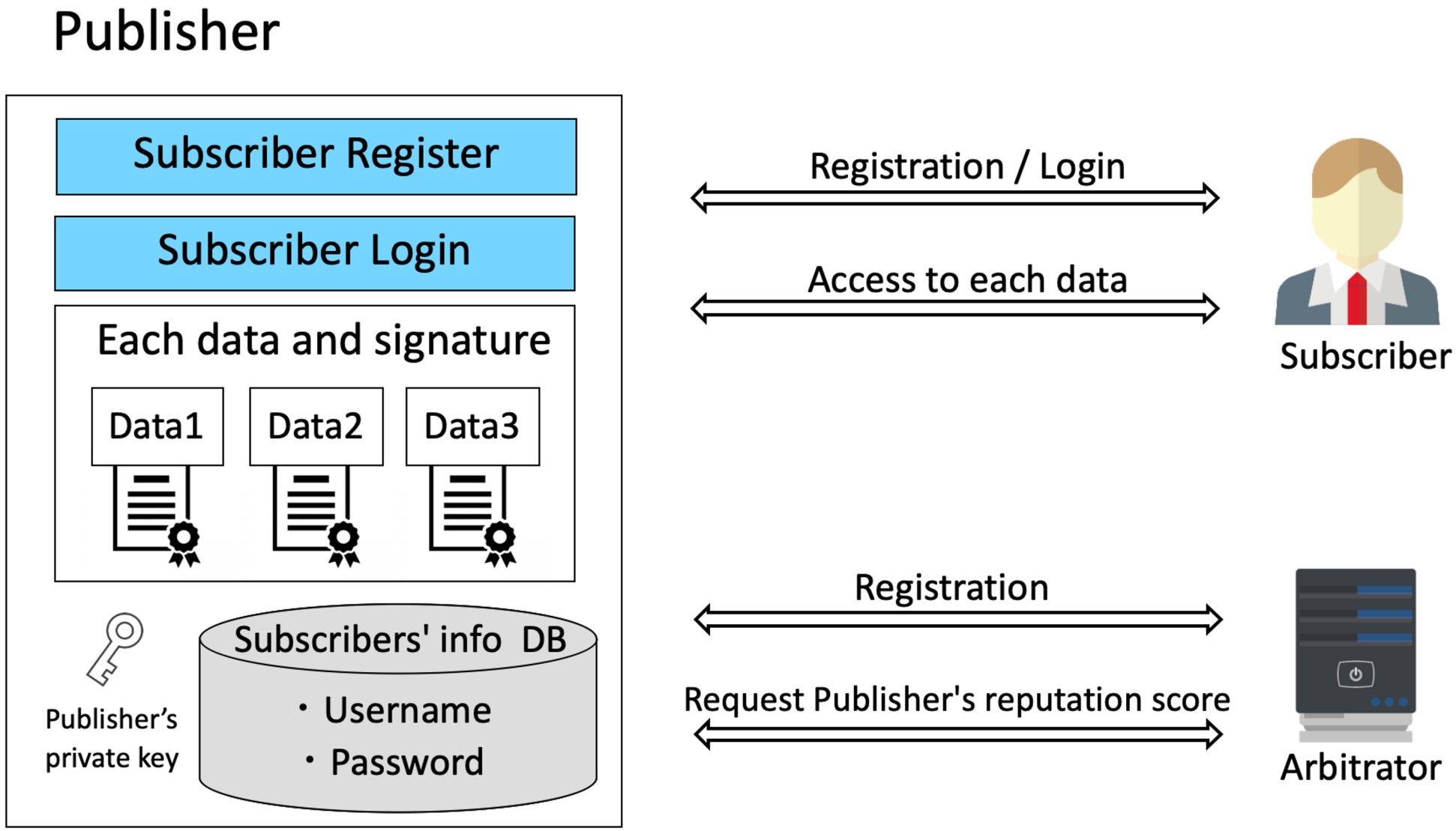
- Introduction
- Secure Publication/subscription
  1. Components
  2. Reputation Algorithm
- Experiment
  1. Experimental methods
  2. Scenario 1 : 100% trusted publisher
  3. Scenario 2 : untrusted publisher
- Conclusion and Future work

