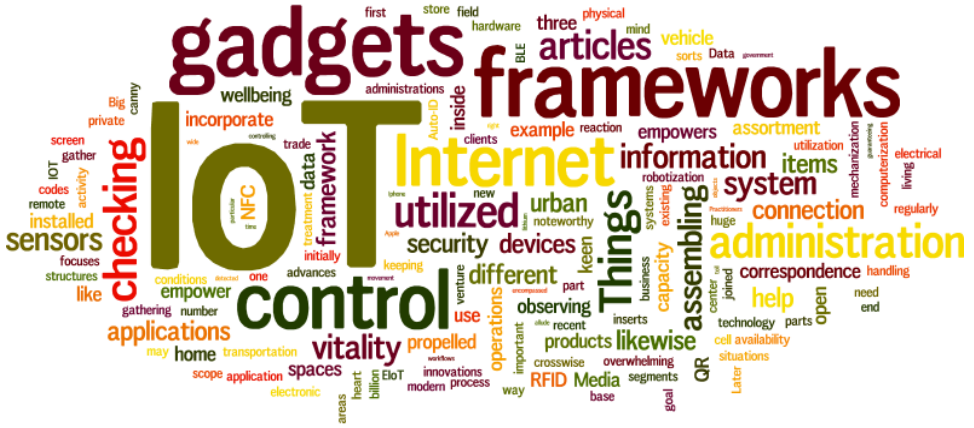
CS578: Internet of Things

Authentication in IoT



Dr. Manas Khatua

Assistant Professor, Dept. of CSE, IIT Guwahati

E-mail: manaskhatua@iitg.ac.in

"We must have life-building, man-making, character-making assimilation of ideas." – **Swami Vivekananda**

IoT network

- **Network of devices** collecting data.
- Communicating the data with **a central entity (in/outside network).**
- Communicating the data with each other **directly/ through multi-hop.**
- **Resource-constrained :** Computational capability, memory.
- **Battery-powered.**

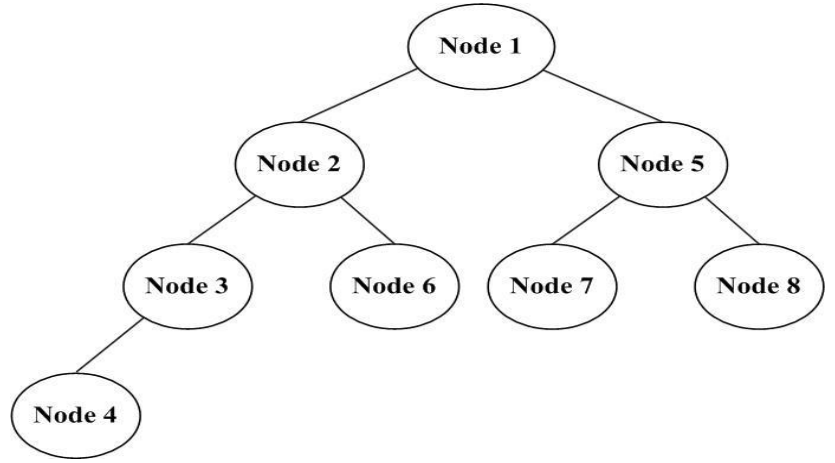


Fig 1: IoT Network

- Example:
  - **6TiSCH Network**

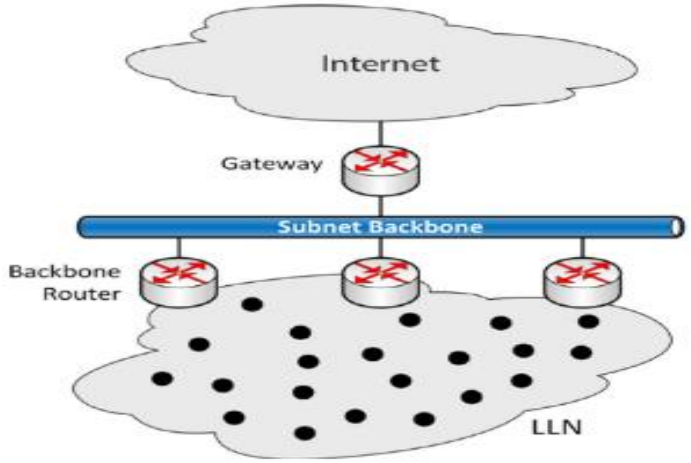


Fig 2: 6TiSCH Network

- Applications:
  - **Agricultural Monitoring**
  - **Industrial Automation**
  - **Healthcare system**

Authentication

- Authentication is a term that refers to the process of **proving that some fact or some document is genuine.**
- In computer science, this term is typically associated with **proving a user's identity.**
- Usually, a user proves their identity by providing their **credentials**, that is, **an agreed piece of information shared between the user and the system**.

✓ **A well-known example is accessing a user account on a website or a service provider such as Facebook or Gmail**

- Before we can access our account, we **must prove our own correct login credentials.**
- Services typically **present a screen that asks for a username along with a password.** Then, they compare the data inserted by the user with the **values previously stored in an internal repository.**

More Real-Life Applications of Authentication

- **Online Banking:** Users log into their bank accounts using **passwords, OTPs, or biometric authentication** for secure access to personal and financial information.
- **E-Commerce Websites (Amazon, eBay):** Authentication helps verify **users' identities to secure their accounts and payment information**. Many platforms use MFA to prevent unauthorized transactions.
- **Smartphone Unlocking:** Smartphones use **passwords, PINs, fingerprint scans, or facial recognition** to authenticate the user before allowing access to the device.
- **Workplace Systems and Corporate Networks:** Employees access internal systems through **login credentials, security tokens,** and sometimes additional authentication methods like VPNs or smart cards.
- **Health Care Portals:** Patients and doctors access medical records via online portals that require authentication through **passwords and sometimes additional verification, like security questions or OTPs.**
- **IoT Devices (Smart Home Systems):** Devices like smart locks, security cameras, or thermostats **require authentication through mobile apps or voice recognition** to prevent unauthorized access to your home systems.

Phases in an Authentication Scheme

- **Enrollment / Registration Phase.**
- **Authentication Phase.**

✓ **Enrollment / Registration Phase.**

- **User / system registers itself to a trusted system.**
- Performed with **sharing credentials**.
- **may or may not be** executed **multiple times.**

✓ **Authentication Phase:-**

- User / system **inputs the shared credential**.
- Trusted system **verifies the same.**
- executed **multiple times.**

Enrollment / Registration Phase

- The **enrollment phase** of authentication is the initial setup stage where a user or device **registers their identity information** with a system to enable **future authentication.**

- This phase is crucial because it sets the **baseline data or "template"** the system will use to **verify the user's identity** during future logins.

✓ **Steps followed during Enrollment / Registration Phase:-**

- **User Identity Capture:** The user provides **an identity element** that the system will use for authentication. **For example:- password**.

- **Data Processing and Storage:-** The system processes the captured data to create a **template** or **profile**. This template or profile acts **as the reference point for future authentication attempts.**

- **Verification and Confirmation:-** To ensure the data **is correctly captured**, some systems will ask the user to repeat the process. For instance, in **biometric enrollment**,user might have to provide their biometric data multiple times.

- **Secure Storage and Encryption:-** The system securely **stores the template data** in an **encrypted format** to protect it from unauthorized access. This ensures that if the authentication **database is compromised,** attackers **cannot easily retrieve or misuse** the original data.

