Computer Communications 216 (2024) 324–345

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

eSIM and blockchain integrated secure zero-touch provisioning for autonomous cellular-IoTs in 5G networks

Prabhakar Krishnan [a], Kurunandan Jain [a], Shivananda R. Poojara [b,*], Satish Narayana Srirama [c], Tulika Pandey [d], Rajkumar Buyya [e]

[a] *Center for Cybersecurity Systems and Networks, Amrita Vishwa Vidyapeetham, Amritapuri-campus, India*
[b] *Institute of Computer Science, University of Tartu, Tartu, Estonia*
[c] *School of Computer and Information Sciences, The University of Hyderabad, Hyderabad, India*
[d] *Research and Development in Cybersecurity, Ministry of Electronics and Information Technology, Government of India, India*
[e] *Cloud Computing and Distributed Systems (CLOUDS) Lab, School of Computing and Information Systems, The University of Melbourne, Australia*

ARTICLE INFO

Keywords:
Zero-touch service provisioning (ZTP)
Autonomous IoT (AIoT)
Zero-touch networks
Embedded SIM (eSIM)
Blockchain
Software defined networking (SDN)
Remote SIM provisioning

ABSTRACT

The growth of the Internet of Things (IoT) paradigm has resulted in a proliferation of connected devices and their applications. *Autonomous IoT* (AIoT) refers to a network of interconnected devices that operate without human intervention, making decisions and performing tasks autonomously. Traditional methods of provisioning IoT devices, such as manual configuration and over-the-air updates, are error-prone and insecure. The emergence of eSIMs (embedded SIMs) provides a viable solution for secure and flexible identity management in IoT devices. This work implements a low-cost, zero-touch remote provisioning system using GSMA standard Over-The-Air (OTA) IoT-SAFE protocol. This research predicts that future IoT devices will be eSIM-enabled, which are simple to configure, provision, validate profiles, and check security policies remotely. IoT onboarding processes are designed where blockchains are used to verify immutable repositories to store this network manifests, verifiable by Ethereum smart contracts. The integrated framework combines blockchain contracts, eSIM-based remote SIM provisioning through IoT-SAFE protocol, and SDN to manage IoT ecosystems' security. The proposed solution is evaluated using simulations and security analysis, and it demonstrates its feasibility at scale and resilience to attacks even under insecure environments. When compared with the baseline IEEE 802.15.4 protocol, our SDN-based Remote-SIM provisioning system (SIeSIM) reduces overhead to about 240 ms Time-To-Provision (TTP), outperforming manual provisioning by nearly 320 % and 210 % compared to expert provisioning in terms of TTP performances, respectively.

1. Introduction

In the Internet of Things (IoT) environment, networks of interconnected devices communicate amongst themselves and exchange data. Networks based on IoTs are expanding rapidly, with more and more devices connected to the Internet daily. Commonly, devices in IoTs are equipped with tags or sensors that collect, store, and transmit information via networks where their management is typically achieved through centralized architectures [1]. Devices using IoTs have grown substantially and are expected to cross 25 billion by 2025 from 14.2 billion in 2019 [2]. Servers collect and analyze data in real-time from these devices. Due to this flaw, anyone may readily access these devices and do calculations in accordance with them. On these devices, end-users are mapped via protocols [3]. Appropriate users and IoT device authentications must consider service constraints in IoTs, as they cannot perform complex transactions or processes. User and device authentication mechanisms must also be scalable, trustworthy, and resistant to threats and assaults. Most authentication methods safeguard IoT devices but depend on centralized databases or servers. [4], which checks users, devices, and communication records in IoTs. The frequency of cyberattacks on IoT networks and devices has grown, with devastating results that can result in major risks. Most current security solutions in use rely on centralized infrastructure (like PKI), which is reliant on third-party service providers being trusted. The drawbacks of this strategy include a single point of failure (SPOF), many-to-one traffic, and restricted scalability. IoT devices frequently lack the same

* Corresponding author.
E-mail address: shivananda.poojara@ut.ee (S.R. Poojara).

https://doi.org/10.1016/j.comcom.2023.12.023
Received 5 June 2023; Received in revised form 18 December 2023; Accepted 18 December 2023
Available online 6 January 2024

authentication security measures as fully working on a computer node.

New IoT authentication methods that integrate with new IoT devices must be proposed, are completely suited to satisfy IoT needs, and are mostly independent of devices and architectures [5]. Secure, trusted connectivity of IoT nodes shall propel the IoT into the next growth stage. The growth path for cellular IoT connectivity is now expected that 98 % of enterprises want an end-to-end security solution that protects data integrity and confidentiality from IoT devices, and 72 % of enterprises consider device-to-cloud security an essential feature when selecting a solution. Trust frameworks and transparency will need to be woven into all IoT layers for our cities to dispel concerns and ensure these new technologies can help our smart cities thrive. The key issue to resolve is providing connectivity and zero-touch provisioning cost-effectively and securely. Identity and provisioning are crucial components of IoT security that enable secure communication between devices. The devices in IoTs rely on secure and reliable communication protocols to transmit and receive data, where device identifications and provisioning are crucial components of security or secure communications between devices. Autonomous IoT (AIoT) refers to a network of interconnected devices that operate without human intervention, making decisions and performing tasks autonomously. AIoT networks have numerous applications, including industrial automation, smart cities, and autonomous vehicles. Standard application layer protocols for the Internet of Things have recently undergone advancements, enhancements, and improvements. However, due to the dynamic nature of IoT applications, traditional and upgraded application layer protocols have not yet met their requirements. Autonomously adapting to changing conditions in the application, these protocols can become intelligent with the help of AI/ML [6]. One of the challenges in deploying AIoT networks is the secure provisioning of services to the devices.

Service provisioning refers to providing access to services, such as data, applications, and updates, to the devices. Traditional service provisioning mechanisms require human intervention, which can be time-consuming, costly, and error prone. Moreover, human intervention increases the risk of attacks and compromises the network’s security. The traditional SIM card-based approach for identity and provisioning in IoT devices is not suitable for the requirements of the IoT ecosystem. The emergence of eSIMs provides a viable solution for secure and flexible identity management in IoT devices. ESIMs are small; programmable chips soldered onto the circuit boards of devices. They are non-removable SIM cards allowing OTA (over-the-air) activations and management. eSIMs can be programmed with multiple profiles, thus allowing them to be used with different carriers or networks. eSIMs can also be remotely provisioned, activated, and managed, eliminating the need for physical SIMs cards and simplified supply chains. eSIM is also tamper-resistant and provides increased security compared to traditional SIM cards. eSIMs can be used in many domains, including programming M2M devices, enabling devices for IoTs independent of tethered smartphones, and changing operator profiles using remote sim provisioning. Thus, eSIMs can be applied in IoTs, consumer, and automotive applications.

Technically eSIMs can be used in several areas, including network authentications (managing connectivity and operator switching), device attestations (identifying and connecting to clouds), end-to-end encryptions (data encryptions), and data integrity (ensuring sign-on for future verifications) as depicted in Fig. 1.

SIM cards have mostly stayed the same since the introduction of 2G. Despite several convenience and security improvements, their identity management has also been static. Numerous IoT applications are essentially constrained by the necessity to link them to devices [7]. The combination of IoT and eSIM technology has significant engineering and scientific value since IoT applications need platforms to transfer data between heterogeneous devices. It intends to do away with the requirement for Subscriber Identity Module (SIM) cards in the context of IoT to provide safe communication to IoT devices. The mobile device’s circuit board can be configured with SIM profiles that contain identities and credentials using the more widely used embedded SIM (eSIM) technology [8]. Smartphones and other edge devices on the Internet of Things (IoT) are becoming more powerful computationally, but there are still times when it’s necessary to offload tasks to other devices. This is especially true for compute-intensive and energy-hungry operations like encryption/decryption and password/authentication management. Therefore, moving specific processing away from devices with limited resources (IoT) and onto more capable devices (cloud, edge servers) is necessary.