Secure Publication/Subscription

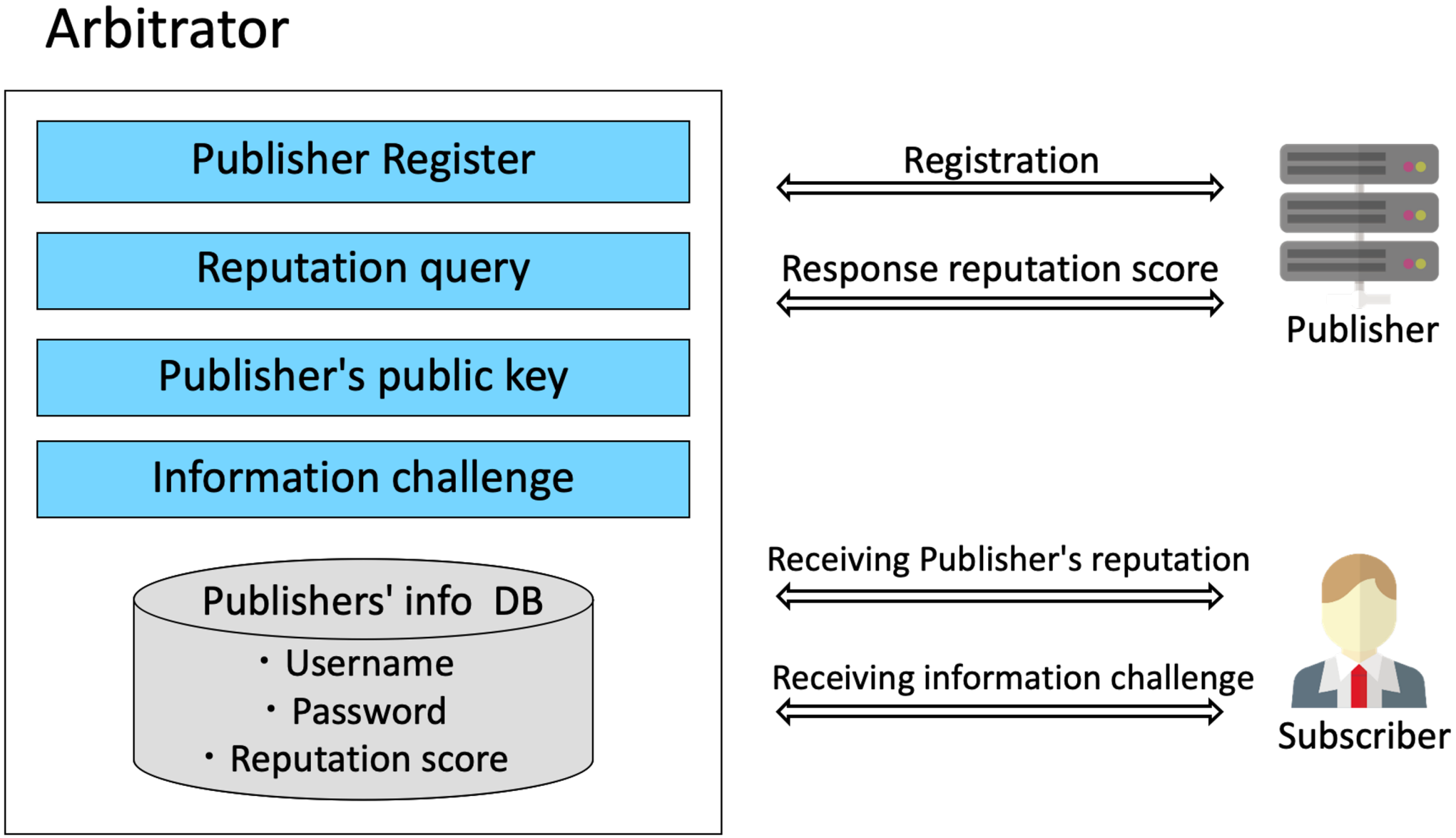
Overview of this framework



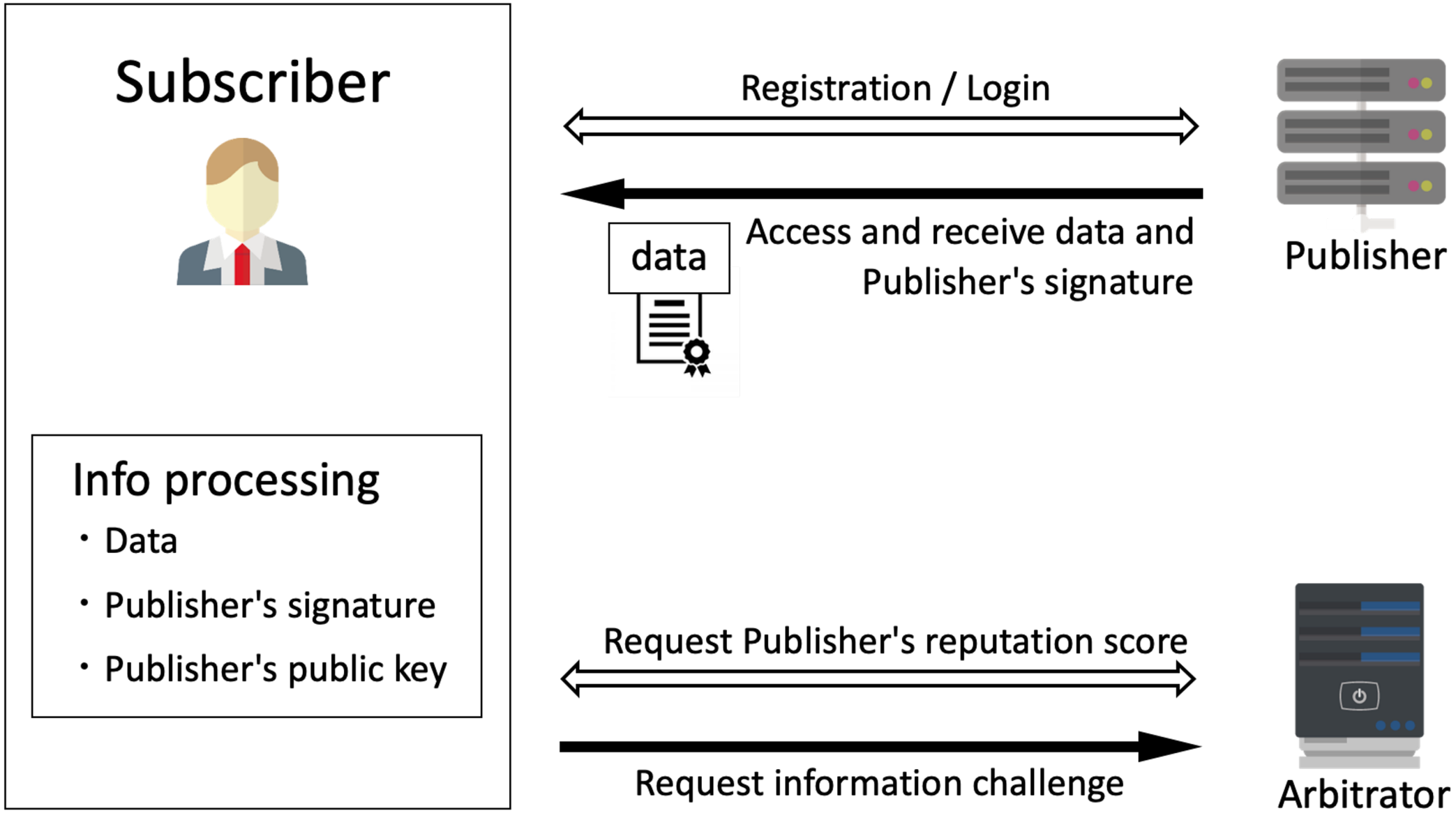
Secure Publication/Subscription



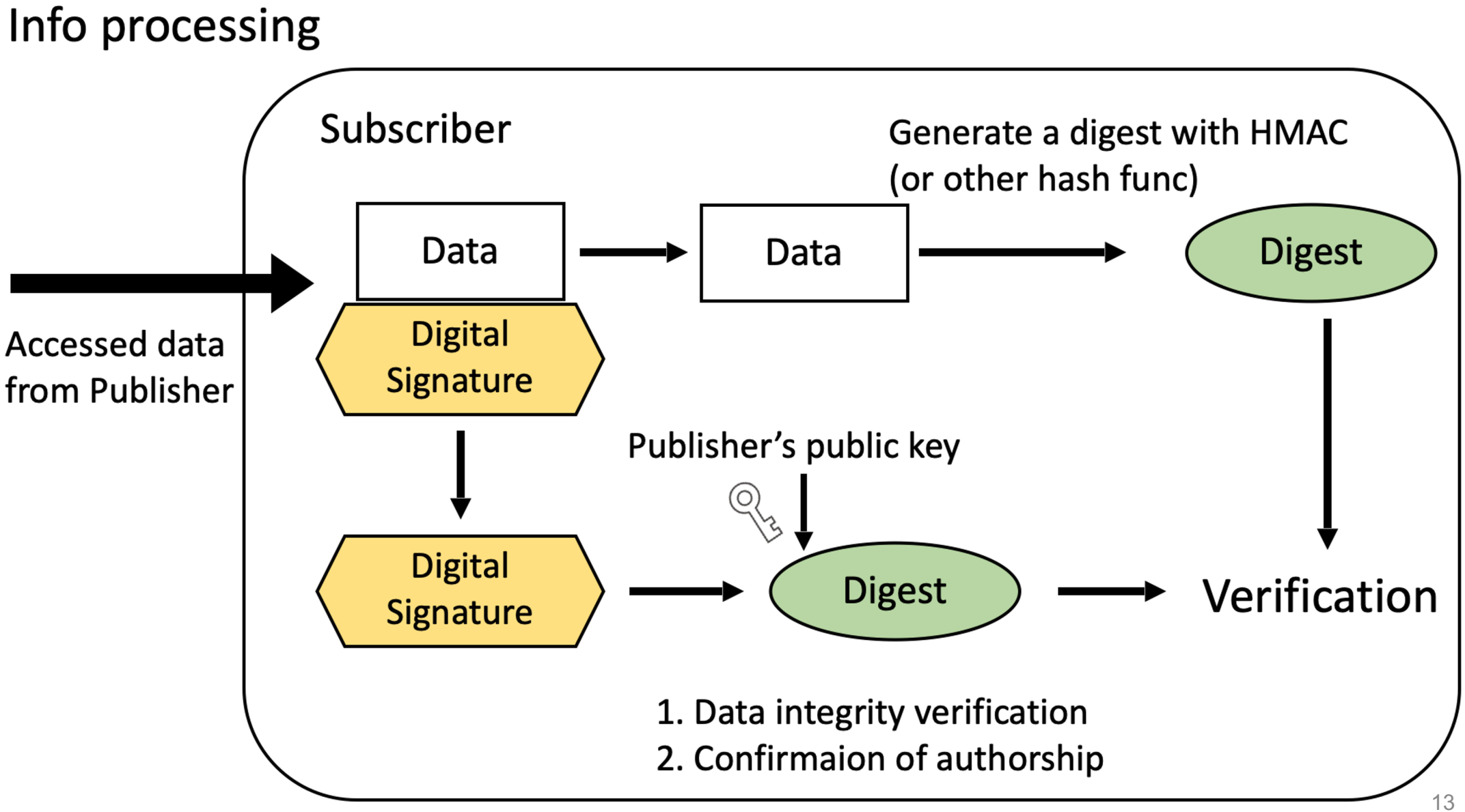
Secure Publication/Subscription



Secure Publication/Subscription



Secure Publication/Subscription



Secure Publication/Subscription

Information challenge

Subscriber

- Publisher's ID and data's digest
- The reason or evidence of error

Arbitrator

1. Verifying the error and truthfulness
2. Updating the reputation score of the Publisher

Table of Contents

- Introduction
- Secure Publication/subscription
  1. Components
  2. Reputation Algorithm
- Experiment
  1. Experimental methods
  2. Scenario 1 : 100% trusted publisher
  3. Scenario 2 : untrusted publisher
- Conclusion and Future work

Secure Publication/Subscription

Reputation Algorithm

We defined the reputation score of a publisher as

$$\frac{the\ number\ of\ correct\ data}{the\ number\ of\ all\ published\ data}$$

However, this number cannot be calculated correctly because it is difficult to determine the truth of the data with 100% probability.