- **Device or Account Linkage:-** In multi-factor authentication (MFA) setups, the enrollment phase might also involve linking additional authentication factors (e.g., a mobile phone number for OTPs, or an authentication app like Google Authenticator). This ensures multiple layers of security.

Example: Biometric Enrollment Process

1. The user **places their finger** on a scanner multiple times.
2. The scanner **captures various angles and sections** of the fingerprint.
3. The system processes these images to create **a unique fingerprint template**.
4. This template is **stored securely and will be used to match future scans** when the user tries to authenticate.

Key Points of the Enrollment/Registration Phase

•**Accuracy**: The enrollment phase ensures that the data collected is **accurate and high-quality** to minimize false rejections or acceptances later.

•**Security:** Data is often **encrypted and stored securely** to protect against theft or tampering.

•**Convenience**: Well-designed enrollment procedures should **be straightforward**, as a poor experience may discourage users from completing setup.

Authentication Phase

- The **authentication phase** in an authentication scheme is when a user or device **attempts to access a system** by providing their **credentials.**
- It is then verified against the **reference data or template** set up during the **enrollment phase**.
- This phase determines whether access will be **granted or denied**.

Steps followed during Enrollment / Registration Phase:-

- **Credentials Submission:-** The user or device provides their **credentials or identifying information**. For example: **Password, biometric, OTP.**
- **Credential Processing :-** System processes **the credentials**, such as **hashing a password or creating a biometric template.**
- **Comparison with Template :-** System compares **the processed credentials** against **stored templates or values.**
- **Decision Making :-** If the credentials match, **access is granted;** otherwise, access is denied.
- **Feedback to User :-** System informs the user of **the outcome** (successful login or error).

Example of Authentication Phase for Various Methods

➢ **Password-Based Authentication**:

1. The user enters a **password.**
2. The system hashes it and **compares** it to the stored hash.
3. If it matches, access **is granted;** otherwise, it's denied.

➢ **Biometric Authentication**:

1. The user provides a **fingerprint or facial scan**.
2. The system processes this and generates **a template.**
3. It **compares** the **generated template** to the **stored one** from enrollment.
4. If they match closely enough, **access is granted**.

Need for Authentication in IoT

- IoT network deployed in **adverse conditions**.
- Devices can easily get **compromised.**
- Important to **verify** the devices.
- **Protecting the communications** from security breach.
- Done by **assigning credentials to devices and verifying** them when needed.
- **Lightweight** due to the **resource-constrained nature**.

Real-life example:-

✓ Mirai Botnet (2016): Hackers used **compromised IoT devices** (e.g., cameras, routers) to launch **massive DDoS attacks** on websites like Twitter, Netflix, and CNN.

General Authentication v/s IoT Authentication

Aspects	General Authentication	IoT Authentication
Device Nature	Traditional devices like servers, computers	Wide range of devices like sensors, wearables, industry appliances etc.
Computational Power	High	Low due to its resource-constrained nature
Scalability	Moderate	Massive (Thousand to millions of device)
Connectivity	Stable	Intermittent (low power network)
Power Constraints	Not significant	Significant (battery-operated devices)
Physical Security	Typically secured with password protection	Often in unsecured or remote locations
Communication	User-to-system interaction (with human intervention)	Device-to-device and device-to-cloud (autonomous)
Challenges	Password theft, data breaches	Device tampering, Device-device security, low power

Types of Authentication Schemes in IoT

Based on Authentication Architecture:

- ❑ **Centralized Authentication Scheme**
- ❑ **Distributed Authentication Scheme**

✓ **Centralized Authentication Scheme:**

- User / system is authenticated by a **single entity**. **For example: Gateway, cloud server etc.**

✓ **Distributed Authentication Scheme:**

- User / system is authenticated by **more than one entity**. **For example: IoT nodes.**

Centralized Authentication Scheme

✓ CHEAP :-

- **Enrollment Phase:**
  - Enrolls via **secure channel**.
  - Gateway **stores credentials** of IoT device.
- **Authentication Phase:**
  - IoT Node1 authenticates itself with other IoT node 2.
  - Via Gateway.
  - **Hash, XoR and concatenation** operation is performed.
  - **Multiplication operations**.
  - IoT Node 1 ⟷ Gateway ⟷ IoT Node 2.

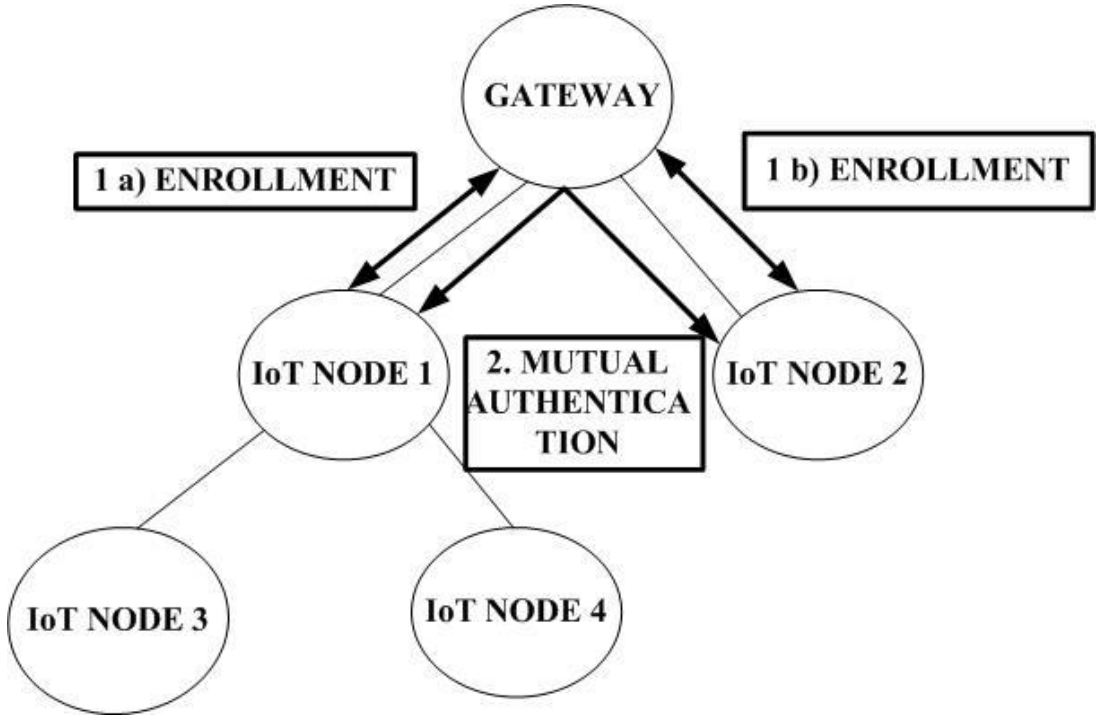


Fig 3: Authentication Flow by Pu et. al.

➢ Pu, Cong, Imtiaz Ahmed, and Sumit Chakravarty. "Resource-Efficient and Data Type-Aware Authentication Protocol for Internet of Things Systems." ***2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA).*** IEEE, 2023.

Centralized Authentication Scheme (Contd..)

✓ CloAuth :-

❑ Enrollment Phase-

- Gateway and user enrolls with CS.

- IoT device enrolls with Gateway.

- CS shares secret with gateway and user.

- Gateway shares secret with IoT device.