Because cloud services are delivered over a public network, they involve some anonymity and security risk. The authors describe case studies in smart healthcare, safety, and emergency response [9] and the

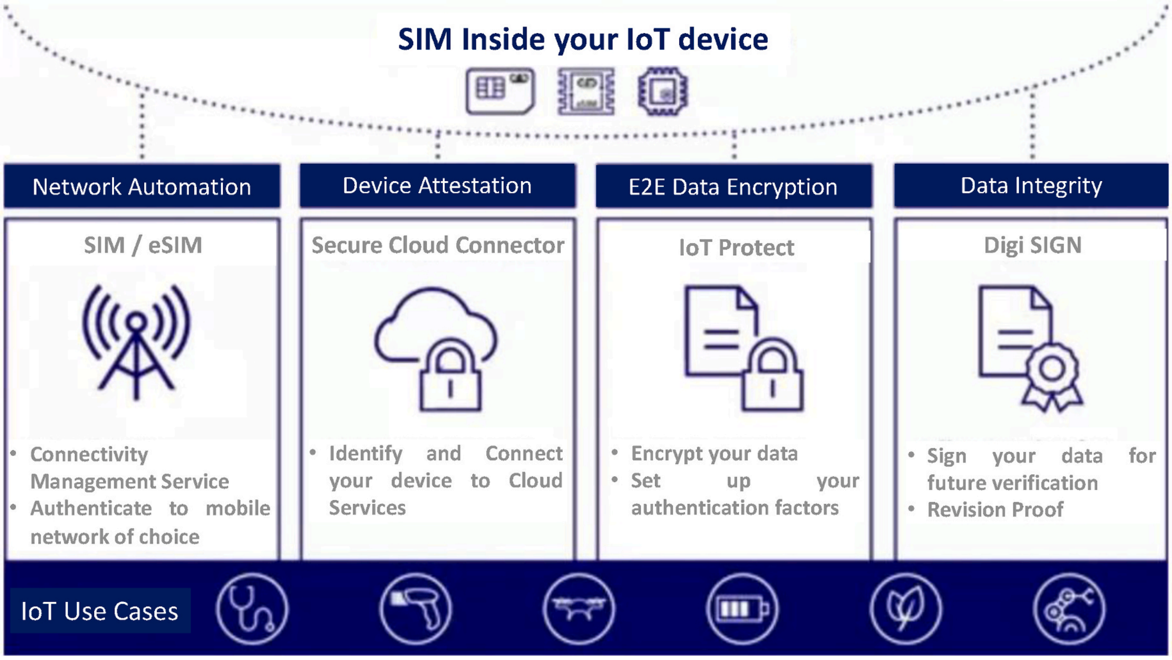
SIM Inside your IoT device
Network Automation
Device Attestation
E2E Data Encryption
Data Integrity
SIM / eSIM
Secure Cloud Connector
IoT Protect
Digi SIGN
• Connectivity Management Service
• Authenticate to mobile network of choice
• Identify and Connect your device to Cloud Services
• Encrypt your data
• Set up your authentication factors
• Sign your data for future verification
• Revision Proof
IoT Use Cases

Fig. 1. Applications of eSIM.

importance of machine learning and task-offloading strategies. eSIMs can be the safest and most trusted platform for offloading security processing tasks for IoT and mobile devices. Unlike conventional SIM cards, eSIMs are powerful embedded microcontroller-based chips with storage capacity and sufficient computation power that are permanent parts of devices. They are smaller than typical nano SIMs, can fit into tiny devices, and are assets to IoTs. The primary features of eSIMs increase the system's communication dependability and profile administrations remotely [10]. They can move network operators' information to new devices using eSIMs with assistance from Remote SIM Provisioning (RSP) infrastructures [11]. They use Zero-Touch Provisioning, which is easy, scalable, and economical [12]. The devices connect immediately to the nearest networks and download specific local profiles. This underlying feature offers a seamless communication process for heterogeneous devices deployed worldwide. The SIM profile contains security-critical information regarding the user credentials that the subscriber can access the mobile networks [13].

Therefore, secure transmission of the SIM profile to the mobile device is paramount. At the same time, unwanted exposure or tampering with such credentials could lead to eavesdropping, identity theft, billing fraud, and various privacy violations against mobile subscribers [14, 51]. This implies the need for careful designs and analyses of RSP protocols. Zero Touch architecture-based protections should not trust all devices while consistently verifying entities before granting access to them and avoiding data breaches. The layered architecture of the SDN-IoT ecosystem powered by blockchain is shown in Fig. 2. There is a definite need for programmable and reliably enforceable security protocols as significant business networks and critical infrastructure service providers for progressive deployments of IoTs. As seen in Fig. 2, SDN controllers manage network services while blockchains offer security and integrity and data transfers through SDNs. In peer-to-peer (P2P) and cloud (WAN) networks, servers, apps, hubs, switches/routers, items, or devices, including sensors, actuators, and hubs, are connected to improve resource management in networks employing IoTs. Blockchain-enabled SDN-IoT ecosystems' layered architecture aims to optimize Blockchain-based SDN frameworks. These environments comprise sensors and gadgets that sense data in real time and communicate it to the next sub-layers. Higher-energy CHs receive data from forwarding devices (switches, routers, phones, and storage devices). The processes are managed by Access Points (APs), which transfer all detected data to SDNs. Data and control planes define Edge Layers in SDN settings. Data from IoT devices is sent through standard gateways (SDN-IoT gateways). Finally, data is received via IoT servers that include Blockchains. We propose two different Blockchains for the control layer and the data layer. Blockchain in the control layer contains the distributed flow rules and maintains the consistency of the flow rules of each cluster. In detail, the chain logs all the updates, thus resulting in a version control management system in the control layer. On the other hand, Blockchain in the data layer works differently. All the switches dump their flow rules in the chain sequentially and verify if they are maintaining the same rule set. If any of the switches do not dump the same rules, the record is not updated, and the switch is isolated from the environment. This isolation helps to identify a fault in the switch and to contain adversaries if the switch is compromised.

TinyML is one of the hottest trends in the embedded computing field right now, with 2.5 billion TinyML-enabled devices estimated to reach the market in the next decade and a projected market value exceeding $70 billion in just five years. Dubbed Tiny Machine Learning (TinyML), this upsurging research field proposes to democratize the use of Machine Learning (ML) and Deep Learning (DL) on frugal Microcontroller Units (MCUs). Traditionally, sensor data is offloaded onto models running on mobile devices or cloud servers. This is not suitable for time-critical sense-compute-actuation applications such as autonomous driving, robot control, and industrial control systems. TinyML allows offline and on-board inference without requiring data offloading or cloud-based inference. The rapid miniaturization of Machine Learning (ML) for low-powered processing has opened gateways to provide cognition at the extreme edge (E.g., sensors and actuators). It is desirable to enable onboard ML on microcontrollers, turning them from simple data harvesters to learning-enabled inference generators and on-device analytics for a variety of sensing modalities (vision, audio, motion, identification, etc.).

1.1. Problem statement

Security in IoTs is crucial for interactions. Customers must trust that their data will be secure against unauthorized users, manipulations, or other undesirable device actions. Thus, authentications are critical for IoTs that need customers to manually handle shared keys that guarantee the device's functionalities and safe connections. Most authentication options on these systems are more user centric. Devices can also authenticate via shared key methods across devices or OAuth2 techniques that are more user-friendly for humans/user authentications. However, attackers learn shared keys and device IDs for impersonations. The developments of solutions based on the Trusted Platform Module (TPM), which provides chains of trust, also face challenges. To avoid impersonation attacks and stop devices from providing data under the identity of another in the context of smart cities, it is essential to guarantee that device identifications are defined and automated. Communication equipment must be encrypted for secure channel communications and to ensure that data provided and received is the same, that is, unaltered.

To automate the bootstrap IoT devices and integrate them into the SIeSIM framework with Zero Touch Provisioning (ZTP) approach, this study suggests employing secure tokens, which offer identities, authentications, and secure communications. Solutions for provisions and authentications of multiple devices can be scaled without having to authenticate each one at a time using device pools. Moreover, devices can be authenticated with one another and authenticate multiple devices. This can guarantee safe storage, monitoring, and authentication of eSIMs; blockchains might offer secure and decentralized solutions for managing eSIMs registered on blockchain networks. Although their terms are open, digital certificates are frequently used to establish identification and authentication. Device provisioning is a laborious process involving identity, key provisioning, and device setups. Automated configuration checks can prevent incorrect forms, a common cause of security and privacy problems.

Embedded AI on microcontrollers is motivated by *applicability*, *independence from network infrastructure*, *security and privacy*, and *low deployment cost*.

- This brings the advantage that less data needs to be transmitted. Instead of sending raw data, only the results of predictions need to be sent. This way, data analytics can be performed directly on the IoT device with low latency and power requirements.
- Privacy-centric security systems: closed-loop sensor/actuation systems, single-purpose devices that don't need connectivity, just some smarts, devices that need a super-fast response time, such as a sensor on a motor detecting a problem and stopping it before it breaks.
- Build devices that use less power and respond ever more quickly. With actual learning on the chip, each sensor could become personalized to the ways in which the device runs in a particular environment.
- The security benefits of using local machine learning are considerable. After all, if you don't connect a device to the internet, you have a much smaller attack surface. That benefit goes hand in hand with privacy.