Secure Publication/Subscription

Reputation Algorithm

Define variables as follows,

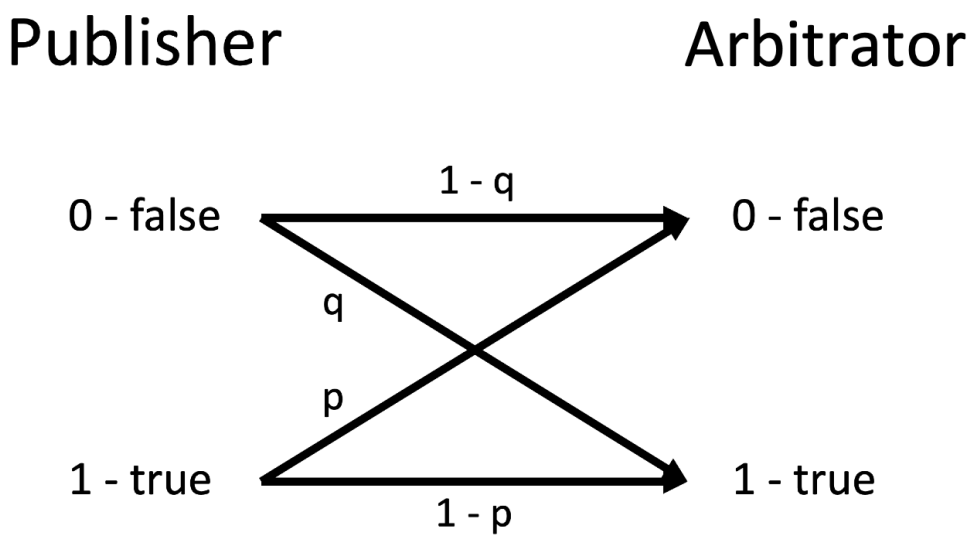
p = the probability that a true piece of data be recognized as false

q = the probability of a false piece of information be admitted as true

N = the number of all published data

true = the number of true data

false = the number of false data



Secure Publication/Subscription

Reputation Algorithm

We can estimate the reputation score like this;

True reputation = $\frac{true}{N}$.

Expected reputation score

= $\frac{false \times q + true \times (1 - p)}{N}$.

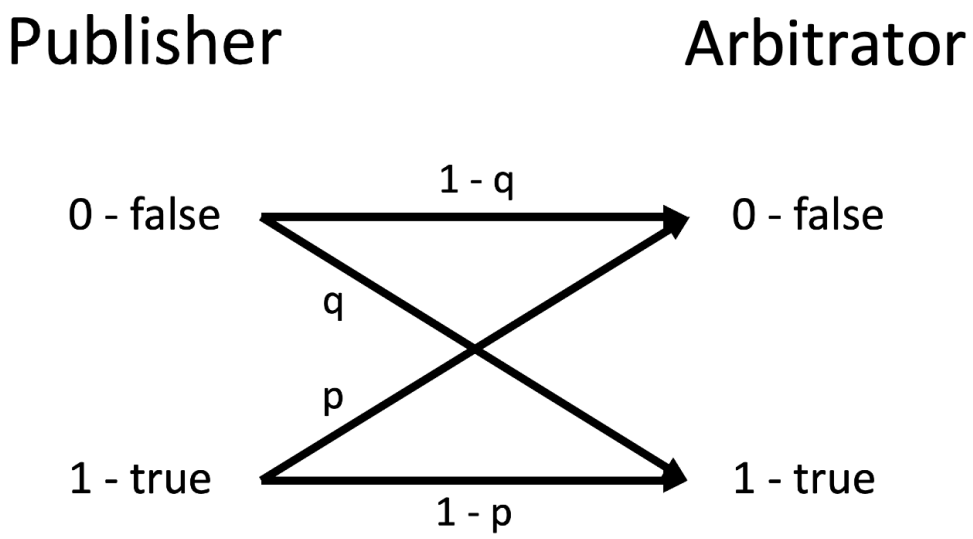


Table of Contents

- Introduction
- Secure Publication/subscription
  1. Components
  2. Reputation Algorithm
- Experiment
  1. Experimental methods
  2. Scenario 1 : 100% trusted publisher
  3. Scenario 2 : untrusted publisher
- Conclusion and Future work

Experiment

In Experiment section, we show the evolution of the Secure Publication Subscription Framework's evaluation estimator and evaluation scores.

- the values of the *p* and *q* are set to 0.3.
- using 1000 randomly generated true/false data.

We exemplify the secure publication/subscription model with the following two scenarios:

- scenario 1 : 100% trusted publisher
- scenario 2 : untrusted publisher

Experiment

The resulting graph shows 3 lines:

- Actual reputation score : the reputation score actually obtained after going through the Secure Publication Subscription Framework.
- Expected reputation score : the estimated value of the reputation score obtained from the actual truth of the data, p and q.
- True reputation : proportion of data that is actually true.

Table of Contents

- Introduction
- Secure Publication/subscription
  1. Components
  2. Reputation Algorithm
- Experiment
  1. Experimental methods
  2. Scenario 1 : 100% trusted publisher
  3. Scenario 2 : untrusted publisher
- Conclusion and Future work

Experiment

Scenario 1 : 100% trusted publisher

1. Subscribers register and login with the Publisher

2. Subscribers subscribe to data from the Publisher

3. Subscribers retrieve the data

4. Subscribers send a query about the Publisher’s reputation to the Arbitrator

Experiment

- True reputation is always 1.
  (In scenario 1, data is always true.)
- Expected reputation score is always 0.7.
  (There is a 30% probability of mistaking true data for false data.)