❑ Authentication Phase-

- takes places using **hash, concatenation and XoR**.

- uses s**calar multiplications**.

- User ⟷ CS ⟷ Gateway ⟷ User ⟷ Gateway ⟷ CS ⟷ User.

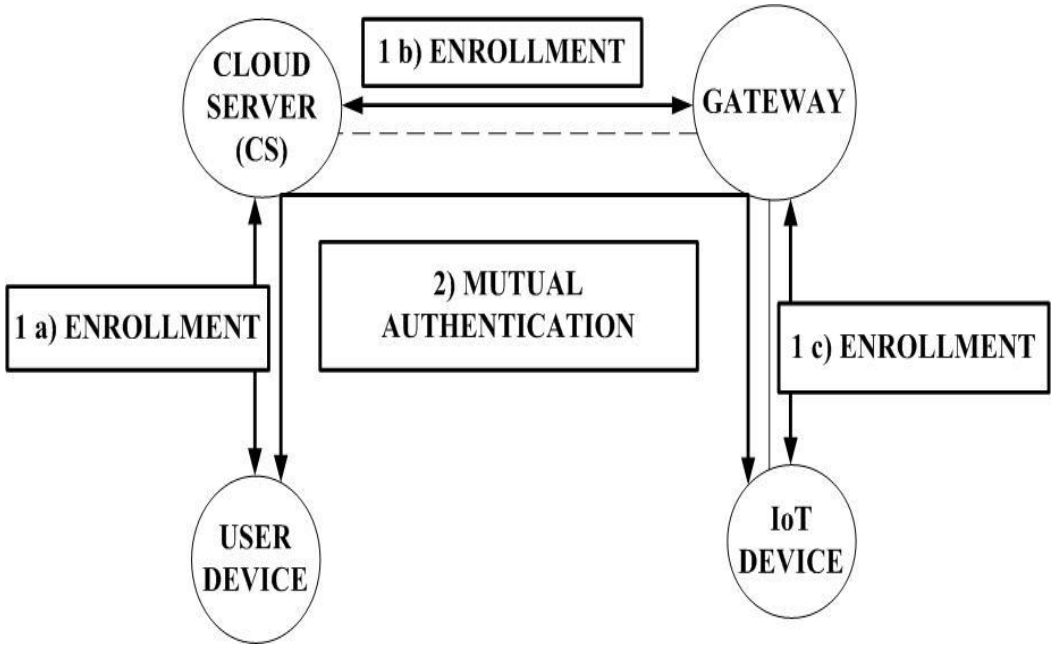


Fig 5: Authentication Flow by Wang et. al.

➢ Wang, Chenyu, et al. "Secure and lightweight user authentication scheme for cloud-assisted internet of things." ***IEEE Transactions on Information Forensics and Security*** 18 (2023): 2961-2976.

Centralized Authentication Scheme (Contd..)

✓ SmartAuth :-

- **Enrollment Phase:**
  - Performed via secure channel.
  - Private-Public key pair stored by user.
- **Authentication Phase:**
  - Based on **encryption-decryption** and **concatenation** operations
  - User device ⟷ Authentication Device ⟷ Controller Device

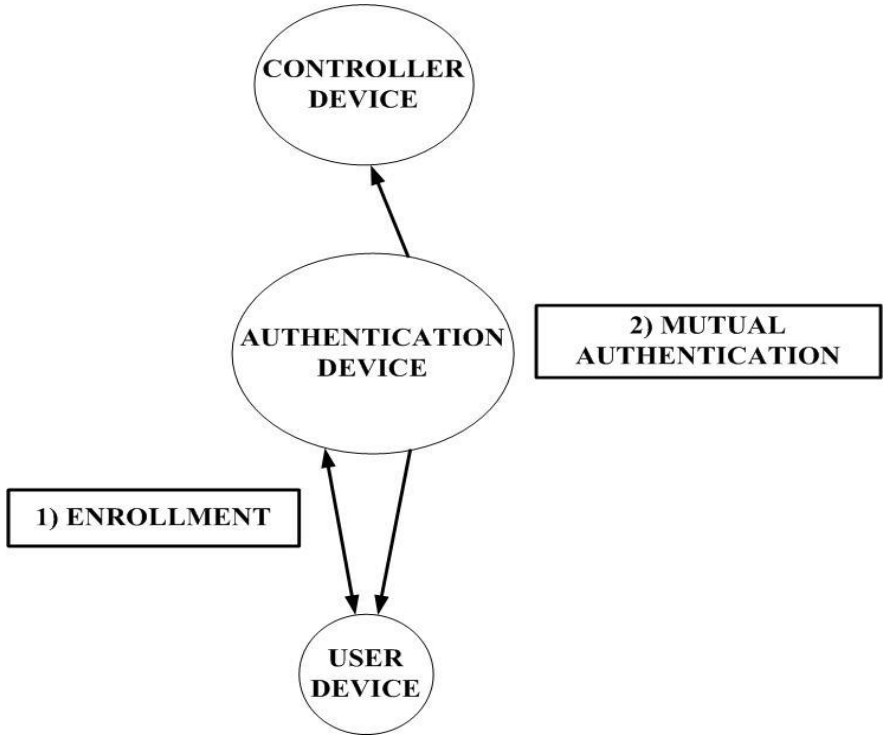


Fig 7: Authentication Flow by Kumar et. al.

➢ Kumar, Vipin, et al. "Light weight authentication scheme for smart home iot devices." ***Cryptography*** 6.3 (2022): 37.

Centralized Authentication Scheme (Contd..)

✓ ProvAuth :-

❑ Prerequisites:

✓ Physically Unclonable Function (PUF):-

- The inherent **physical variations** present in a **device's hardware** creates a **unique, unpredictable response** for any **given input** (often referred to as a **"challenge").**
- A PUF can be represented as **R = P(C),** i.e., a PUF P maps a **challenge C to a unique response R**.
- A challenge and its corresponding response from a PUF is termed a **challenge-response pair (CRP).**
- If a PUF is excited using **the same challenge multiple times**, it will always produce **the same response.**