The proposed network architecture can be used by any IoT network deployment in cellular networks (LTE, 4G, 5G, and beyond networks) irrespective of the protocols and requires minimal procedural changes when adapting to eSIMs. This study suggests adopting the IoT-SAFE

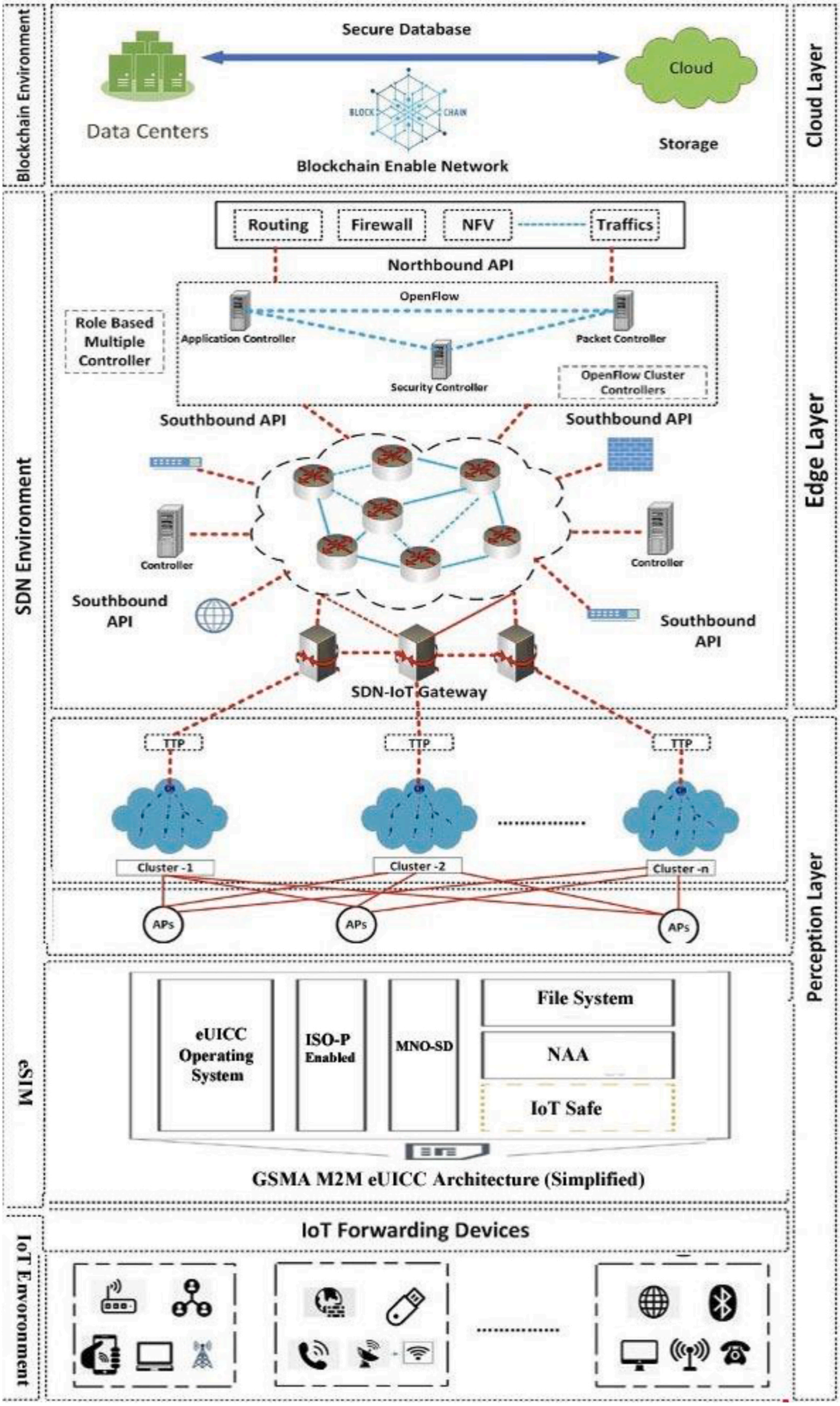

Fig. 2. Layered architecture of Blockchain-enabled SDN-IoT ecosystem.

protocol-based eSIM for zero-touch service provisioning in autonomous IoT to solve the issues with provisioning, secure registration, and authentication. The system is low-cost, zero-touch remote provisioning, making it easier to deploy and operate an IoT solution that is secure, scalable, and manageable over time. It helps solve the challenge of provisioning millions of IoT devices across an ecosystem by enabling provisioning and credential lifecycle management from a remote IoT security service. The proposed approach makes it possible for devices to be supplied safely and automatically without human involvement, guaranteeing that the network is secure.

1.2. Major contributions

- We present our systematic study and review of eSIMs and their usage in blockchains, device provisioning, and implementations of IoT SAFE protocol.
- layered hierarchy to deploy a distributed yet efficient Blockchain-enabled SDN-Cellular IoT framework.
- A novel authentication scheme for device provisioning in IoTs using eSIMs and blockchains is proposed.
- Informal and experimental security analysis shows that the proposed scheme can overcome security flaws and vulnerabilities to attacks in IoTs.
- Privacy-centric security systems: closed-loop sensor/actuation systems, single-purpose IoT devices that don't need connectivity, just some smarts, devices that need a super-fast response time. The security benefits of using local machine learning are considerable. After all, if you don't connect a device to the internet, you have a much smaller attack surface.
- Extensive Performance and comprehensive security, scalability analysis, and comparative experimental results in the state of the art are presented.

The rest of the paper is organized as follows: Section II introduces challenges in securing networks of IoTs. Section III presents the literature study and a discussion of the related works. Section IV illustrates the system architecture of the proposed scheme, which is described in detail. Section V shows the performance evaluation for the security of devices connected to IoTs. Section VI discusses the limitations and future scope. Section VII concludes the paper.

2. Background and motivation

2.1. eSIM technology

eSIMs are small and programmable chips soldered onto circuit boards of devices. They are non-removable SIMs that allow over-the-air (OTA) activations and management. eSIMs can be programmed with multiple profiles, enabling them to be used with different carriers or networks. eSIMs can also be remotely provisioned, activated, and managed, eliminating the need for physical SIM cards and simplifying supply chains. eSIMs are also tamper-resistant and provide increased security compared to traditional SIM cards. eSIM technology enables secure identity and large-scale connectivity orchestrations amongst nodes of IoTs. Device platforms in IoTs must also comply with GSMA IoT SAFE protocol, allowing the orchestration of secure communication channels between devices and servers at distant data centers or in Cloud infrastructures. IoT SAFE applets (applications) on IoT devices embed eSIMs, and devices are immediately and securely provided with apps as soon as they are turned on. IoT SAFE Security servers carry out secure provisioning. eSIMs can also be configured to perform various tasks (see Fig. 3). The programmable elements of eSIMs include reading files, implementing cryptographic procedures (Symmetric and Asymmetric), verifying signatures, generating key pairs, maintaining public/private keys, and generating randomized key values.

2.2. IoT SAFE protocol

Developed by the mobile industry, IoT SAFE (IoT SIM Applet For Secure End-2-End Communication) enables IoT device manufacturers and service providers to leverage the SIM as a robust, scalable, standardized hardware Root of Trust to protect IoT data communications. IoT SAFE Framework provides a standard mechanism to secure IoT data communications using a highly trusted SIM and a secure end-to-end solution for IoT device security, including secure provisioning. Fig. 4 displays IoT SAFE eSIM architecture and is explained below.

In the above figure, key GSMA IoT Security recommendations include utilizing 'Roots of Trust' in hardware to enable end-to-end, chip-cloud security and services. This necessitates the incorporation of both provisioning and the usage of security credentials into devices. Because they offer enhanced security and cryptography characteristics and are completely standardized secure components, eSIMs are ideally suited to operate as Roots of Trust in devices. This enables interoperability between vendors and consistencies of device deployment. IoT SAFE solution's SIM Applet, developed for mobile sectors for Secured End-2-End Communications, assists IoT device manufacturers and service providers to use SIMs as secure, scalable, standardized hardware Roots of Trust and protect IoT data in exchanges.

IoT SAFE provides standard ways to secure data transfers in IoTs using trustworthy SIMs rather than proprietary or less trusted hardware component devices. eSIMs are utilized inside the device as a small 'crypto-safe' to securely create a (D)TLS connection with a related application cloud/server that is compatible with eSIMs. The common API provides extremely secure eSIM for use as the 'Root of Trust' by IoT devices and assistance in deploying millions of IoT devices. IoT devices securely execute mutual (D)TLS authentication to a server using asymmetric or symmetric security algorithms, calculate shared secrets, protect long-term keys, and allow provisioning and credential lifecycle management via remote IoT security services. IoT SAFE's primary characteristics that enable the secure provisioning of IoT devices are as

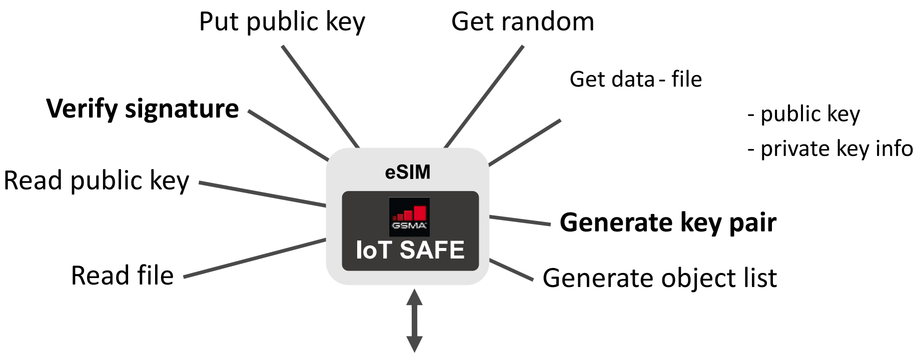

Fig. 3. eSIM Programmable elements.

