Санкт-Петербургский
государственный
университет
www.spbu.ru

CONTINUOUS AUTHENTICATION IN INTERNET OF THINGS SYSTEMS

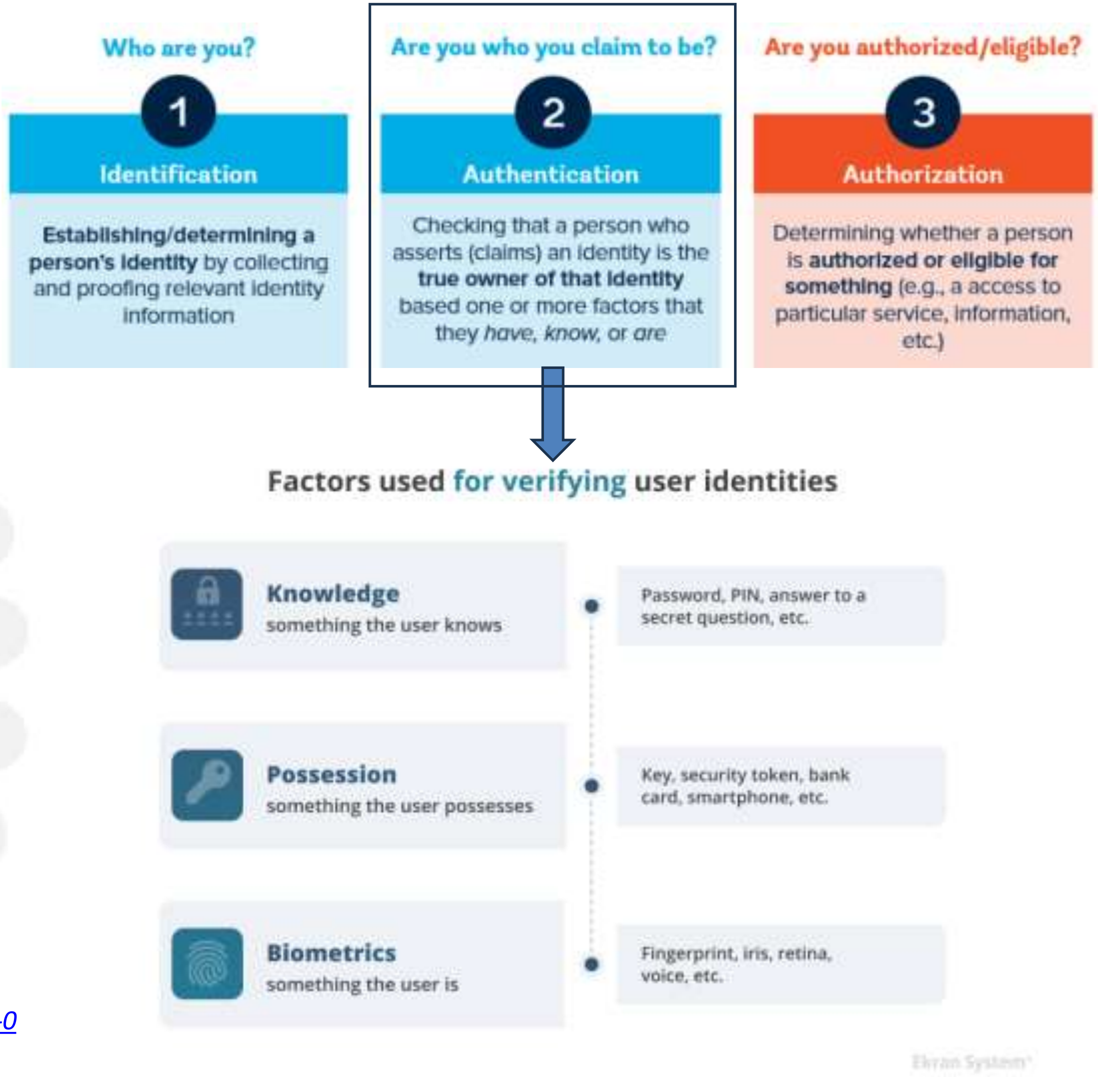
by Iurii Matiushin, Saint Petersburg State University
and Vladimir Korkhov, PhD, Saint Petersburg State University

Questions

- What are authentication and continuous authentication?
- What challenges does IoT offer in terms of authentication?
- What methods and approaches can fit the task of continuous authentication in IoT systems?
- What are the future research directions?