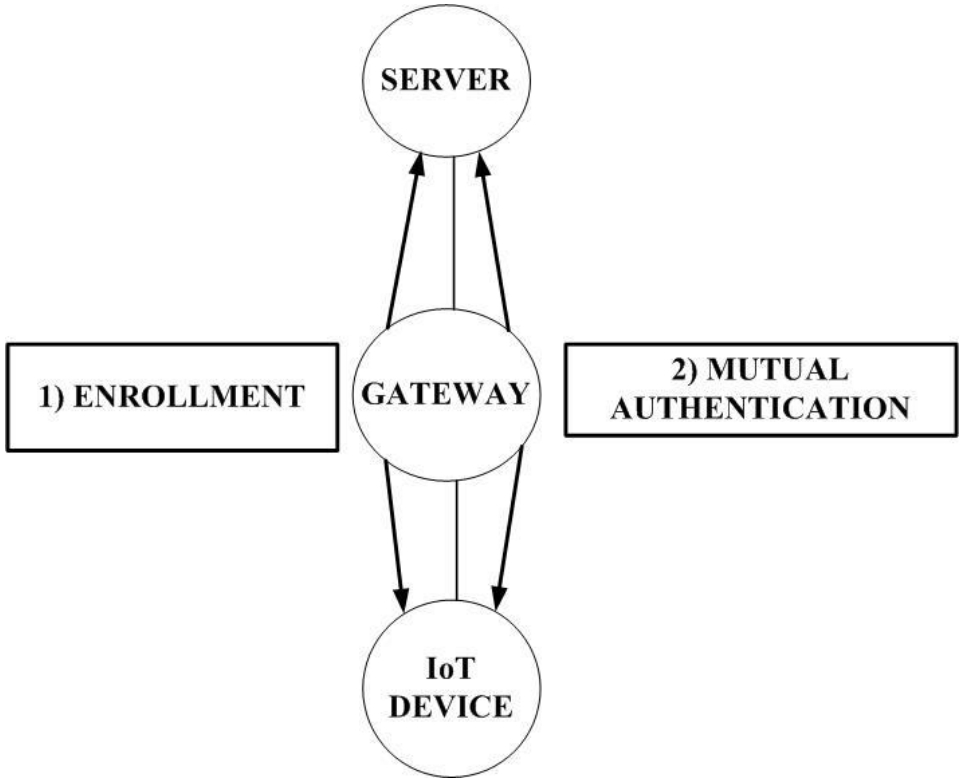


Fig 6 : Authentication Flow by Aman et. al.

➢ Aman, Muhammad Naveed, Mohammed Haroon Basheer, and Biplab Sikdar. "Data provenance for IoT with light weight authentication and privacy preservation." ***IEEE Internet of Things Journal*** 6.6 (2019): 10441-10457.

Centralized Authentication Scheme (Contd..)

✓ ProvAuth :-

❑ Prerequisites:

✓ Physically Unclonable Function (PUF):-

- The **same challenge** is applied to **different PUFs**, the **response** will be significantly **different**.
- This implies that **each PUF** is **unique** in terms of its **CRPs**.
- It removes the need of key storage from IoT device.
- It protects devices from physical and cloning attack.

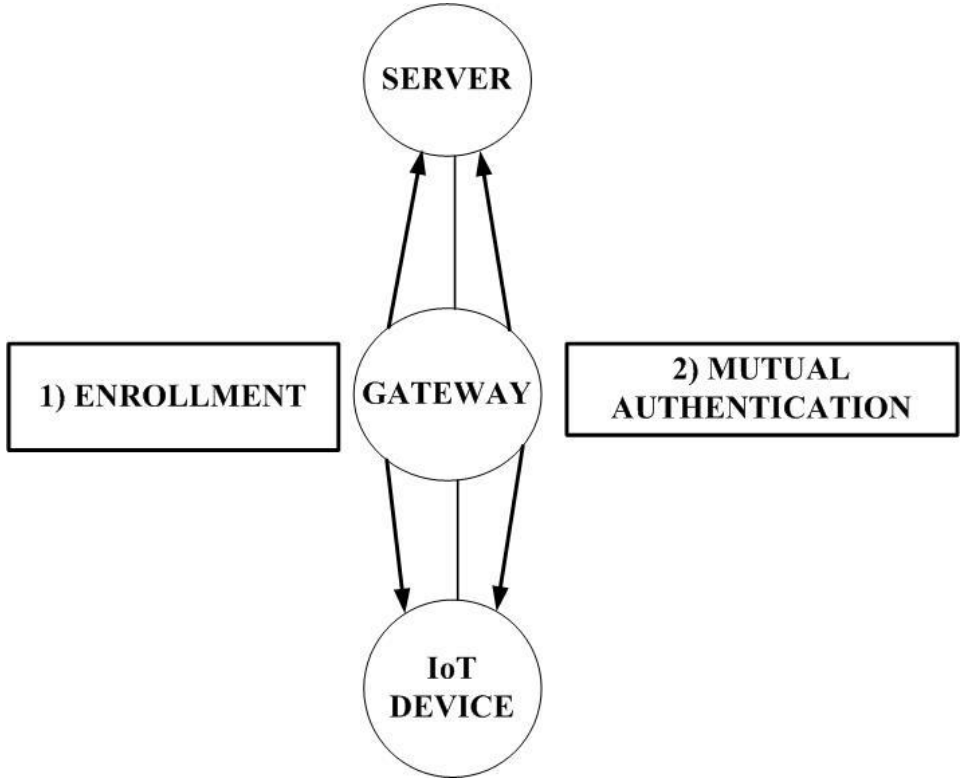


Fig 6 : Authentication Flow by Aman et. al.

➢ Aman, Muhammad Naveed, Mohammed Haroon Basheer, and Biplab Sikdar. "Data provenance for IoT with light weight authentication and privacy preservation." ***IEEE Internet of Things Journal*** 6.6 (2019): 10441-10457.

Centralized Authentication Scheme (Contd..)

✓ ProvAuth :-

❑ Enrollment Phase:

- IoT device enrolls with server via secure channel.
- Step 1 :- Server
  - ✓ generates **initial challenge: C^i**
  - ✓ Generates a pseudonym identity for the IoT Device A: **PID^i**
  - ✓ **Sends C^i and PID^i** to IoT Device via **secure channel**.
- -Step 2 :- IoT Device
  - ✓ A generates **$R^i = PUF(C^i)$** and send it to **server.**
- -Step 3:- Server
  - ✓ Server **stores CRP and pseudonym identity**.
- - IoT Device A:-
  - ✓ Stores **C^i and PID^i** with itself.

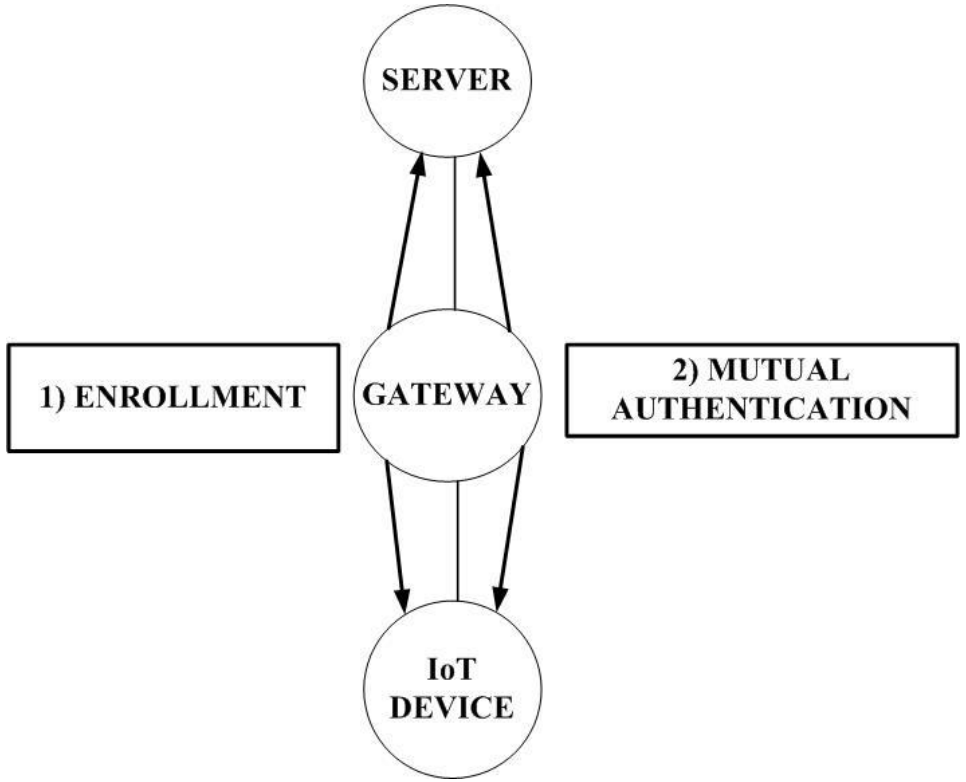


Fig 6 : Authentication Flow by Aman et. al.