Actual reputation score	0.713
Expected reputation score	0.700
True reputation	1.000

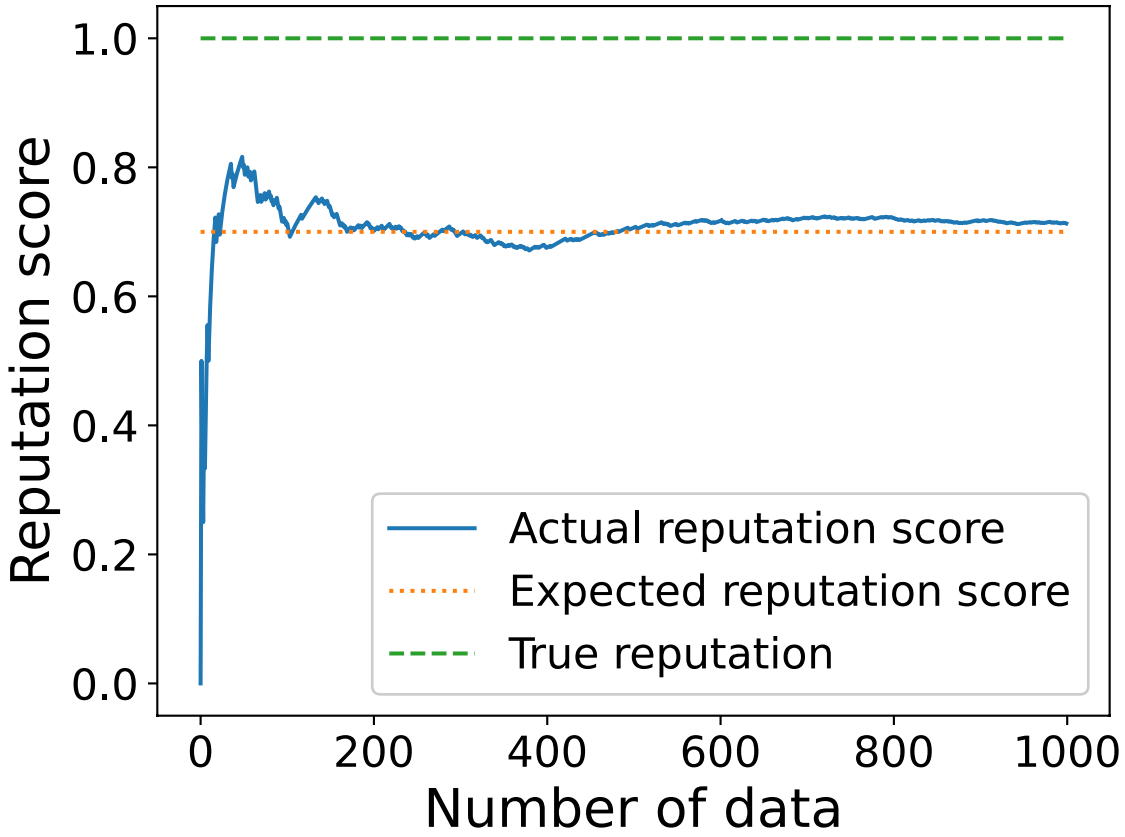


Table of Contents

- Introduction
- Secure Publication/subscription
  1. Components
  2. Reputation Algorithm
- Experiment
  1. Experimental methods
  2. Scenario 1 : 100% trusted publisher
  3. Scenario 2 : untrusted publisher
- Conclusion and Future work