What is authentication?

- *Authentication* is a part of a larger system access pipeline.
- Arguably most important from the security standpoint.
- Authentication methods are numerous, usually classified by *factor*.



Who are you?

1 Identification

Establishing/determining a person's identity by collecting and proofing relevant identity information

Are you who you claim to be?

2 Authentication

Checking that a person who asserts (claims) an identity is the **true owner of that identity** based one or more factors that they *have*, *know*, or *are*

Are you authorized/eligible?

3 Authorization

Determining whether a person is **authorized or eligible for something** (e.g., a access to particular service, information, etc.)

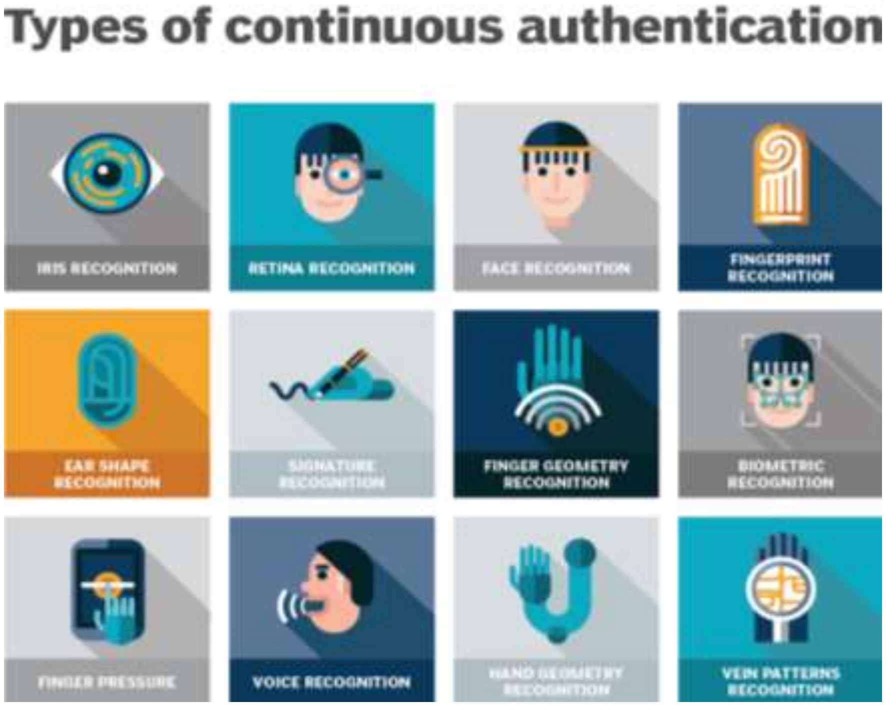
Factors used for verifying user identities

Knowledge something the user knows	Password, PIN, answer to a secret question, etc.
Possession something the user possesses	Key, security token, bank card, smartphone, etc.
Biometrics something the user is	Fingerprint, iris, retina, voice, etc.

1. https://id4d.worldbank.org/guide/id-101-basic-concepts-0
2. https://www.ekransystem.com/en/blog/continuous-authentication

Continuous authentication

- *Continuous authentication (CA)* is a new approach to user authentication.
- CA main idea – check the user’s authenticity *many times* throughout the session.
- CA is a part of a broader security paradigm called Zero-Trust Security Architecture.
- Multiple CA algorithms exist, many are based on *biometric methods* (inherence factor).



1. https://www.ekransystem.com/en/blog/continuous-authentication
2. https://www.techtarget.com/searchsecurity/definition/continuous-authentication

Common CA methods

Keystroke-based user recognition

How the user presses the keys, enters certain combinations, etc.

Face identification

Continuous observation of the user’s face via a camera

Mouse movement recognition

How the user moves the mouse, clicks the mouse buttons, etc.

Touch gesture-based authentication

How the user interacts with a touchscreen device, presses, swipes, performs multi-touch gestures, etc.