➢ Aman, Muhammad Naveed, Mohammed Haroon Basheer, and Biplab Sikdar. "Data provenance for IoT with light weight authentication and privacy preservation." ***IEEE Internet of Things Journal*** 6.6 (2019): 10441-10457.

Centralized Authentication Scheme (Contd..)

✓ ProvAuth :-

❑ Authentication Phase :-

- **Step 1: IoT Device A**

  - ✓ Generates $\mathbf{R^i = PUF(C^i)}$.
  - ✓ Generates a random nonce $\mathbf{N_a}$.
  - ✓ Encrypts nonce with R^i : $\mathbf{\{N_a\}_{Ri}}$
  - ✓ $\mathbf{M_0 = \{PID^i , \{N_a\}_{R^i}\}}$
  - ✓ **Authentication parameter:** $\mathbf{I_0 = H(M_0 \,||\, R^i)}$.
  - ✓ Sends $\mathbf{M_0 \,||\, I_0}$ to **server via. Gateway**
  - ✓ **Authentication parameter** helps server to **verify the integrity of** $\mathbf{M_0}$

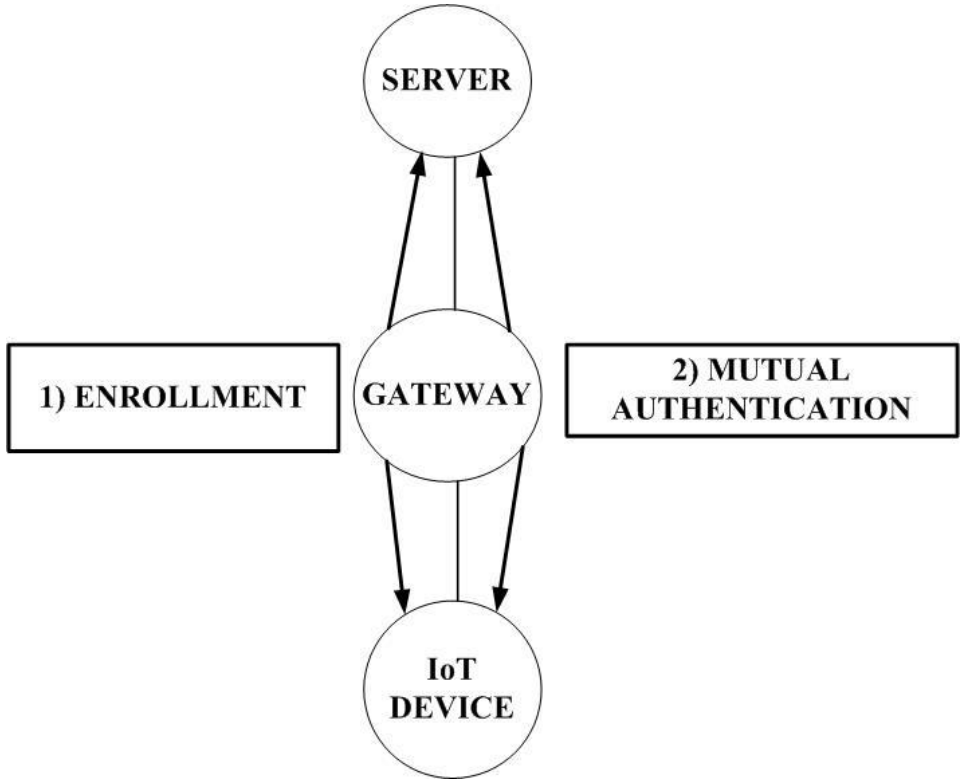


Fig 6 : Authentication Flow by Aman et. al.

➢ Aman, Muhammad Naveed, Mohammed Haroon Basheer, and Biplab Sikdar. "Data provenance for IoT with light weight authentication and privacy preservation." ***IEEE Internet of Things Journal*** 6.6 (2019): 10441-10457.

Centralized Authentication Scheme (Contd..)

✓ ProvAuth :-

❑ Authentication Phase :-

- **Step 2: Server :-**

  - ✓ **Locates PID^i** in the memory.
  - ✓ Reads the **CRP: (C^i, R^i).**
  - ✓ **Verifies I_0.**
  - ✓ Generates **nonce N_b** .
  - ✓ **$M_1 = \{ PID^i, N_a \,||\, N_b \}$**
  - ✓ **Auth. Parameter: $I_1 = H(M_1 \,||\, N_a \,||\, N_b \,||\, R^i)$**
  - ✓ Sends **$M_1 \,||\, I_1$** to **IoT device via. Gateway**

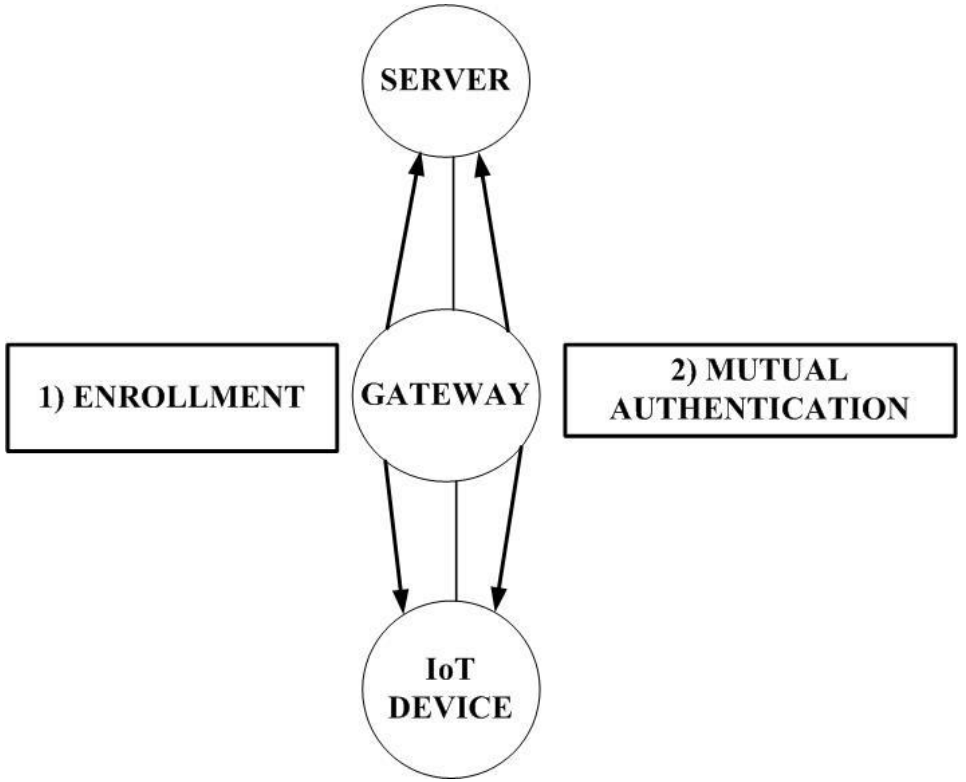


Fig 6 : Authentication Flow by Aman et. al.