Experiment

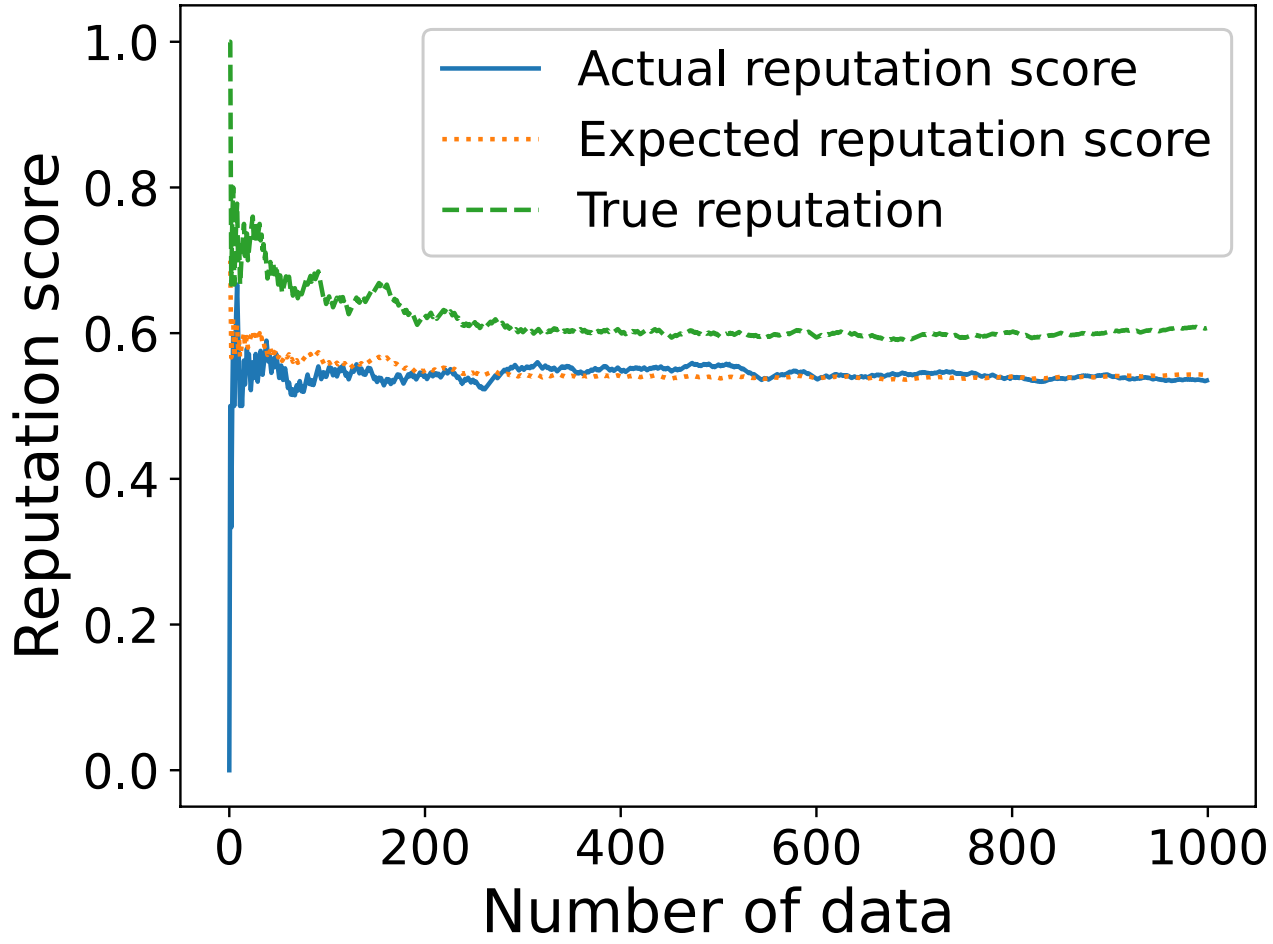
Scenario 2 : can be untrusted publisher

1. Subscribers register and login with the Publisher
2. Subscribers subscribe to data from the Publisher
3. Subscribers retrieve the data
4. Subscribers issue an information challenge
5. The Arbitrator decides the data as true/false, and updates the Publisher's reputation
6. Subscribers query the reputation of the Publisher from the Arbitrator

Experiment

Experimental results with 60% data accuracy.