User behaviour-based authentication

The patterns of the user’s interactions with the system, possibly combined with other methods

IoT challenges for CA

Limited computational and storage resources

- Resource-intensive authentication methods might not be optimal

Limited energy and bandwidth

- Important to choose lightweight authentication methods and take network limitations into account

Lack of conventional user interface

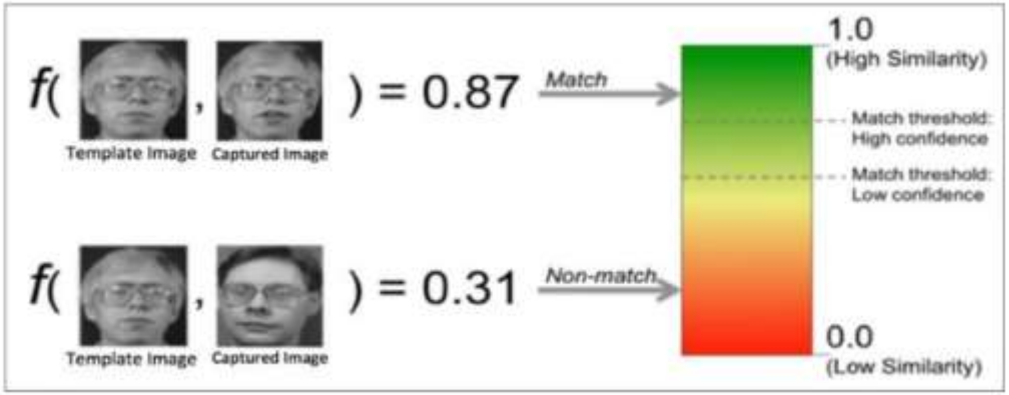
- Most common continuous authentication methods require input devices

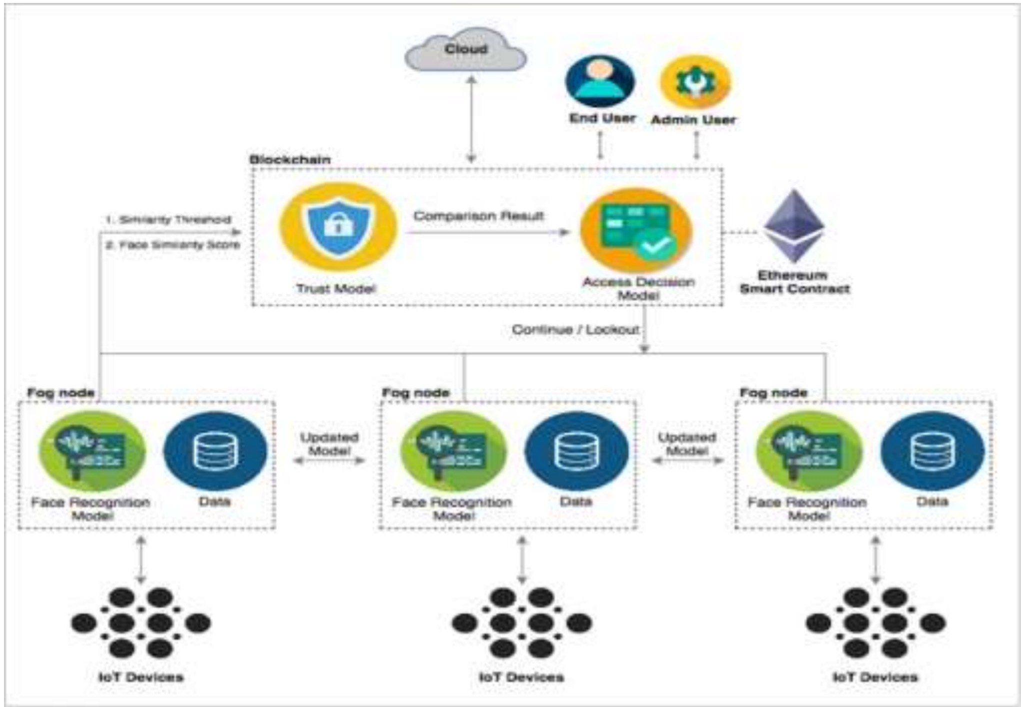
Existing approaches for IoT

- Continuous authentication methods that can be suitable for IoT environments include:
  - ➢ Face recognition and blockchain-based method
  - ➢ User gait-based method
  - ➢ Shared secret-based hybrid method
  - ➢ PUF (physical unclonable function)/device architecture-based hybrid method
  - ➢ Context-based hybrid method
- The following slides provide a brief overview of each method.

