Authenticating Legacy IoT Devices Without SIM Cards in 5G Networks Using Federated Identity

David Araújo

Cybersecurity Course, Department of Electrical and Electronic Engineering, Universidade de Aveiro, Aveiro, PT
Email: davidaraujo@ua.pt

This paper explores the integration of federated identity management (FID) into 5G networks to address the challenges of securing and authenticating IoT devices. As 5G networks enable the massive growth of IoT devices, traditional authentication methods struggle with scalability and security, especially for legacy devices lacking modern security features. FID offers a unified authentication framework that allows IoT devices to access multiple services across different domains with a single set of credentials, improving efficiency and security. The paper discusses the role of federated identity protocols, such as the Network Service Federated Identity (NS-FId), in enabling multi-level authentication, authorization, and secure access. Additionally, it examines how integrating FID into core network functions like the Unified Data Management (UDM) system enhances service access and user authentication. This approach ensures seamless interoperability, improved security, and continuous connectivity for IoT devices across diverse 5G network slices and service providers.

Keywords: Legacy IoT Devices, 5G Networks, Authentication, Federated Identity, SIM Cards, Internet of Things (IoT), Security Protocols, Multi-level Authentication, Device Registration, Scalability

1. INTRODUCTION

The growth of 5G networks has transformed Internet of Things (IoT) connectivity but created challenges for older IoT devices that lack 3GPP capabilities. These devices often struggle with security issues and difficulty connecting to advanced networks.

Federated identity provides a scalable solution by allowing devices to authenticate across multiple providers, ensuring secure and seamless access. This paper explores how federated identity can meet the authentication needs of legacy IoT devices in 5G, covering integration, benefits, and challenges.

2. BACKGROUND

2.1. 5G Networks and IoT

5G improves IoT connectivity by supporting more connected devices and ensuring strong authentication. It meets the needs of various components like sensors, actuators, cameras, and automated guided vehicles, enabling the digitalization, automation, and distributed computing necessary for modern businesses to succeed [1].

With its ability, 5G is key to Industry 4.0, with private networks expected to grow from thousands to tens of thousands [1]. This growth is fueled by private spectrum availability, cost-effective cloud deployments, and scalable systems. By replacing older wired and WLAN systems, 5G simplifies deployment and reduces total costs while providing reliable, low-latency connectivity.

2.2. Legacy IoT Devices

IoT refers to the expanding network of physical devices with sensors, software, and connectivity. From smart thermostats and wearables to industrial sensors, IoT devices are becoming increasingly common across various sectors and in daily life.

Legacy IoT devices without SIM cards face significant challenges in 5G networks, especially in terms of authentication and security. Traditional SIM-based authentication relies on physical SIM cards to store credentials, ensuring device identity and data integrity. Without these, devices lack a secure hardware component, making them more vulnerable to unauthorized access and cyberattacks [2].

In 5G networks, methods such as EAP-TLS (Extensible Authentication Protocol-Transport Layer

Security) are used [3]. These methods do not rely on SIM cards but use digital certificates for mutual authentication. While offering more flexibility, they also pose challenges for legacy devices that lack the necessary hardware or software to support these protocols. As a result, these devices may struggle to meet the security standards of 5G networks, potentially weakening the integrity of the overall IoT ecosystem [4].

These solutions should focus on secure, lightweight methods that can easily integrate into existing infrastructure, ensuring that all IoT devices, can function securely within 5G environments [5].

2.3. Federated Identity

Federated identity is a system that allows users to access multiple applications or services with a single set of credentials across different organizations or domains. It simplifies authentication by sharing identities between various identity management systems, enabling access without requiring separate logins for each service [6].

This concept is interesting because IoT devices often interact with multiple services and platforms, requiring a unified authentication method. Federated identity enables these devices to authenticate once and access various services, improving efficiency and security. This is particularly useful in environments where devices from different manufacturers or organizations must work together [7].

By adopting federated identity, organizations can implement Single Sign-On (SSO), allowing users or devices to access multiple services with a single authentication process. This not only strengthens security by centralizing authentication and access control, but also offers a lightweight and efficient way to manage authentication across diverse services [7].

3. AUTHENTICATION CHALLENGES IN 5G IOT

3.1. Security Concerns

Despite their advancements, 5G networks introduce significant security challenges for IoT. The increased connectivity expands the attack surface [2], with billions of IoT devices becoming potential targets for cybercriminals. Many consumer-grade devices lack strong security due to limited resources and weak or default configurations, increasing the risk of DDoS attacks, malware infections, and data breaches. 5G's complex architecture also leaves room for sophisticated man-in-the-middle attacks, and the heavy reliance on APIs in 5G networks creates vulnerabilities that attackers could exploit to gain unauthorized access or disrupt operations [8].