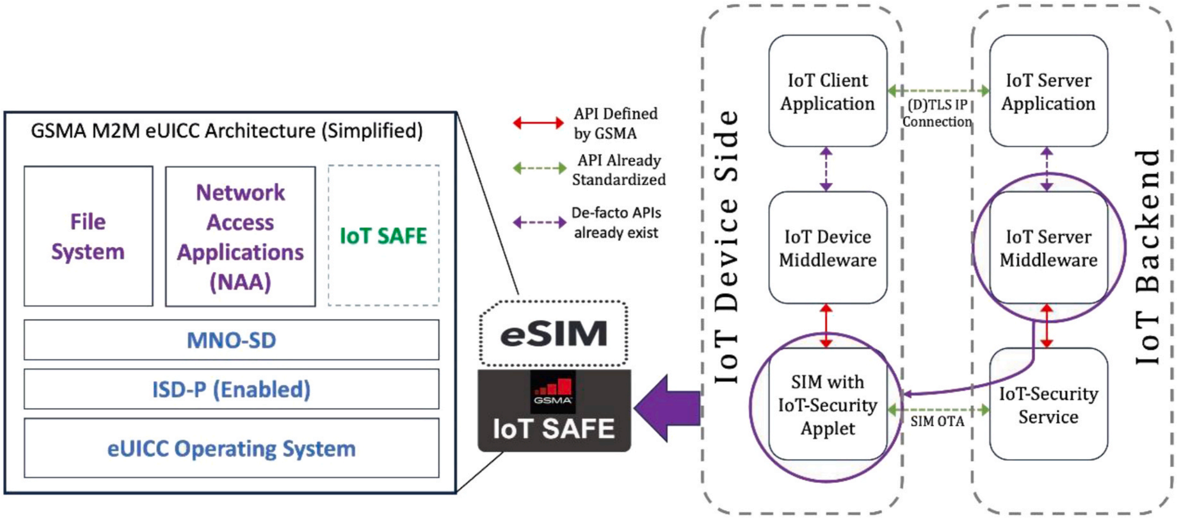

Fig. 4. IoT SAFE eSIM architecture

follows:

- Identity and access management: IoT SAFE creates secure communication channels between devices and the network, assigning each IoT device a distinct identity. This ensures that authorized devices can only access the network and that their exchange data is secure.
- Authentication and authorization: IoT SAFE offers robust techniques for preventing unauthorized access to IoT networks and devices. Digital keys, certificates, and other security measures are included to guarantee that only permitted parties may access the network and the data.
- OTA provisioning: IoT SAFE allows devices to be remotely set up and updated with security updates and firmware, thanks to OTA provisioning. This ensures that gadgets constantly use current security standards and are safe from dangers.
- Secure boot and firmware update: IoT SAFE provides secure boot and firmware update mechanisms that only authenticated and authorized firmware can be loaded onto devices. This prevents malicious firmware from being installed on devices and compromising their security.
- Secure storage and processing: IoT SAFE ensures that IoT data is securely stored and processed. This includes data encryption at rest and in transit, secure storage of encryption keys, and secure data processing.

Overall, IoT SAFE provides a comprehensive and robust security framework that enables the secure provisioning of IoT devices. By delivering unique identities, authentication and authorization mechanisms, OTA provisioning, secure boot and firmware update, and secure storage and processing, IoT SAFE ensures that IoT devices are protected against a wide range of security threats.

2.3. *eSIM-based secure identity and provisioning for IoT*

Earlier research has shown that eSIM can provide several benefits for IoT, including reduced complexity and cost of device management, improved security, and greater flexibility. The work in Ref. [1] found that eSIM can reduce the cost of device management by up to 50 % compared to traditional SIM card provisioning methods. The study also found that eSIM can improve security by providing enhanced tamper resistance and secure data exchange between devices and networks. eSIM can offer greater flexibility and scalability for IoT deployments, allowing network operators to quickly provision and manage many devices. The eSIM provides a viable, secure identity and provisioning solution in IoT devices. It enables secure, remote provisioning and activating IoT devices, eliminating the need for physical SIM cards. The eSIM also allows for flexible network selection and management, enabling IoT devices to connect to different networks depending on the location and availability of network coverage. eSIM-based identity and provisioning can also help address the challenges associated with IoT security. The eSIM enables secure authentication and identity management, which helps prevent unauthorized access and data breaches. The eSIM also allows for secure and encrypted communication between devices, which helps protect against data tampering and interception. The lightweight m2m communication protocol developed by Open Mobile Alliance (OMA) is an open standard for fulfilling the requirements of mobile low-power devices with very little processing power. This protocol is being rapidly accepted for device management and service activations amongst telecom carriers.

The deployment of TinyML eSIM-based IoT devices in the 5G/6G networks can have multiple approaches:

- Over-the-Air (OTA)Approaches. Flashing Over-the-Air (FOTA) updates are commonplace in resource-abundant situations, and there have been attempts to democratize TinyML in an OTA fashion. OTA updates provide the ability to resolve bugs and security vulnerabilities identified post-deployment or even support completely different functionality
- *F*ederated Learning model - the research in TinyML has led to breakthroughs in Reformable TinyML, i.e., TinyML solutions that can improve themselves via local or OTA updates. The edge devices update the parameters of a shared model on board, send the local versions of the updated model to a server, and receive a common and robust aggregated model without the data ever leaving the edge devices.
- Task Offloading: On/off-loading of computational tasks can be harnessed during edge-enabled machine learning scenarios. Such loading strategies should be an add-on to the existing dynamic configuration of edge-aware specifics. By doing so, TinyML can empower the transfer of resource-intensive jobs from the resource-frugal edge devices.

The profiles used on SIMs can be provided in many formats, including UXP, ASN.1, and even Excel spreadsheet, where UXP based on XML is the most often used format. The language is called SIM Profile Mark-up Language. SM-DP is a platform for storing and delivering digital eSIM Profiles. The platform protects Profiles using Profile Protection Keys, which are maintained in a repository and are associated with

Endpoint Identifiers (EID). SM-DP + binds these supported Profiles to their corresponding EID and securely downloads them to the associated eUICC's Local Profile Assistant (LPA). SM-DP also executes Remote Profile Management activities, such as profile enabled, disabled, or deleted remotely. LPA of eSIMs is a digitalized solution. LPAs are functional components that offer the LPD (Local Profile Download), LDS (Local Discovery Server), and LUI (Local User Interface) capabilities in Devices (LPAd) or the eUICC (LPAe). These capabilities are necessary to ensure that the device supports the Discovery server function and the Profile Download in the eUICC and that the user may manage their eSIM through the interface on the device. The Device is a user equipment that connects to a mobile network via an eUICC. Remote SIM Provisioning can be a smartphone or a handset, but it can also be a companion device that depends on the capabilities of the primary device. Fig. 5 depicts the architecture of the provisioning of eSIMs.

2.4. Blockchain integrated secure zero-touch service provisioning

Blockchain-based eSIM management for IoT provisioning is a decentralized approach to eSIM management that uses blockchain technology to provide secure storage, tracking, and authentication of eSIMs. Each eSIM is registered on a blockchain network, which allows for secure and tamper-proof storage and monitoring of the eSIM throughout its lifecycle. Blockchain-based eSIM management provides several benefits for IoT provisioning. First, it provides a secure and decentralized solution for eSIM management, reducing the risk of centralized attacks or data breaches. Second, it allows for more efficient and secure tracking of eSIMs throughout their lifecycle, reducing the risk of lost or stolen eSIMs. Finally, it provides a more transparent and auditable solution for eSIM management, allowing for greater accountability and traceability. However, there are also some challenges associated with blockchain-based eSIM management. For example, blockchain networks can be slow and require significant computational resources, which could affect the speed and efficiency of eSIM provisioning. Additionally, the decentralized nature of blockchain networks can make it challenging to coordinate and manage eSIMs across different network operators and service providers. The goal for managing the overall IoT device life cycle is to set up each IoT device (short-range and long-range) to communicate with its intended destination. The installation and configuration of each IoT device and actuator is a painfully long experience that requires field specialists' significant efforts and technical knowledge. The IoT device manual provisioning process is executed in stages when the IoT device arrives on-site: (1) Technicians install and turn on the IoT device; Manual configuration and provisioning of devices are done; IT backend accepts IoT device credentials manually and connects to the device management system; IoT device starts working and configures devices for provisioning. Zero Touch helps reduce human errors and delays during the deployment of Io devices. It also reduces travel costs and workforce requirements and allows field technicians to focus on other operational tasks like preventive and reactive maintenance work.

The Zero-Touch feature is attractive because the IoT devices are automatically installed without needing a specialized IoT technician to be available in the field. Therefore, Zero Touch can streamline IoT devices' installation and commissioning process. For example, when a new IoT device is installed, such as a thermostat, the user switches it on and connects to the environment. The device network automatically verifies the service pre-loaded into IoT devices. On verification of the service and required authorization, the platform starts measuring dataflows based on the usage of the IoT device, and the service enabled in the IoT device gets integrated into the e-service provider's network system. Zero Touch saves time, effort, and cost, making it a highly desirable solution that benefits industries that depend on IoT, including the oil and gas sector, smart buildings, smart factories, smart airports, and smart cities. Zero Touch helps reduce human errors and delays during the deployment of IoT devices. It also reduces travel costs and workforce requirements and allows field technicians to focus on other operational tasks like preventive and reactive maintenance. The Zero-Touch feature is attractive because the IoT devices are automatically installed without needing a specialized IoT technician who has pre-loaded the IoT device during the manufacturing stage. After verification of the service and required authorization, the environment starts measuring dataflows based on the usage of the IoT device, and the service enabled in the IoT device gets integrated into the billing system of the service provider's network.