Blockchain-based method

- **Article:** *Continuous authentication architecture based on Blockchain for internet of things* by F. Hussain Al-Naji and R. Zagrouba.
- **Method:** *CAB-IoT* – a distributed and scalable blockchain-based CA method.
- *Face recognition* is used to detect intruders with the help of a trust module.
- A *distributed ledger* is used, based on Ethereum smart contract.





Gait-based method

- **Article:** *Continuous Authentication and Authorization for the Internet of Things* by M. Shahzad and M. P. Singh.
- **Method:** *WifiU* – dynamic biometric authentication based on gait.
- Based on changes in *CSI (channel state information)* and *RSS (received signal strength)* as a user is walking.
- The system learns the user's walk patterns and uses them for authentication.

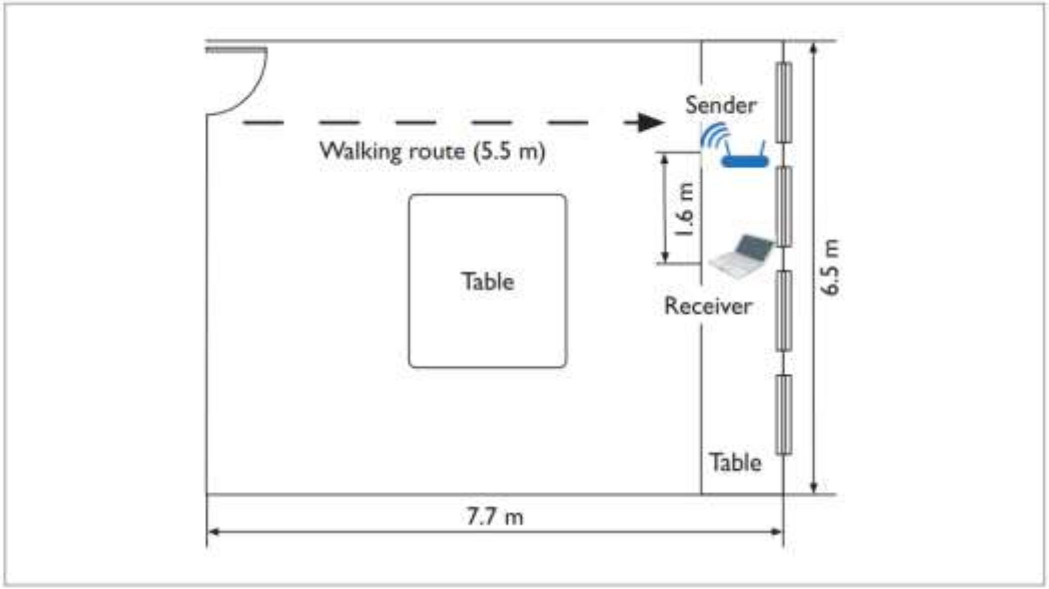
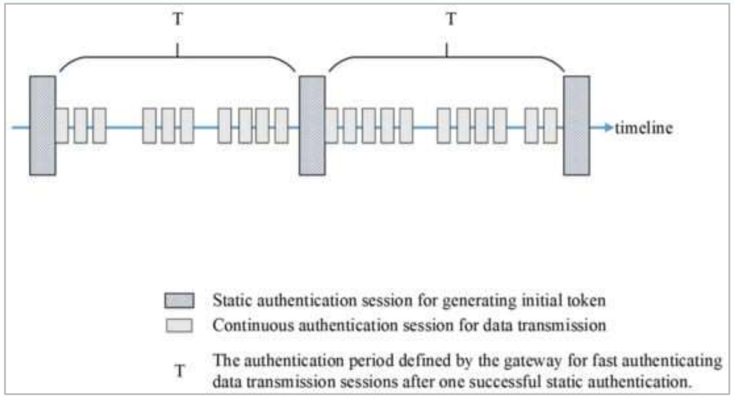


Figure 1. Data collection environment. Walking in an area of 50 square meters, we gathered more than 2,800 gait instances from 50 human subjects.