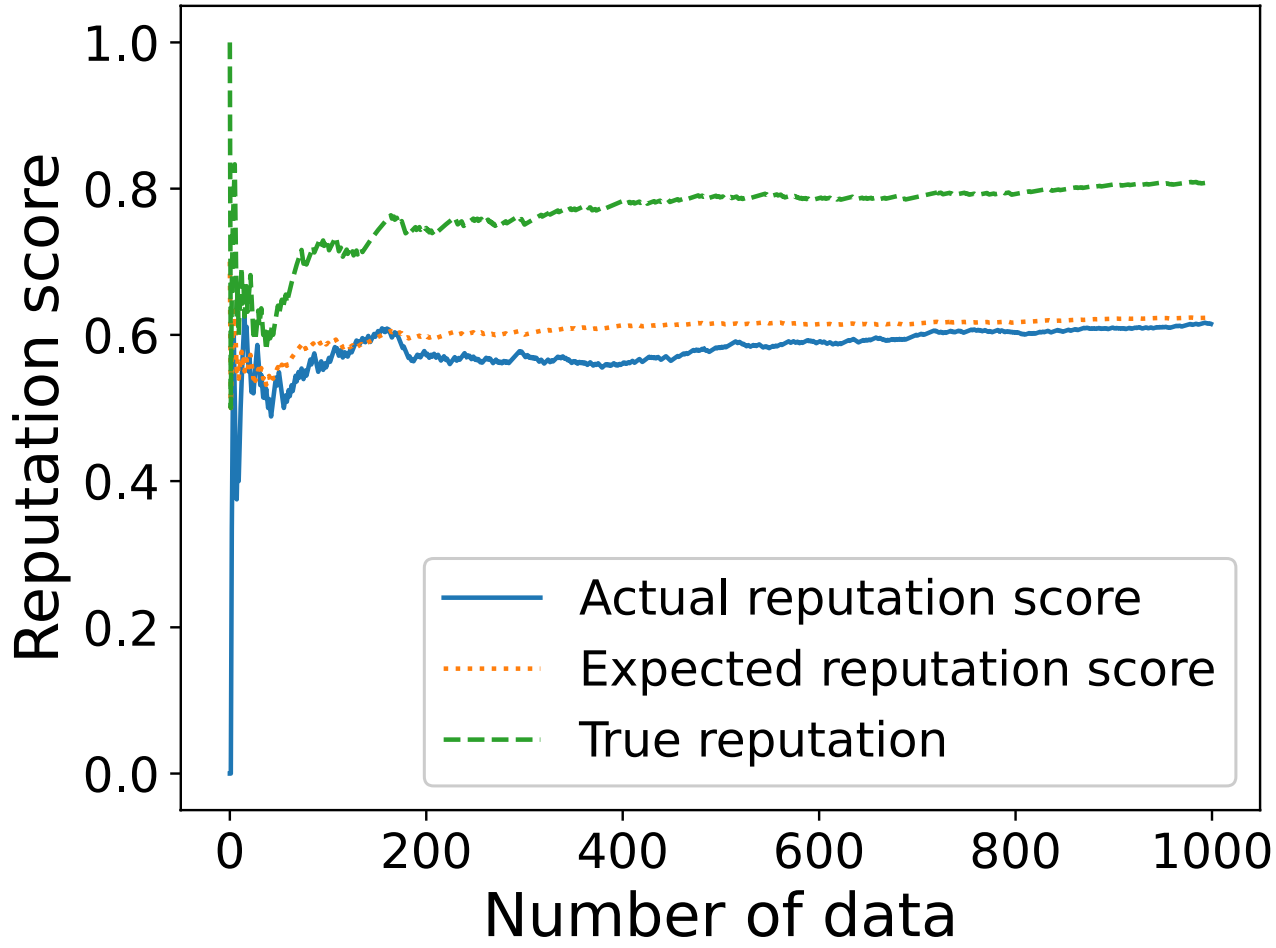
Actual reputation score	0.535
Expected reputation score	0.543
True reputation	0.607



Experiment

Experimental results with 80% data accuracy.

Actual reputation score	0.615
Expected reputation score	0.623
True reputation	0.808



Experiment

- The actual reputation score converges to the expected reputation score
  (with a sufficient number of data and a certain degree of accuracy in determining the truth of the data).

- If *p* and *q* are known, the Publisher's true reputation can be estimated from the actual score.

Table of Contents

- Introduction
- Secure Publication/subscription
  1. Components
  2. Reputation Algorithm
- Experiment
  1. Experimental methods
  2. Scenario 1 : 100% trusted publisher
  3. Scenario 2 : untrusted publisher
- Conclusion and Future work

Conclusion and Future work

In this study, we proposed a new framework that allows subscribers to check the accuracy of information based on the reliability of the publisher's historical data by checking the reputation score.

With fake news becoming a major problem, it is important to have a system that allows subscribers to easily verify the authenticity of information. As such a system, our framework can be one of the promising options.

Conclusion and Future work

As future research, integration of AI algorithms to automatically identify fake news with expert arbitrators is a promising path.

Although the accuracy of discriminating fake news has been a challenge for AI technologies, our expert framework can aid by using AI algorithms to improve false positives/negatives.