2.5. Challenges of using eSIMs for securing IoTs

eSIMs-based identities and provisioning present opportunities for innovations and growth of ecosystems using IoTs. For example, eSIMs can enable new business models and revenue streams for service providers like pay-on-use subscriptions and dynamic network selections. eSIMs also facilitate adopting new applications in IoTs, like connected vehicles and smart homes or cities. A study by ENISA (European Union Agency for Cybersecurity) dives deep into eSIM technology's security

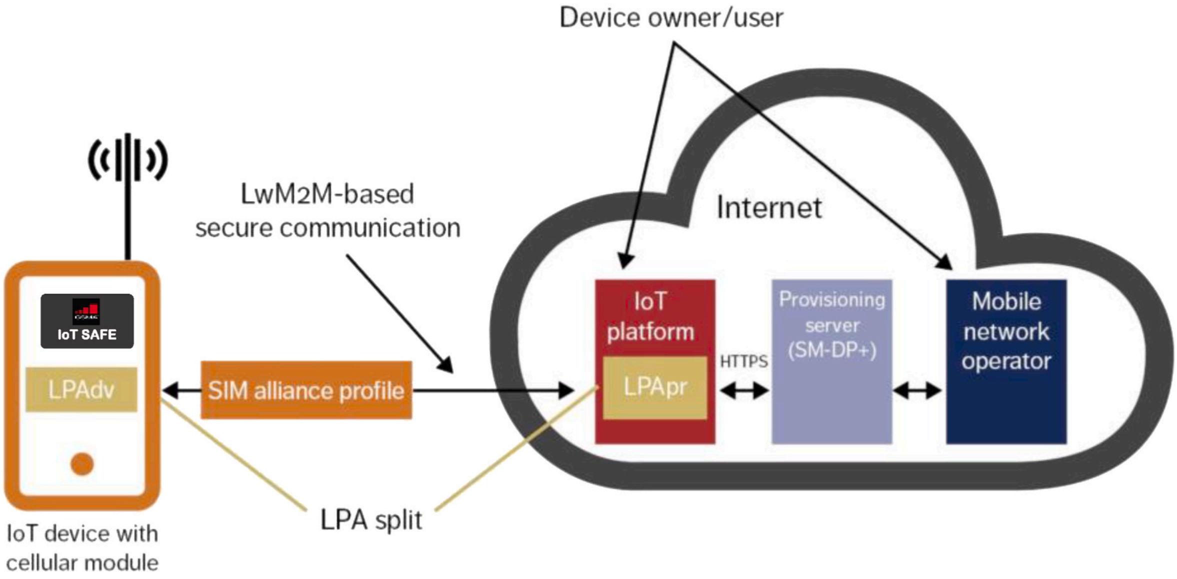

Fig. 5. Architecture of eSIM provisioning.

challenges. The report identified challenges associated with software attacks like bloated and locked profile assaults, memory exhaustion and undersized memory exploits, and eSIM swapping. Cybercriminals have the potential to disrupt services or obtain confidential data. Even though there have only been a few recorded cybersecurity issues, widespread IoT deployments and the associated growth in the usage of eSIMs might cause an increase in cyber events. Significant problems in the provisioning and administration of devices, which may be time-consuming and expensive, are the root of IoT implementations. A difficulty to be considered in security designs is the secure provisioning of services to devices, where service provisioning refers to procedures for granting access to services, including data, applications, and updates to devices. Traditional service provisioning mechanisms require human interventions, which can be time-consuming, costly, and error prone. Moreover, human intervention increases the risk of attacks and compromises the security of networks. eSIMs are considered an alternative to stem these issues. Another critical challenge in the use of eSIMs is a common standard. Lack of standardization in eSIM technology can lead to interoperability issues between different devices and networks. Securing reliable OTA management requires robust security protocols and infrastructures, which can be complex to achieve in remote or challenging environments.

2.6. SDN orchestration and IoT device lifecycle management

The integration of Software-Defined Networking (SDN) orchestration and IoT lifecycle monitoring offers several benefits that significantly contribute to the overall performance and efficiency of IoT systems:

- **Dynamic Network Management:** SDN allows for centralized management and control of network resources. By integrating SDN with IoT lifecycle monitoring, you gain the ability to dynamically allocate and optimize network resources based on real-time IoT device demands. This flexibility ensures efficient network utilization, enhancing overall performance.
- **Traffic Segmentation and Prioritization**: SDN enables traffic segmentation and prioritization. Integrating it with IoT lifecycle monitoring allows identifying and prioritizing IoT-related traffic. Critical data from IoT devices can be given higher priority, ensuring smoother and more efficient communication.
- **Enhanced Security**: With SDN, security policies can be centrally managed and enforced across the network. When combined with IoT lifecycle monitoring, detecting anomalies or potential security threats in IoT devices becomes easier. This integration allows quicker responses to security breaches or policy violations, bolstering overall system security and efficiency.
- **Optimized Resource Allocation**: IoT lifecycle monitoring provides insights into the behavior and performance of IoT devices throughout their lifecycle. Integrating this information with SDN allows for more informed decisions on resource allocation. For example, resources can be dynamically allocated based on device behavior patterns to optimize performance and efficiency.
- **Scalability and Flexibility**: SDN's agility in reconfiguring networks aligns well with the dynamic nature of IoT ecosystems. The integration allows for scalability as IoT device numbers grow or change. This adaptability ensures that network resources can be efficiently adjusted to accommodate new devices without compromising performance.
- **Proactive Maintenance**: Potential issues or failures can be predicted by monitoring the IoT device lifecycle. When integrated with SDN, this data enables proactive maintenance and resource allocation adjustments to prevent or minimize downtime. It ensures that the network is continuously optimized for performance.

In summary, the integration of SDN orchestration and IoT lifecycle monitoring synergizes network management with device behavior insights. This results in a more efficient, responsive, and adaptable network that can handle the dynamic demands of IoT ecosystems, ultimately enhancing overall system performance and efficiency.

3. Review of related work

Several prior works have proposed solutions to address the challenges of secure service provisioning in AIoT networks. Some have suggested solutions based on Public Key Infrastructure (PKI), which enables secure authentication and encrypting messages between devices. However, PKI-based solutions may need to be more scalable and efficient, as they require a centralized authority to manage the keys and certificates. Other studies have proposed solutions based on blockchain technology, which enables decentralized and secure communication and storage of data. However, blockchain-based solutions may be too complex and resource-intensive for AIoT networks, as they require significant computational resources and may introduce latency in the communication between devices. The usage of eSIMs in applications of IoTs is a rapidly developing area of research. eSIMs are generic terms used for eSIMs housed on small chips that offer digital storage for mobile subscribers. These SIMs can be used to identify subscribers in various goods, such as wearable technology, PCs, security systems, and mobile operator networks. POS (point-of-sale) devices and IoTs. Studies have shown that eSIM can provide several benefits for IoTs, including reduced complexity and cost of device management, improved security, and greater flexibility. The researchers in Ref. [15] detailed the developments of eSIMs as roles and trust amongst telecom organizations. The study outlined several gaps in the repartitioning of responsibilities between telecom operators and supply chains.

An architecture employing eSIM and the advantages of using eSIMs in IoTs were examined in the study [16]. Emergency calling systems ushered in a new era of connectivity in automobiles. They support a wide range of applications, including managing temperatures inside cars, fuel alarms, alternate route navigations, vehicle tracking, security alarms, and driving information. eSIMs-linked automobiles were studied in Ref. [17]. Although using eSIMs looks simpler for customers, increasing their market shares is not guaranteed. The study in Ref. [18] assessed if consumer eSIM solutions for smart products were feasible. Distribution centers might connect intelligent items to private networks and get specialized services. The study's experiments for smart product switching across IoT networks were successful. The study found that local eSIM operations with pre-loaded profiles minimized service outages and were favored over regular M2M eSIMs that needed OTA signaling.

To increase effectiveness, subscribers' personal information was stored with service providers instead of eSIM. The study in Ref. [19] focused on eSIMs. eSIMs allow consumers to switch carriers without physically moving, making it beneficial to security systems. Since information theft can occur, systems must impose strict evaluations and differentiations of IoT and non-IoT devices. The study in Ref. [20] examined the effects of eSIM on the trust dynamics among telecom sector players. To promote the use of eSIM technology, the research identified several gaps in repartitioning duties between operators and providers based on real-world instances.

Blockchains are distributed, unchangeable ledgers that make it easier to record transactions and monitor assets in commercial networks. Intangible assets, such as intellectual property, patents, copyrights, and trademarks, can be as tangible as a house, vehicle, cash, or land. On blockchain networks, almost anything of value may be recorded and sold, lowering risk and increasing efficiency. Businesses depend on the information, and timely and accurate information retrieval enables smarter judgments. Blockchains are the right technologies for delivering secure information because they offer instant, shareable, and fully transparent data recorded on immutable ledgers that network users can only view with permission. Among other things, a blockchain network can monitor orders, payments, accounts, and production. Blockchains can be operated in permission or non-permission modes. IoT devices are mere players in blockchains or smart contracts with access via Edge switches. The gateways for devices in IoTs save manifests for devices' networks which are then used to control blockchain deployments. In SDN-enabled Pervasive Edge Computing (PEC) environments, blockchains are used for authenticating identities of IoT devices [21] and introduce distributed security platforms with edge clouds and SDN capabilities.