Shared secret method

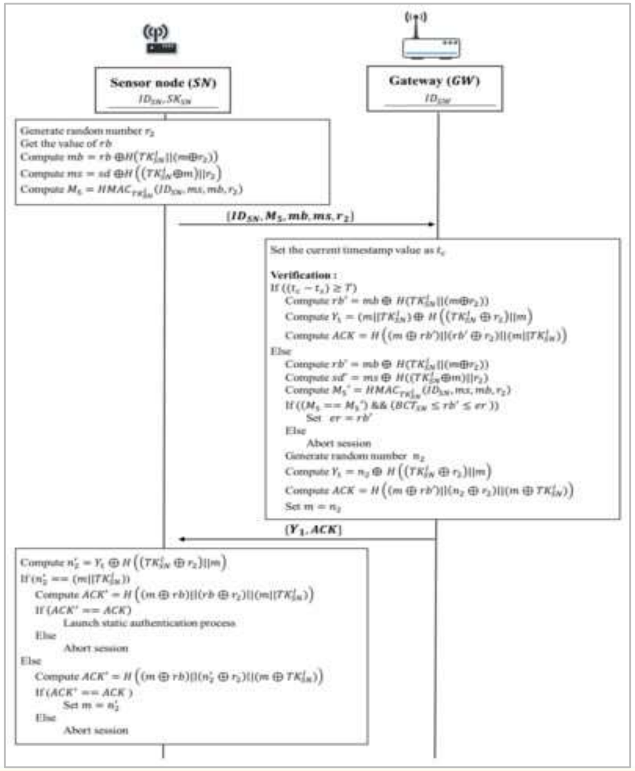
- **Article:** *A Lightweight Continuous Authentication Protocol for the Internet of Things* by Y.-H. Chuang et al.
- **Method:** *hybrid* static and continuous device authentication protocol.
- First, the device and the gateway are *initialized*, sharing important information, including a shared secret.
- During the *static* authentication phase, the device authenticates via cryptography and sends its data to the gateway.
- During the *continuous* authentication phase, the gateway uses the message's timestamp and the device's battery charge.



▨ Static authentication session for generating initial token

□ Continuous authentication session for data transmission

T The authentication period defined by the gateway for fast authenticating data transmission sessions after one successful static authentication.



```
Generate random number $r_2$
Get the value of $rb$
Compute $mb = rb \oplus H(TK_{SN}^{i} || (m \oplus r_2))$
Compute $ms = sd \oplus H((TK_{SN}^{i} \oplus m) || r_2)$
Compute $M_5 = HMAC_{TK_{SN}^{i}}(ID_{SN}, ms, mb, r_2)$
```