➢ Aman, Muhammad Naveed, Mohammed Haroon Basheer, and Biplab Sikdar. "Data provenance for IoT with light weight authentication and privacy preservation." ***IEEE Internet of Things Journal*** 6.6 (2019): 10441-10457.

Centralized Authentication Scheme (Contd..)

✓ ProvAuth :-

❑ Authentication Phase :-

- **Step 3: IoT Device :-**

  - ✓ **Verify I_1.**
  - ✓ Session Key: $k_1 = N_a \oplus N_b$
  - ✓ $PID^{i+1} = H(ID_{A.} || N_a || R^i)$
  - ✓ **Auth par:** $I_{2.} = H(PID^i || PID^{i+1} || N_a || N_b || R^i)$
  - ✓ Sends I_2 to **server via. Gateway**

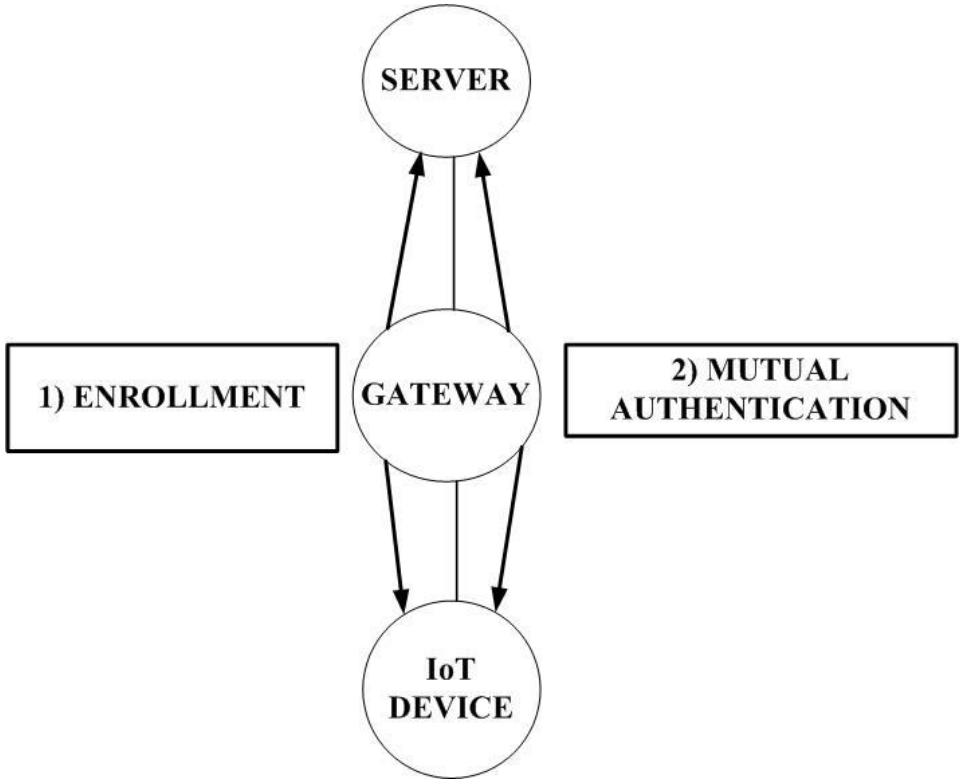


Fig 6 : Authentication Flow by Aman et. al.

➢ Aman, Muhammad Naveed, Mohammed Haroon Basheer, and Biplab Sikdar. "Data provenance for IoT with light weight authentication and privacy preservation." ***IEEE Internet of Things Journal*** 6.6 (2019): 10441-10457.

Centralized Authentication Scheme (Contd..)

✓ ProvAuth :-

❑ Authentication Phase :-

- **Step 4: Server :-**

  - ✓ Regenerates $\mathbf{PID^{i+1} = H(ID_{A.} \,||\, N_a \,||\, R^i)}$
  - ✓ **Verify I_2.**
  - ✓ Stores $\mathbf{PID^{i+1}}$

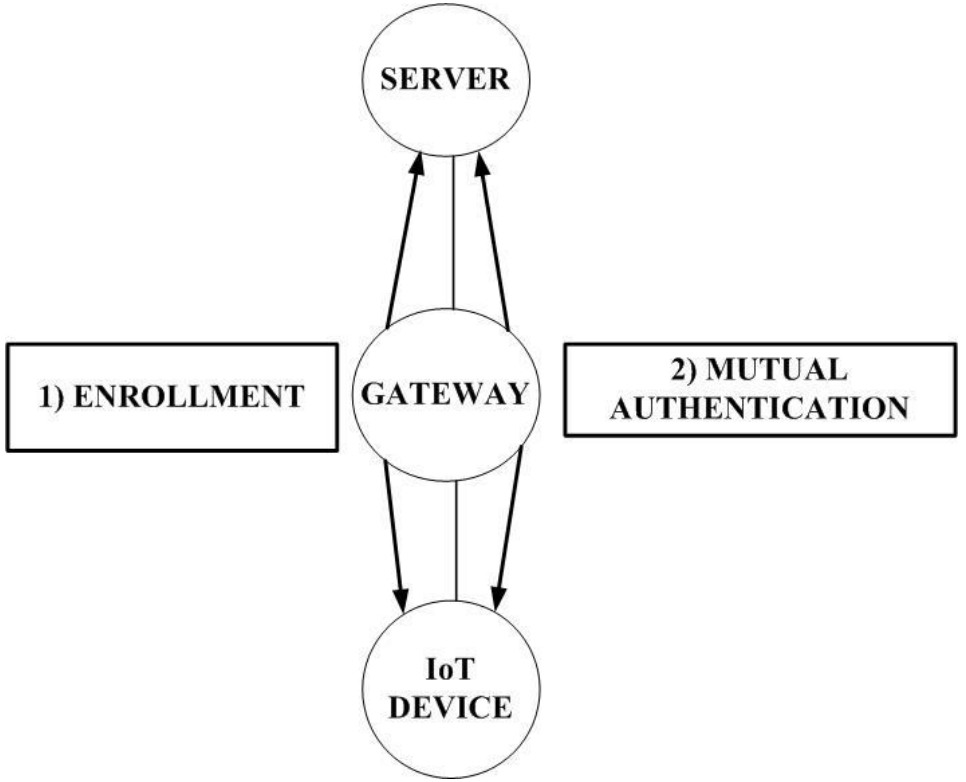


Fig 6 : Authentication Flow by Aman et. al.

➢ Aman, Muhammad Naveed, Mohammed Haroon Basheer, and Biplab Sikdar. "Data provenance for IoT with light weight authentication and privacy preservation." ***IEEE Internet of Things Journal*** 6.6 (2019): 10441-10457.

Drawbacks of Centralized Scheme

- **Resource overhead** on Centralized entity, as it has to authenticate all IoT nodes.
- Centralized entity can fail due to s**ecurity breach or malfunction**, failing the scheme.
- **Imposes resource and communication overhead**, as nodes need communicate with authenticator, by traversing many intermediate nodes.
- Do not provide **equal amount of security** to every node.

.
.

Distributed Authentication Scheme

✓ HessianAuth :-

- Parent node acts as an **authenticator**.

- **Enrollment Phase:**
  - **Public key generation** by Node 1.
  - **Node 1** sends that to N**ode 2**.
  - **Node 2** store the Public key of 1

- **Authentication Phase:**
  - **Node 1** sends **generated signature** to Node 2
  - Node 2 **verifies signature** with Node 1: **Public Key**.