To track the resource usage of IoT devices, EdgeChains in Ref. [22] used a "credit-based resource management" architecture underpinned by static criteria (such as "priority, application type, access pattern history"). Device-to-device communications were recorded and stored on blockchains to protect the Internet of Things. In Ref. [23], a blockchain-based IoT device identity authentication system was proposed. Blockchains stored information on device identities, and the Blockchain of Things (BCoT) Gateways recommended in the study could record authorized transactions. To determine device models, the study looked at traffic patterns. Existing solutions do not support intelligent control in IoT settings because they rely on specific controllers or programs to control IoT devices remotely.

A viable alternative is using a single gateway device, like a smartphone, to manage many IoT devices. However, it might be challenging to ensure security when handling the management of IoT devices. SDN-enabled gateways [24] provide dynamic network traffic flow managements that support defense mechanisms against assaults by identifying and preventing suspicious network traffic flows. A developing IoT network might be jeopardized by poorly managed devices and flawed firmware upgrades, and eSIMs combined with other IoT devices are becoming increasingly popular. IoT SENTINEL was created in Ref. [25] to identify various IP-based IoT device types connected to networks. This study's device model and software version establish the kind of device, and passive network traffic monitoring was used to identify the device type. For feature engineering, a total of 23 packet characteristics—all of which were generated from encrypted data and independent of packet content—were used. According to the author, the recommended method can correctly identify devices with little overhead.

In a smart grid for device management, IoT devices are identified and registered using blockchain [26]. The consensus was also investigated in the system. Based on transactions that users upload to blockchains, hackers may use machine learning techniques to de-anonymize them. Obfuscations anonymize user identities based on transaction histories in blockchain-based IoT applications since IoT devices execute transactions in timely patterns, and obfuscations of timestamps are utilized to disrupt these unwanted patterns, resulting in reduced informed and blind assaults [27]. Blockchains created distributed authentication systems in which smart contracts stored users' wallet addresses and IDs to enable login to apps following authentications. This process took a bit longer than usual because of the volume of transactions on Ethereum. According to testing results, the suggested technique was highly effective at preventing attacks like man-in-the-middle, impersonation, replay, and denial-of-service (DoS) [28].

To address these security issues and improve the robustness of the 5G network, authors of [47] introduced the Secure Blockchain-based Authentication and Key Agreement for 5G Networks (5GSBA); using blockchain [52] as a distributed database, our 5GSBA decentralizes authentication functions from a centralized server to all base stations. It can prevent single-point-of-failure and increase the difficulty of DDoS attacks. In this article [48], the authors present a comprehensive intelligence and secure data analytics framework for 5G networks based on the convergence of Blockchain and AI named "Block5GIntell".

For Industrial IoT (IIoT), a private blockchain-based trusted anonymous access architecture [53]is recommended, where trusted access is supplied by three different types of SoftwareDefined Networking (SDN) controllers. A particular module is designed to offer a balanced trade-off between dependability, confidentiality, and efficiency within the system. In situations when there is heavy traffic, this module works better than traditional methods [29]. The study in Ref. [30] designed IoT security, including layers in design, namely, perception, network, and application. The study concentrated on current disadvantages in access control mechanisms which were indicators for IT companies to work on present authentication drawbacks and securing future IoT environments. NB-IoT (Narrow Band-Internet of Things) cellular wireless network standard, which fulfilled several critical IoT needs, as detailed in the book [31].

NB-IoT is stimulating the industry to develop new use cases and related products. The authors described how IoT devices (such as sensors) are designed to run anywhere and for more than ten years without maintenance, using NB-IoT's enhanced network coverage and exceptional power-saving capabilities. Industrial users may use the book to learn how to leverage NB-IoT capabilities for their IoT projects. Also included are additional system components (such as IoT cloud services) and embedded security issues. The author examines NB-IoT in-depth from the perspective of application engineering, concentrating on IoT device development. To decrease the computational complexity of security protocols in many IoT devices, a 5G Authentication and Key Agreement (AKA) protocol based on upgraded symmetric keys was presented in Ref. [32]. The improved version of Braekens' protocol was created to provide forward secrecy by modifying the shared key for low-cost Internet of Things devices. According to the research, the developed model was immune to the Linkability of Failure Messages (LFM). The protocol was nonetheless susceptible to DoS assaults. Platform architecture for deploying zero-touch Pervasive Artificial Intelligence-as-a-Service (PAIaaS) in services with blockchain smart contracts was proposed in Ref. [33].

The PAIaaS standardized Pervasive AI at all levels and unified the interfaces to facilitate service deployment across application and infrastructure domains. FL-as-a-service was used as a use case to evaluate the model's effectiveness. This showed the model's ability to self-optimize and adapt to the 6G network dynamics. However, the smart contract agents only gradually figured out the best course of action for delivering the service. The work in Ref. [34] demonstrated a blockchain-based, IoT-embedded voting D-App that is safe and anonymous. Privacy was safeguarded by preserving vote secrets and preventing corrupted authorities from forging votes. By achieving privacy and verifiability, the designed protocol was proven effective. In Ref. [35], a zero-touch management approach for IoT based on Digital Twin (DT) technology was proposed. DT was represented using ontologies and knowledge graphs, and IoT elements were mapped onto them.

The DT scheme offered a solution for the device management problem under zero-touch management through the example. However, zero-touch management still needs to optimize the networks, which might pose problems for IoT network provisioning. In the work in Ref. [36], a simple IoT device identity privacy method in a 5G network was implemented. The deployed algorithm, HashXor, only needed the IoT device to do two hash and three Xor operations. The examination of execution times showed that HashXor was computationally effective. However, IoT devices with insufficient resources were only subjected to light computation. In Ref. [37], a transparent third-party approach based on proxy-based federated authentications was suggested for cloud-edge federations. The transparency in the federated paradigm enables the edge and cloud operators to install the built proxy. According to experimental findings, federated edge-to-cloud and cloud-to-edge authentication using a proxy-based concatenation of authentication protocols can shorten authentication times. However, the third-party authentication made the system vulnerable to insider assaults. The work in Ref. [38] presented a low-cost client-side encryption method for secure IoT provisioning.

The strategy employed an inexpensive algorithm based on the Advanced Encryption Standard (AES) and ATECC608 tamper-resistant keys. According to the paper, the IoT device is securely provided to a cloud platform. But with the ATECC608, altering any secret keys may lead to further security problems. The SIM Profile Transparency Protocol (SPTP), developed in Ref. [39], aims to detect fraudulent SIM profile provisioning. The SPTP included the Private Index Calculator (PIC) and Transparency Ledger (T) for the authentication process. A security investigation showed subscriber privacy was offered based on IMSI permission. Due to the attestations' reliance on reliable notaries, the system architecture took time. For IoT devices with firmware, the work in Ref. [40] advocated provisioning, authentication, and secure communication techniques. To address this, the YubiAuthIoT identity management and authentication technique was created. The overall provisioning ran more slowly than usual. The model's flaw was that the IoT nodes weren't monitored once provided.

In summary, related works of eSIMs in IoT highlight improved security, reduced device complexity/costs, and remote management capabilities. Challenges in adopting eSIMs include interoperability and standardization issues, limited vendor support, and the complexity of IoTs. Blockchain technology provides several advantages, such as distributed consensus, tamper-proof records, and enhanced security. However, limitations that need to be addressed include the scalability and interoperability of blockchain-based solutions. In terms of provisioning: eSIMs, blockchains, and secure communication protocols provide m efficient security solutions. However, challenges stem from lightweight and efficient authentication protocols, greater interoperability, and network coordination. IoT SAFE protocol can provide end-to-end security for IoT devices, including secure provisioning.

Table 1
A summary of related works.

Publication	Key Focus	Key Findings
Almadhoun et al. [3]	Integration of blockchain for IoT security	• Presents IoT SAFE authentication protocol using blockchain for IoT • Decentralized trust and transparency benefits
Yadav, S. et al. [8]	IoT SAFE protocol architecture and features	• Presents the IoT SAFE protocol and its key features • Highlights secure identity management and authentication in the IoT SAFE architecture
Ahmed A et al. [12]	Security Analysis of the Remote SIM Provisioning	• Provides an in-depth analysis of IoT security challenges • Explores the application and benefits of the IoT SAFE framework in addressing IoT security concerns
Silva et al. [14]	IoT SAFE framework for secure IoT device lifecycle management	• Proposes an architecture for secure provisioning and management of IoT devices using IoT SAFE • Addresses secure bootstrapping, authentication, and secure communication in the IoT SAFE framework
Thatte et al. [16]	Opportunities and challenges of eSIM in IoT	• Discusses challenges of eSIM adoption in IoT • Privacy concerns and standardization challenges
Apilo et al. [18]	eSIM-Based Mobility Solutions for Advanced Smart Products	• Provides an in-depth analysis of Cellular IoT eSIM solutions • Explores the application and benefits of the IoT SAFE framework in mobile IoT devices
Gaber et al. [20]	Study on eSIM-IoT SAFE-based solution for Smart Cities	• Presents an experimental evaluation of IoT SAFE-based secure provisioning of IoT devices • Assesses the performance and security aspects of the provisioning process using IoT SAFE
Gong et al. [23]	Blockchain-based IoT Identify management	• Authentication framework with Blockchain for IoT Devices Identity • Benefits of immutability and distributed consensus in securing Identity and Management (IAM) processes

Table 1 provides a brief overview of the existing works in this field and explains the Key findings, limitations, or gaps that the proposed framework aims to address.