$\{ID_{SN}, M_5, mb, ms, r_2\}$

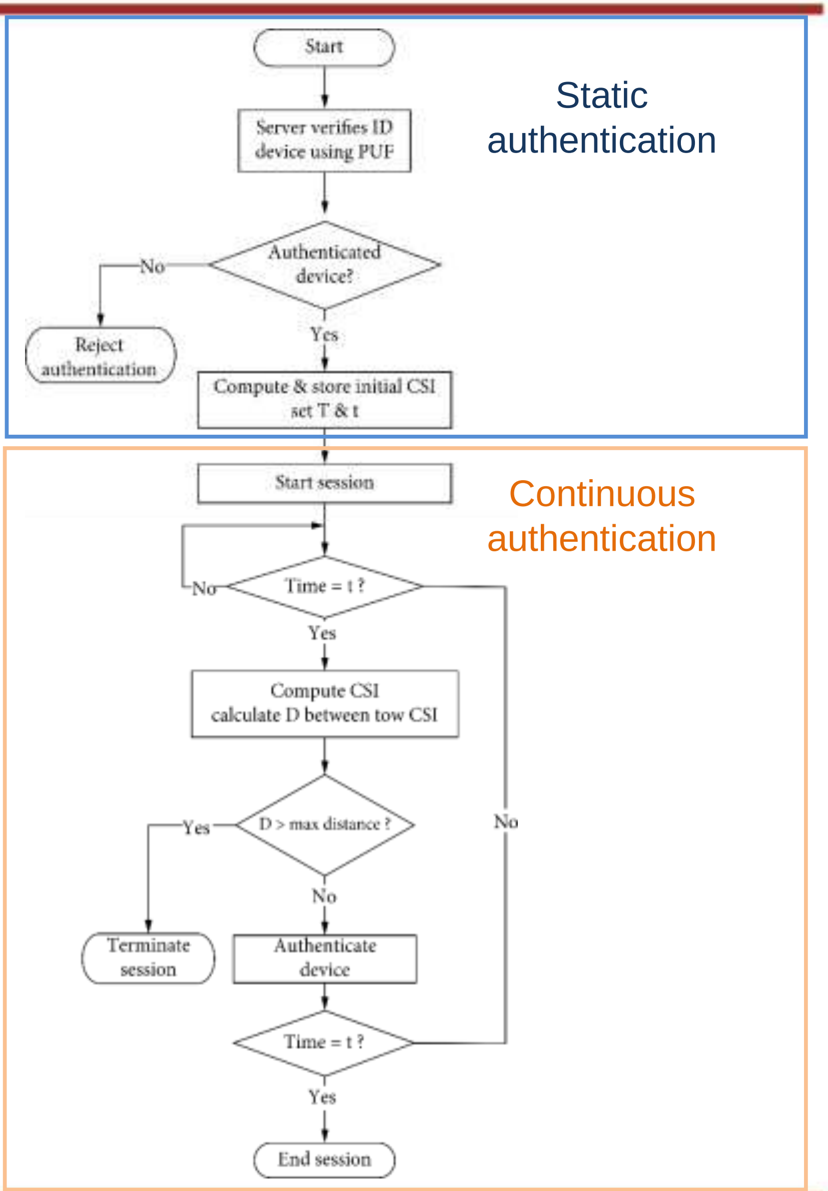
```
Set the current timestamp value as $t_c$

Verification :
If $((t_c - t_s) \geq T)$
    Compute $rb' = mb \oplus H(TK_{SN}^{i} || (m \oplus r_2))$
    Compute $Y_1 = (m || TK_{SN}^{i}) \oplus H((TK_{SN}^{i} \oplus r_2) || m)$
    Compute $ACK = H((m \oplus rb') || (rb' \oplus r_2) || (m || TK_{SN}^{i}))$
Else
    Compute $rb' = mb \oplus H(TK_{SN}^{i} || (m \oplus r_2))$
    Compute $sd' = ms \oplus H((TK_{SN}^{i} \oplus m) || r_2)$
    Compute $M_5' = HMAC_{TK_{SN}^{i}}(ID_{SN}, ms, mb, r_2)$
    If $((M_5 == M_5') \&\& (BCT_{SN} \leq rb' \leq er))$
        Set $er = rb'$
    Else
        Abort session
    Generate random number $n_2$
    Compute $Y_1 = n_2 \oplus H((TK_{SN}^{i} \oplus r_2) || m)$
    Compute $ACK = H((m \oplus rb') || (n_2 \oplus r_2) || (m \oplus TK_{SN}^{i}))$
    Set $m = n_2$
```

$\{Y_1, ACK\}$

```
Compute $n_2' = Y_1 \oplus H((TK_{SN}^{i} \oplus r_2) || m)$
If $(n_2' == (m || TK_{SN}^{i}))$
    Compute $ACK' = H((m \oplus rb) || (rb \oplus r_2) || (m || TK_{SN}^{i}))$
    If $(ACK' == ACK)$
        Launch static authentication process
    Else
        Abort session
Else
    Compute $ACK' = H((m \oplus rb) || (n_2' \oplus r_2) || (m \oplus TK_{SN}^{i}))$
    If $(ACK' == ACK)$
        Set $m = n_2'$
    Else
        Abort session
```