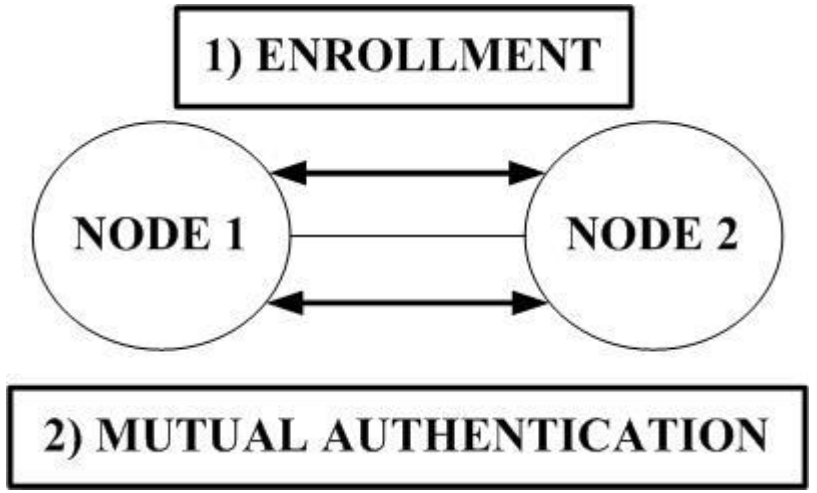


Fig 10: Authentication Flow by Dey et. al.

➢ Dey, Debasmita, Saket Chandra, and Nirnay Ghosh. "HessianAuth: An ECC-based distributed and efficient authentication mechanism for 6LoWPAN networked IoT devices." ***Proceedings of the 24th International Conference on Distributed Computing and Networking***. 2023.

Distributed Authentication Scheme (Contd..)

✓ PHIP , ImpliCertAuth :-

- ❑ Parent node acts an authenticator.
- ❑ **Enrollment Phase :**
  - **Node ↔ CA**.
  - Node sends **public key** to CA.
  - CA sends a **certificate** to Node.
  - Node stores the **certificate**.
- ❑ **Authentication Phase :**
  - **Node 1 ↔ Node 2**
  - Node 1 sends its **certificate** to Node 2.
  - Node 2 **verifies** and sends its **certificate.**
  - Node 1 **verifies the certificate**.

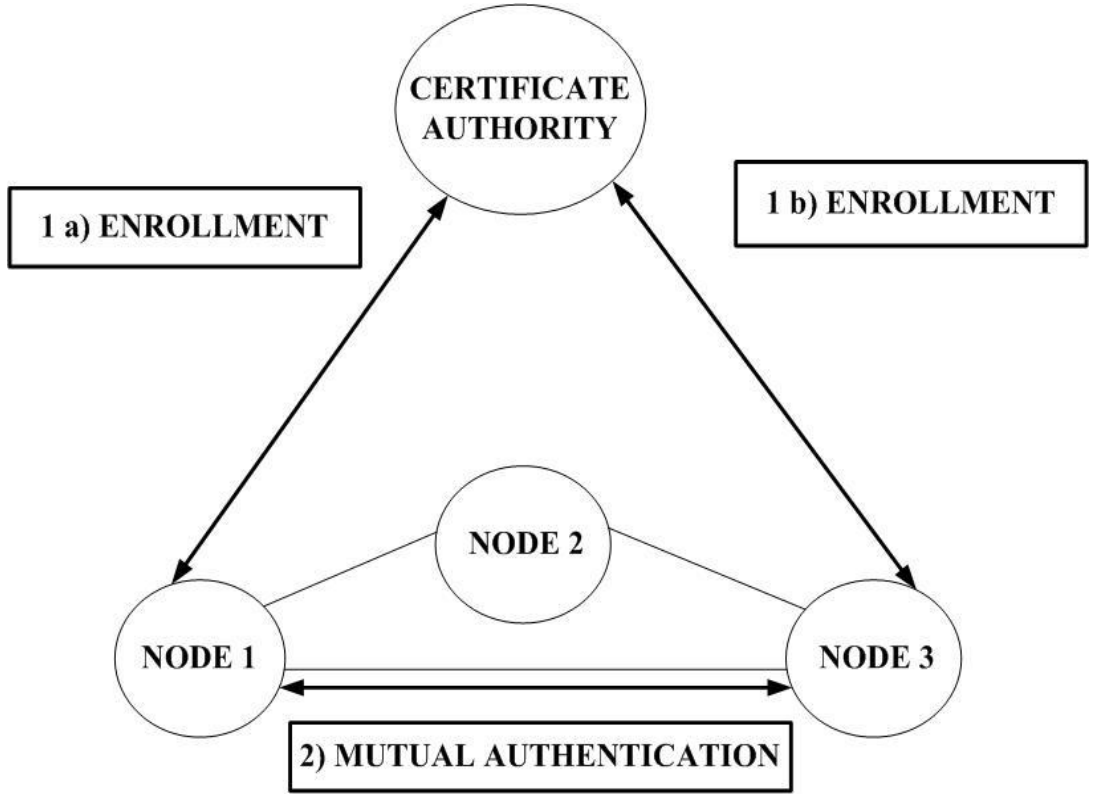


Fig 12: Authentication Flow by Hossain et. al. and Siddhatha et. al.

- Hossain, Mahmud, and Ragib Hasan. "P-hip: A lightweight and privacy-aware host identity protocol for internet of things." ***IEEE Internet of Things Journal*** 8.1 (2020): 555-571.
- Siddhartha, Valmiki, Gurjot Singh Gaba, and Lavish Kansal. "A lightweight authentication protocol using implicit certificates for securing IoT systems." ***Procedia Computer Science*** 167 (2020): 85-96.

Distributed Authentication Scheme (Contd..)

✓ EdgeAuth :-

- Edge node acts as an authenticator.

- **Enrollment Phase:**
  - **Node ↔ Edge Server**
  - Node sends **public key** to Edge.
  - Edge **stores public key** in secure database.
  - Edge sends **its public key**.

- **Authentication Phase:**
  - **Node 4 ↔ Edge Server ↔ Node 5**
  - 4 sends credentials to edge using keys.
  - Edge **verifies it** .
  - Edge sends its credentials to 5.
  - 5 verifies the credential from edge.
  - Encryption is performed.