4. Proposed SIeSIM solution

The proposed SIeSIM solution is an integrated framework combining blockchains, eSIMs, IoT-SAFE protocol, and SDNs to manage the security of IoT ecosystems. Future IoT devices with eSIM are simple to set up, validate profiles, and check security policies. Blockchains are utilized in SIeSIM's IoT onboarding procedures, where Ethereum smart contracts may validate an immutable repository used to store network manifests. To control the security of IIoT ecosystems, the integrated framework incorporates Software-Defined Networking (SDN), eSIM-based remote SIM provisioning, and blockchain contracts. Fig. 6 depicts the workflow of the proposed scheme.

4.1. Approach to realizing the solution

Innovative approaches could lead to more efficient eSIM-based secure provisioning for IoT devices, and specific examples of the same are detailed below.

- **Blockchain-based eSIM management:** Using blockchain technology could provide a secure and decentralized solution for eSIM management. Each eSIM could be registered on a blockchain network, providing secure storage, tracking, and authentication of the eSIMs. This approach could reduce the need for a centralized eSIM management platform and provide a more secure and efficient solution.
- **Machine learning-based access control and Edge Gateway:** Machine learning algorithms could be used at the gateway (with heavy processing and communication resources) to analyze and learn access patterns of IoT devices, which could be used to establish access control policies. The resource-constrained 5G devices can offload more compute-intensive operations and security processing to the gateway or edge servers. This approach could provide more efficient and accurate access control by detecting and predicting access patterns, reducing the risk of unauthorized access.
- **Multi-party computation-based credential sharing:** Multi-party computation (MPC) could be used to share eSIM credentials securely among multiple devices. This approach would allow for more efficient and secure sharing of credentials without exposing the credentials to any individual device. This could reduce the risk of credential theft and provide a more efficient and secure method of credential sharing.
- **Artificial Intelligence on the Extreme Edge:** With the eSIM-empowered SoC on the IoT device, we enable onboard ML on microcontrollers, turning them from simple data harvesters to learning-enabled inference generators and on-device analytics for a variety of sensing modalities (vision, audio, motion, identification, etc.). The security and privacy benefits of using local machine learning are considerable.
- **Lightweight cryptography-based eSIM provisioning:** Lightweight cryptography algorithms could be used to reduce the computational burden of eSIM-based secure provisioning for IoT devices. Using more efficient and lightweight cryptography algorithms could make the eSIM provisioning process more efficient and faster, reducing the time and resources required for eSIM provisioning.

These potential approaches could lead to more efficient and secure eSIM-based secure provisioning for IoT devices. Further research and development in these areas will be necessary to determine their feasibility and effectiveness.

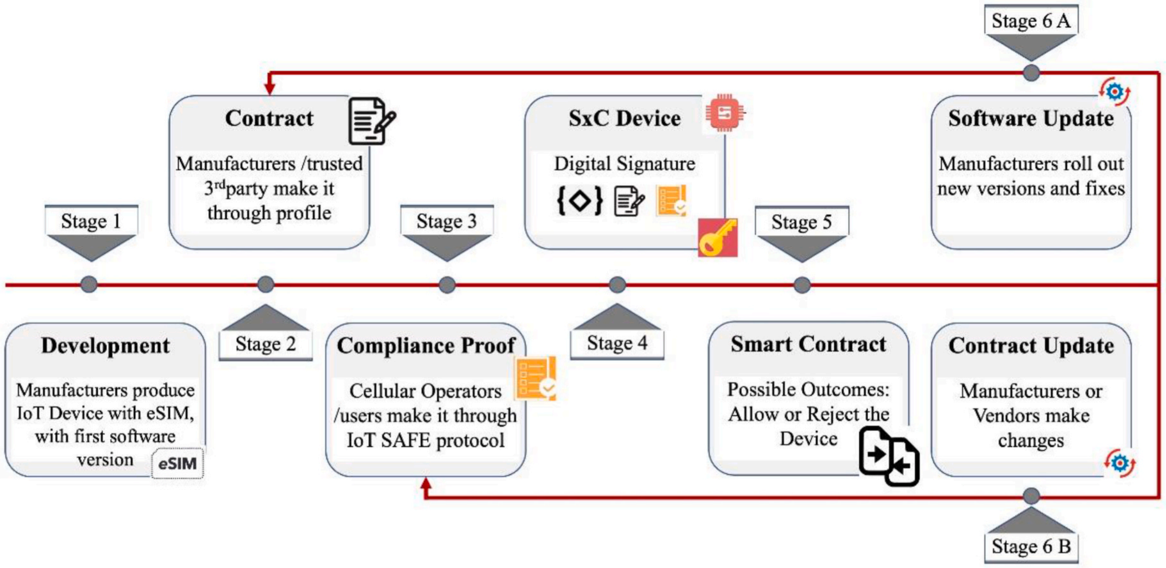
Stage 6 A
Contract
Manufacturers /trusted 3rdparty make it through profile
SxC Device
Digital Signature
Software Update
Manufacturers roll out new versions and fixes
Stage 1
Stage 3
Stage 5
Development
Manufacturers produce IoT Device with eSIM, with first software version
eSIM
Stage 2
Compliance Proof
Cellular Operators /users make it through IoT SAFE protocol
Stage 4
Smart Contract
Possible Outcomes: Allow or Reject the Device
Contract Update
Manufacturers or Vendors make changes
Stage 6 B

Fig. 6. Proposed workflow of SIeSIM Framework

4.2. Architecture

These potential approaches could lead to more efficient and secure eSIM-based secure provisioning for IoT devices. Further research and development in these areas will be necessary to determine their feasibility and effectiveness. This work's proposed architecture of the SIeSIM solution is depicted in Fig. 6 and detailed below. IoT devices have eSIMs that are IoT SAFE protocol enabled and implemented in their hardware. A new device connects to IoTs using their primary service provider, like Cellular service providers. The registrations and authentications of these devices on service providers are executed using blockchains running on SDNs. Controllers of SDNs are responsible for these connections and authorizations where corresponding service providers are connected to SDNs. Authorized devices are then registered, and provisioning happens. Once provisioned, these devices are monitored continuously, where the details are retrievable from blockchains. Unauthorized connections/intrusions are detected and avoided to stop network damage. The technological integration is built upon the modular identify service,

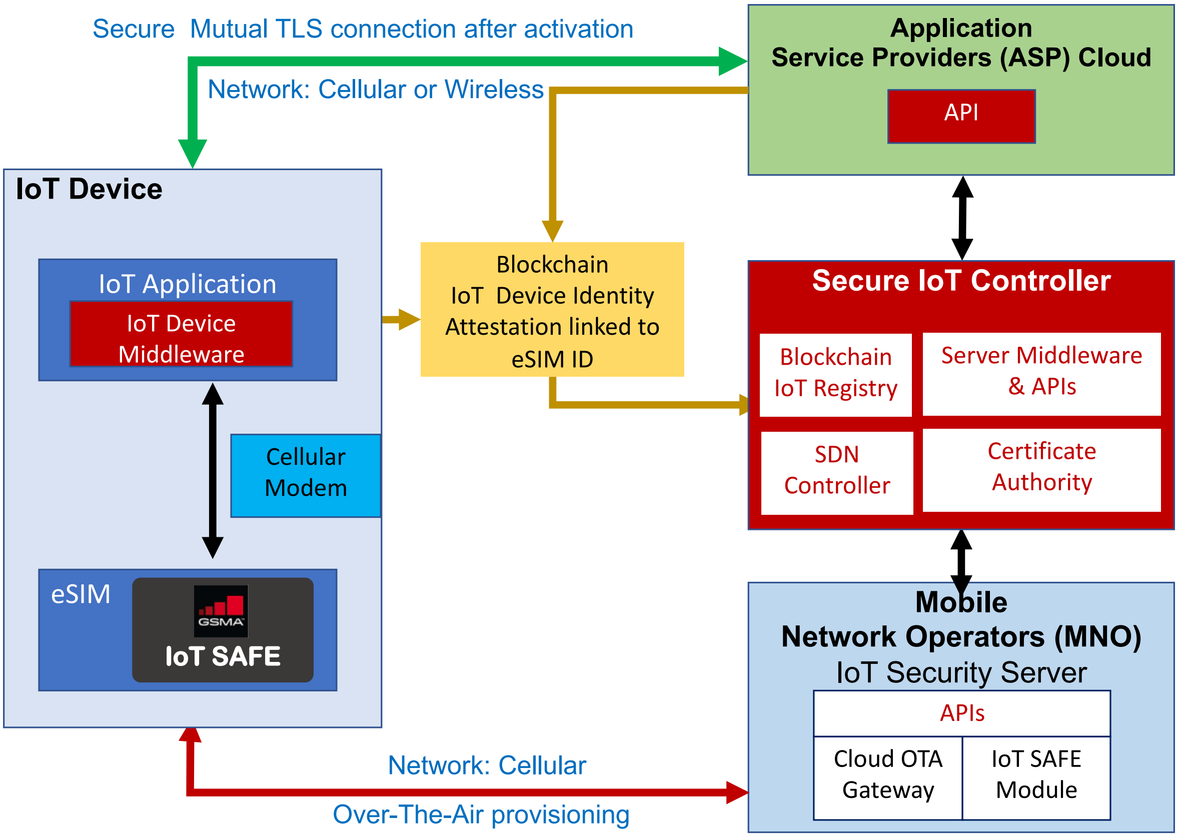

Fig. 7. Architecture of SIeSIM framework.

where we made use of the built-in certificate request clients in IETF RFC 7030 Enrollment over Secure Transport, ISO/IEC 11889 Trusted Platform Module (TPM), and PKCS#11 interface standards. Fig. 7 shows the architecture of the proposed scalable and secure zero-touch schema, known as the SIeSIM Framework.