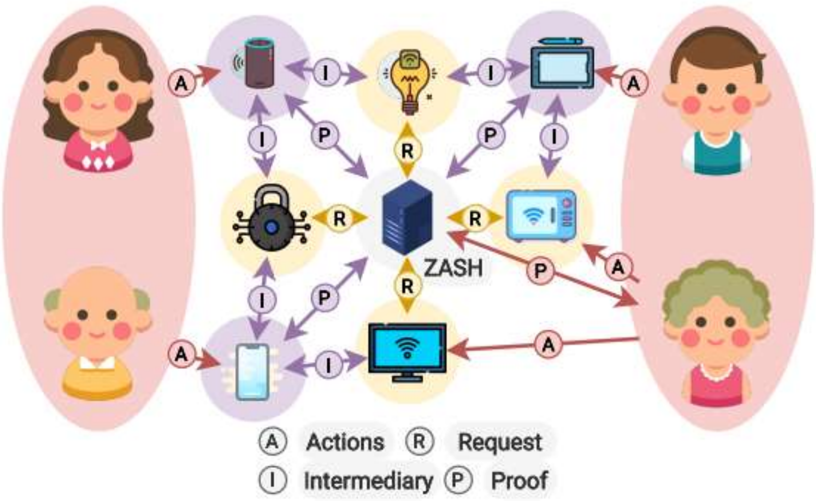
PUF-based method

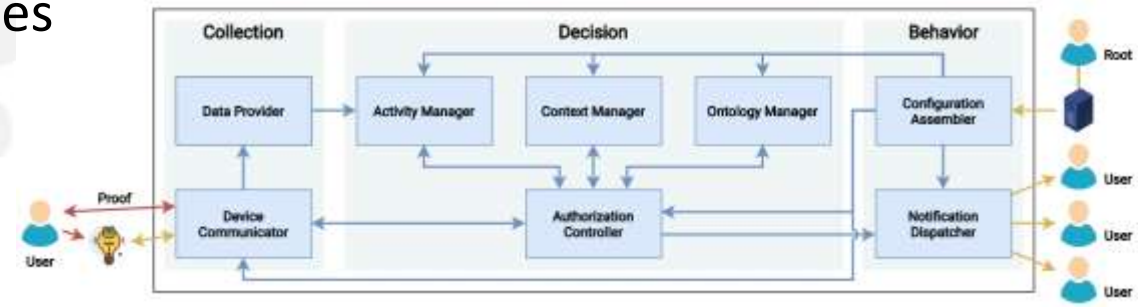
- **Article:** *PUFDCA: A Zero-Trust-Based IoT Device Continuous Authentication Protocol* by S. Alshomrani and S. Li.
- **Method:** *PUFDCA* – two-stage hybrid device authentication method based on unique device properties and device location.
- The first stage uses PUF (physical unclonable function), which is based on a device's physical microstructure.
- The second stage uses CSI measurements to verify the device's location during a session.



Context-based method

- **Article:** *Zero Trust Access Control with Context-Aware and Behavior-Based Continuous Authentication for Smart Homes* by G. R. de Silva, D. F. Macedo, and A. L. dos Santos.
- **Method:** *ZASH* – Zero-Aware Smart Home System.
- The method uses context clues (time, device, etc.) and prompts the user for a biometric proof (e. g. fingerprint) in case of suspicious behaviour.





Methods comparison

Name	Year	Main principle	Advantages	Limitations
CAB-IoT	2020	Based on face recognition and a distributed ledger	Limited bandwidth and storage requirements, resources-intensive processes handled by fog nodes, high accuracy	Limited robustness testing so far; face observation needed; fog nodes needed
WifiU	2017	Based on user’s gait, or the manner of walking	Does not need special hardware or lighting, easier to deploy and better coverage vs. video-based methods	Distance limited to 6 m, recognition accuracy limited, single user only, walking needed
Chuang et al.	2018	Static authentication via a shared secret, continuous authentication via timestamp and battery charge	Lightweight cryptography, taking limited computing resources and storage into account,	Needs initialization phase, needs secure storage for secrets, frequent messaging
PUFDCA	2022	Static authentication via PUF, continuous authentication via device location	Lightweight, low energy consumption, resistance against multiple attack types	Static authentication required before each connection, needs secure environment
ZASH	2021	Context clues and biometric proof in case of suspicion	Flexible, multiple access levels, protects against impersonation attacks	Needs stable behaviour patterns

Prospective CA for IoT

Based on existing methods suitable for IoT, we can identify several features that a prospective continuous authentication algorithm could have:

- ✓ Distributed – added scalability
- ✓ Biometric – most common and efficient approach
- ✓ Hybrid – combines static and continuous authentication for flexibility and security
- ✓ Context-aware – for further security
- ✓ User type-aware – useful in both home and corporate IoT

Conclusions

- Continuous authentication (CA) is a newer and more secure way of user authentication.
- IoT presents unique challenges for CA, including limited computational resources and lack of keyboard/mouse input.
- Several CA methods suitable for IoT have been considered.
- Each method has its own advantages and limitations; some are concerned with authenticating *devices*, while others are concerned with authenticating *human users*.
- Future research directions:
  - ➢ Biometric technologies most applicable to IoT-suitable CA
  - ➢ Distributed technologies most applicable to IoT-suitable CA
  - ➢ New algorithms based on the existing algorithms' best features

Санкт-Петербургский
государственный университет
spbu.ru