A fragmented IoT ecosystem complicates security further, as the lack of standardization across devices, manufacturers, and protocols creates vulnerabilities [2]. Without uniform security measures, low-cost devices often lack advanced encryption, leaving them exposed. Many legacy IoT devices were not designed for 5G and lack modern security features [2]. Upgrading these devices can be costly and time-consuming, especially for industries with large-scale deployments.

Technologies like Software Defined Networks (SDNs) and Network Function Virtualization (NFV), crucial to 5G, require strong security across all layers [2]. For example, centralized controls in SDN could become single points of failure if compromised.

3.2. Scalability Issues

Managing the authentication of millions of IoT devices in 5G networks presents scalability challenges. Traditional authentication methods may struggle to efficiently handle such a large volume, leading to potential security risks and network inefficiencies.

To address these challenges, automated Public Key Infrastructure (PKI) systems have become crucial. These systems manage the issuance and handling of digital certificates, allowing devices to authenticate securely without manual intervention. Manufacturers of 5G equipment increasingly rely on automated PKI for efficient authentication and certificate management as devices are deployed [9].

The cost of deploying and maintaining 5G infrastructure can also be a barrier, especially for smaller businesses. However, as 5G becomes more widespread and affordable, its scalability and performance benefits for IoT applications will justify the initial investment [10].

Ensuring compatibility between legacy systems and new standards is essential for seamless communication and efficient resource management [11].

4. FEDERATED IDENTITY FOR LEGACY IOT AUTHENTICATION

A study published in IEEE Xplore introduces an Identity Federation mechanism that reuses SIM authentication for cellular IoT devices, simplifying the authentication process while enhancing security. By enabling single sign-on features, this solution reduces the burden on IoT providers to develop proprietary identity management systems. Leveraging existing SIM authentication infrastructure, it provides affordable, enhanced security for the growing number of IoT devices expected to connect to 5G networks, thus reducing operational costs [12].

Another source on ResearchGate explores the potential of Federated Identity Management (FIdM) in 5G networks, where the heterogeneous nature of 5G poses challenges for service access and security. FIdM, particularly through Single Sign-On (SSO), can simplify user access across multiple service providers while addressing key security concerns such as authentication, authorization, and privacy. The paper proposes a Network Service Federated Identity (NS-

FId) model, designed to complement the 5G Service-Based Architecture (SBA), offering a seamless, secure user experience across diverse 5G services [13].

4.1. Network Service Federated Identity Protocol

The NS-FId protocol enables seamless service authorization in 5G networks by utilizing federated identity management. It allows users to access multiple services across different domains with a single set of credentials, streamlining authentication and improving the user experience [14].

Adapting NS-FId for legacy IoT devices, which often lack advanced security and standardized authentication methods, presents challenges. However, federated identity management can provide a unified authentication framework that enhances security without requiring extensive hardware upgrades. Implementing protocols like NS-FId allows legacy IoT devices to securely participate in modern 5G services, improving both security and interoperability [14].

4.2. Multi-level Authentication

Federated identity management enhances IoT security in 5G networks through multi-level authentication, complementing existing security mechanisms. This approach simplifies access to multiple services across domains with a single set of credentials, reducing the need for repeated logins. By supporting mutual authentication, authorization, and secure access, protocols like NS-FId ensure that appropriate security measures are applied at every level of the network and application [14].

4.3. Integration with 5G Infrastructure

Integrating federated identity management into 5G core network functions, particularly the Unified Data Management (UDM) system, improves user authentication and service access. The UDM manages user data and profiles, and its compatibility with federated identity management systems is vital for seamless authentication across multiple service providers. Federated servers store user data, which assists Identity Providers (IdPs) in implementing federated identity processes, working in tandem with the data stored in the UDM. This integration allows users to authenticate through various access points using credentials such as user IDs, cryptographic keys, digital signatures, or certificates. Once authenticated, services like identity verification, access control, and attribute sharing are enabled through a unified framework, enhancing security and the user experience [14].

5. IMPLEMENTATION CONSIDERATIONS

5.1. Device Registration Process

Registering legacy IoT devices using FID in a 5G network involves several steps [15]:

1. **Device Identification**: Assign a unique identifier to each IoT device to distinguish it within the network.
2. **Credential Generation**: Generate a set of credentials for the device, which may include certificates or keys, to facilitate secure authentication.
3. **Federated Identity Association**: Associate the device's credentials with a federated identity provider, enabling the device to authenticate across multiple services without managing separate credentials for each.
4. **Registration with 5G Network**: Register the device with the 5G network, ensuring that the device's federated identity is recognized and trusted by the network's authentication framework.

This process ensures that legacy IoT devices can securely and efficiently integrate into 5G networks.

5.2. Security Measures

Implementing additional measures such as temporary identities and encryption can significantly strengthen this process.