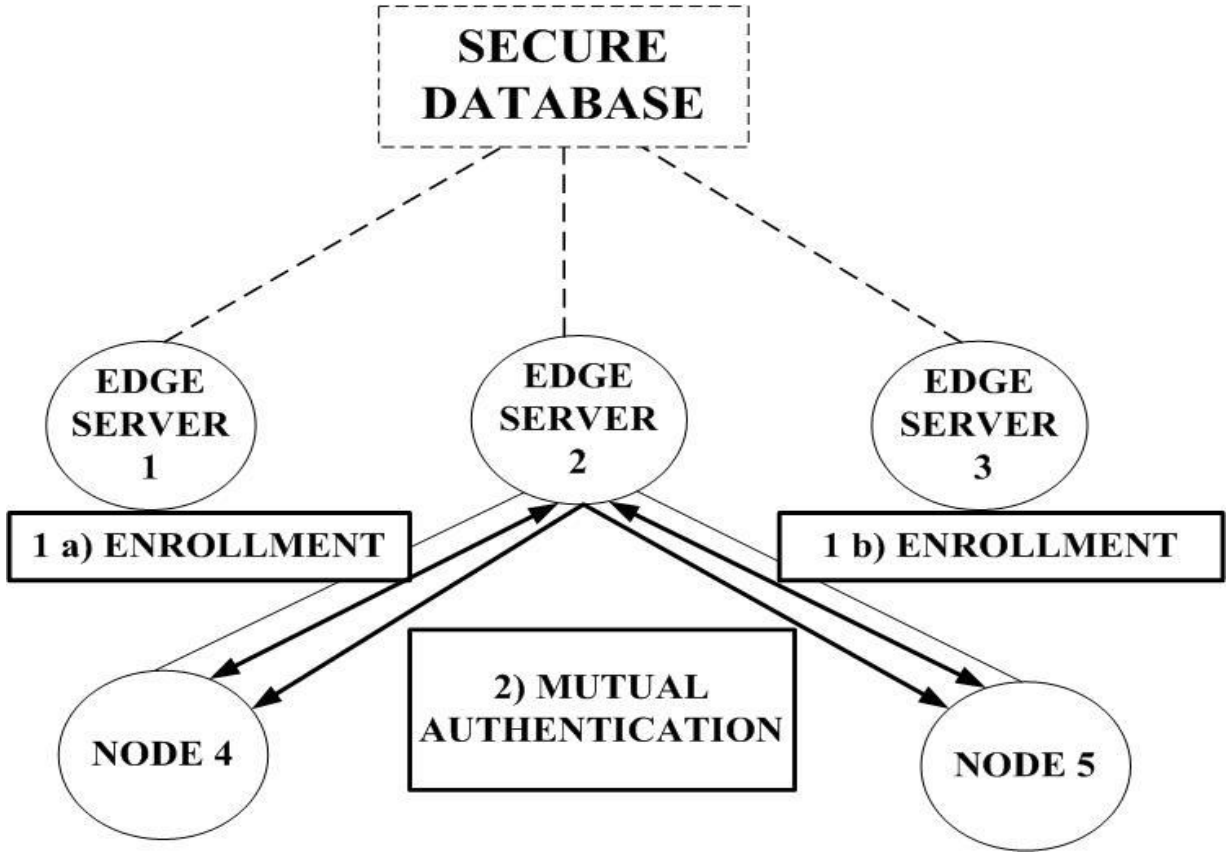


Fig 14: Authentication Flow by Shahidinejad et. al.

➢ Shahidinejad, Ali, and Jemal Abawajy. "Decentralized lattice-based device-to-device authentication for the edge-enabled IoT." ***IEEE Systems Journal*** (2023).

Distributed Authentication Scheme (Contd..)

✓ LightSAE :-

- .Newly joined nodes authenticated by parent node.
- **Enrollment Phase:**
  - **Common keys** : **DK**- Network Key, **PK**- Key Set.
- **Authentication Phase:**
  - Node 4 ⟷ Newly Joined Node.
  - **E(DK, K || ID); K ϵ PK : Authentication Request**.
  - **E(K, (DK ⊕ R1) || E(K,X));** R1, X are random numbers : **Challenge**.
  - **E(K, R1 || X)** : **Challenge Response**.

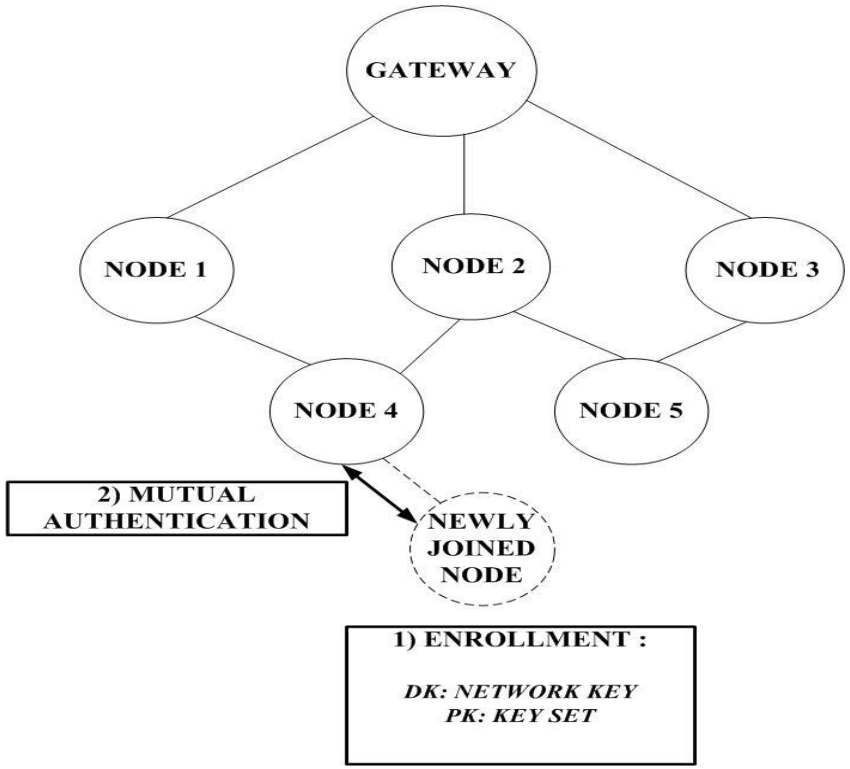


Fig 8: Authentication Flow by Rosa et. al.

➢ Rosa, Pedro, André Souto, and José Cecílio. "Light-SAE: a lightweight authentication protocol for large-scale IoT environments made with constrained devices." ***IEEE Transactions on Network and Service Management*** 20.3 (2023): 2428-2441.

References

1) Pu, Cong, Imtiaz Ahmed, and Sumit Chakravarty. "Resource-Efficient and Data Type-Aware Authentication Protocol for Internet of Things Systems." ***2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications*** (TPS-ISA). IEEE, 2023.

2) He, Daojing, et al. "A lightweight authentication and key exchange protocol with anonymity for IoT." ***IEEE Transactions on Wireless Communications*** 22.11 (2023): 7862-7872.

3) Wang, Chenyu, et al. "Secure and lightweight user authentication scheme for cloud-assisted internet of things." ***IEEE Transactions on Information Forensics and Security*** 18 (2023): 2961-2976.

4) Aman, Muhammad Naveed, Mohammed Haroon Basheer, and Biplab Sikdar. "Data provenance for IoT with light weight authentication and privacy preservation." ***IEEE Internet of Things Journal*** 6.6 (2019): 10441-10457.

5) Kumar, Vipin, et al. "Light weight authentication scheme for smart home iot devices." ***Cryptography*** 6.3 (2022): 37.

6) Rosa, Pedro, André Souto, and José Cecílio. "Light-SAE: a lightweight authentication protocol for large-scale IoT environments made with constrained devices." ***IEEE Transactions on Network and Service Management*** 20.3 (2023): 2428-2441.

7) Dey, Debasmita, Saket Chandra, and Nirnay Ghosh. "HessianAuth: An ECC-based distributed and efficient authentication mechanism for 6LoWPAN networked IoT devices." ***Proceedings of the 24th International Conference on Distributed Computing and Networking***. 2023.

8) Hossain, Mahmud, and Ragib Hasan. "P-hip: A lightweight and privacy-aware host identity protocol for internet of things." ***IEEE Internet of Things Journal*** 8.1 (2020): 555-571.

Thanks!