- **Temporary Identities**: Assigning temporary identities to IoT devices helps protect their permanent identifiers from potential tracking or spoofing. These temporary identifiers are valid only for a limited duration or specific session, reducing the risk of unauthorized access. By frequently updating these identities, the network minimizes the chances of identity-based attacks [16].
- **Encryption**: Employing robust encryption techniques ensures that data transmitted between IoT devices and the network remains confidential and tamper-proof. End-to-end encryption safeguards the integrity of the data, making it inaccessible to unauthorized entities. This is particularly important in IoT ecosystems where sensitive information is frequently exchanged.

5.3. Challenges and Limitations

Implementing FID for legacy IoT devices in 5G networks presents several challenges and limitations, particularly concerning device capabilities and necessary infrastructure updates.

- **Device Capability Limitations**: Legacy IoT devices often possess limited computational resources, making it difficult to support the complex

cryptographic operations required for FID protocols. Additionally, these devices may lack the necessary firmware or hardware support to integrate with modern identity management systems, posing significant obstacles to seamless FID implementation [17].

- **Infrastructure Updates**: Adopting FID necessitates substantial updates to existing network infrastructure. This includes deploying new identity providers, updating authentication servers, and ensuring compatibility across various network components. Such overhauls can be resource-intensive and may disrupt current services during the transition period.
- **Support for Devices without SIM Cards and 3GPP Credentials**: Despite these challenges, FID offers a viable solution for authenticating IoT devices that lack SIM cards or 3GPP credentials. By leveraging alternative authentication mechanisms, such as digital certificates or pre-shared keys, FID can establish trust relationships between devices and network services without relying on traditional SIM-based authentication. This flexibility is particularly beneficial for integrating a diverse range of IoT devices into 5G networks, enhancing scalability and interoperability [18].

6. CONCLUSIONS

Using FID to authenticate legacy IoT devices in 5G networks brings major benefits. It improves security with stronger authentication and helps manage large numbers of devices more easily. FID also supports devices without SIM cards or traditional credentials, allowing more IoT devices to connect to 5G networks smoothly.

However, there are challenges. Many older devices lack the capabilities needed, and upgrading infrastructure can be costly. Overcoming these issues is key to making FID widely usable.

Future efforts should focus on creating lightweight FID systems for devices with limited power and processing. Setting universal standards will ensure different devices and networks work well together. Strengthening security with better encryption and temporary IDs can further protect the system. By tackling these challenges, FID can become a reliable solution for secure, scalable IoT authentication in 5G networks.

REFERENCES

[1] Fontes, F., Freitas, M., and Calé, R. Heading to a successful private digital convergence. Technical report. Altice Labs.

[2] Korucuoglu, I. The impact of 5g on iot security: challenges and opportunities.

[3] Monem, M. A. Why eap protocol is used in 5g security?

[4] CableLabs A comparative introduction of 4g and 5g authentication. Technical report. Cable Labs.

[5] Ren, X., Cao, J., Li, H., and Zhang, Y. Novel authentication protocols tailored for ambient iot devices in 3gpp 5g networks. *arXiv (Cornell University)* , **?**

[6] Okta, I. What is federated identity?

[7] Santos, M. L. B. A., Carneiro, J. C., Franco, A. M. R., Teixeira, F. A., Henriques, M. A. A., and Oliveira, L. B. A federated lightweight authentication protocol for the internet of things. *arXiv (Cornell University)* , **?**

[8] Cervantes, R. The impact of 5g on network security and iot.

[9] Sign, G. Iot device security.

[10] Castle, W. What is the impact of 5g on iot scalability?

[11] Testbed, I. g. I. Internet of things (iot) integration: Identifying blockages and optimizing resource allocation in 5g/6g networks.

[12] Santos, B., Do, V. T., Feng, B., and van Do, T. Towards a standardized identity federation for internet of things in 5g networks. *2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pp. 2082–2088.

[13] Edris, E., Aiash, M., and Loo, J. The case for federated identity management in 5g communications, . 06.

[14] Kiyemba Edris, E. K., Aiash, M., and Loo, J. K.-K. Network service federated identity (ns- fid) protocol for service authorization in 5g network. *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, pp. 128–135.

[15] Mahapatra, B., Singh, V., Bhattacharjee, R., and Srinivasan, C. R. Ml-aka: an authentication protocol for non-standalone 5g-based c-iot networks. *Designs*, **8**, 128.

[16] Mitchell, G. 5G anonymity and the SUCI - mpirical.

[17] Lagutin, D., Kortesniemi, Y., Fotiou, N., and Siris, V. A. Enabling Decentralised Identifiers and Verifiable Credentials for Constrained IoT Devices using OAuth-based Delegation. *Workshop on Decentralized IoT Systems and Security (DISS)* , **?**

[18] Weidenfeller, T. and Bausch, C. Cross-domain identity of things - Ericsson Technology.