How does it work? Thanks to the Secure IoT Registry with Blockchain, generic IoT devices can safely connect to the appropriate resources. The IoT Registry offers zero-touch IoT device registration, activation, deactivation, transfer, and deletion through digital certificates. A security applet on the eSIM creates and saves the public and private key pair on the SIM. To manage these certificates, we employ asymmetric keys. The private key never leaves the SIM. An IoT device securely registers to the relevant MNO and receives provisioning with the mobile network operator (MNO) profile when powered on for the first time. The IoT security applet receives a request to create a public/private key pair over the air. The MNO receives the public key and creates a certificate signing request. The ASP registers an IoT device by giving the eID, MNO id, and any other pertinent data. A registry payload is built using this data.

The registry payload is safely transferred to the IoT device thanks to establishing a trusted relationship with the MNO. The IoT device generates a fresh public/private key pair. The IoT registry receives the IoT device CSR from the MNO for signing. The MNO and the ASP receive the signed cert from the registry. The signed CERT is delivered to the IoT SIM by the MNO. The activation occurs when the ASP endpoint is created, the private/public key pair is generated, and the client certificate is sent to the eSIM.

In the SIeSIM Framework, eSIMs loaded with necessary profiles also have IoT SAFE installed on the attached device. On entering IoTs, they first contact their cellular service providers over the air, where the devices pass through an IoT security server with an IoT SAFE module installed. The machines are registered, activated, and provisioned through controllers of SDNs, which use blockchains or cloud service providers based on the networks the device connects to. The security controller verifies necessary elements of authorizations like digital certificates at the back end before devices can log on and access IoTs. The proposed architecture offers several advantages:

1. Improved security: ESIMs provide a secure identity and authentication mechanism for IoT devices, reducing the risk of unauthorized access and data breaches.
2. Simplified device management: The eSIM management platform allows for remote provisioning and management of the eSIMs, reducing manual intervention and simplifying device management.
3. Scalability: The architecture is highly scalable, allowing for deploying many IoT devices with eSIMs.
4. Standardization: The architecture can be implemented using standardized eSIM technology and protocols, ensuring interoperability and compatibility with other systems.

Overall, this architecture provides a comprehensive and robust framework for the secure provisioning of IoT devices using the IoT SAFE protocol and blockchain technology. By providing secure identity management, authentication and authorization, OTA provisioning, and secure storage and processing of data, the architecture ensures that IoT devices are protected against a wide range of security threats.

4.3. Overview of the Components

1. IoT devices with eSIMs: Each device is equipped with an eSIM, securely provisioned with the necessary credentials and certificates. The eSIM provides secure identity and authentication for the device, enabling it to communicate securely with other devices and cloud services.
2. eSIM management platform: The eSIM platform is responsible for securely provisioning and managing the eSIMs on IoT devices. It provides a secure interface for the device manufacturer or IoT service provider to remotely control the eSIMs, including updating credentials and certificates and managing access policies.
3. Security gateway: The security gateway acts as a secure intermediary between the IoT devices and the cloud services. It enforces access policies and provides secure communication between the devices and cloud services. The security gateway authenticates the devices using their eSIMs and provides secure end-to-end communication between them and cloud services.
4. SDNs: SDNs provide backend processing and storage for IoT data generated by devices. They also provide the necessary APIs for devices to communicate with SDNs securely.
5. IoT Device: This component represents the physical IoT device that needs to be securely provisioned. The device is equipped with an eSIM and securely communicates with the IoT platform using the IoT SAFE protocol.
6. IoT Platform: This component represents the cloud based IoT platform that manages IoT devices. The platform is responsible for securely provisioning the machines, managing their identities, and providing secure communication channels for data exchange.
7. IoT SAFE Services: This component provides the core security services required for secure IoT device provisioning, including device identity management, authentication and authorization, OTA provisioning, and secure storage and processing of data.
8. Blockchain: This component represents the distributed ledger technology that provides a tamper-proof record of device identities and transactions. The blockchain securely stores device identities and transaction history, ensuring the data cannot be modified or tampered with.
9. Identity and Access Management (IAM): This component provides an IoT platform's centralized identity and access management system. It manages the authentication and authorization of IoT devices, users, and applications and ensures that only authorized entities can access the IoT platform and data.
10. Security and Compliance: This component provides the necessary security and compliance controls to ensure the IoT platform and devices comply with relevant security and privacy regulations. This includes regular security assessments, vulnerability scanning, and compliance audits.

The security gateway provides a safe intermediary between IoT devices and cloud services. It enables a secure connection between the devices and cloud services and enforces access controls. The security gateway allows secure end-to-end communication between the devices and cloud services and authenticates the devices using their eSIMs.

4.4. Authentication and provisioning sequence

The fluxes between the various components are shown in Fig. 8. To confirm the endpoints' legitimacy when an IoT device wishes to connect with them, the Endpoint device has to be provisioned before any communications may be transmitted to Orion. The Endpoint devices (which may number in the multiples) are provided by the City Manager (root CA). The following device to be supplied is the user/company manager (sub-CA) overseeing and authenticating their subset of IoT devices. The user or enterprise management then provisions the IoT devices.

4.5. Profile activation

In eSIM, multiple profiles can be integrated into a single eSIM. By doing this, the user can switch carriers (i.e., Mobile Network Operators). The activation user profile is mathematically denoted as,

$$E_{user}[p_1, p_2, \ldots., p_n] \text{ or } p_q, q = 123\ldots., n \tag{1}$$

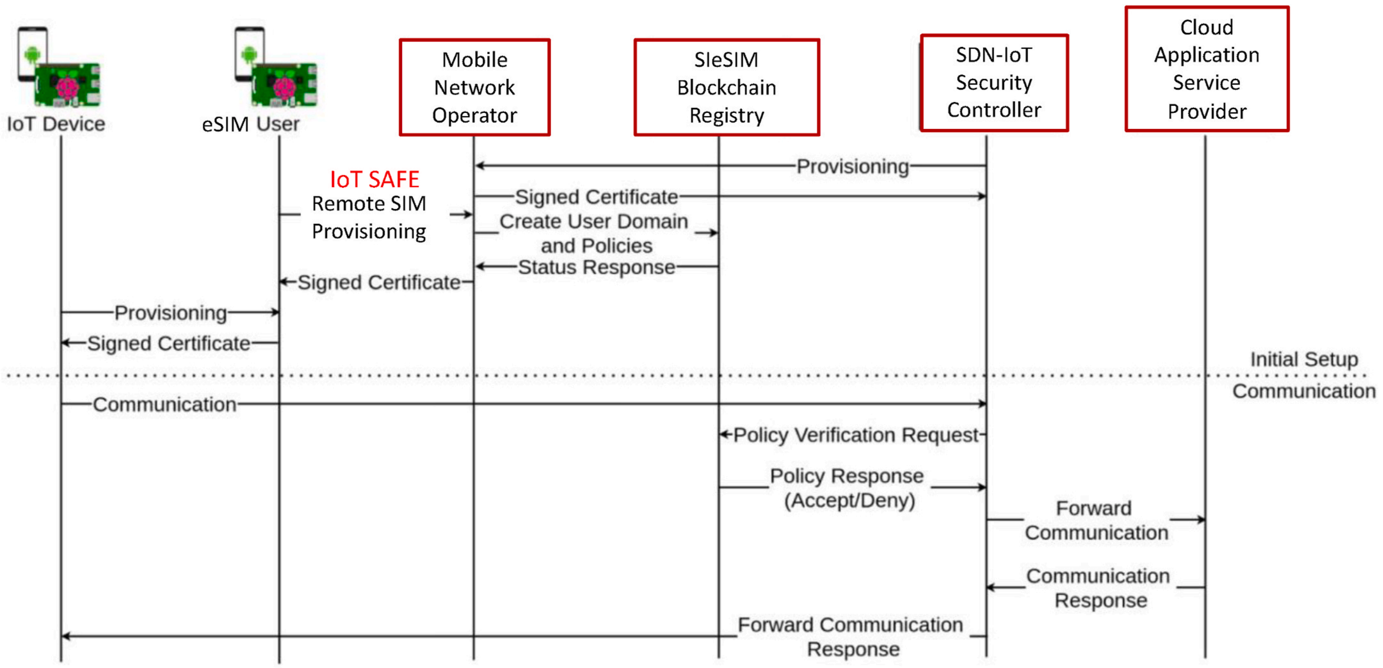

Fig. 8. SIeSIM authentication to provisioning sequence diagram.

Where is the authenticated eSIM user? Field p_n depicts the n^{th} profile activated in the eSIM.

Key generation: During the activation of the profile in eSIM, a key is generated with the Montgomery Curve Master Key-based Elliptic Curve Cryptography (MCMK-ECC). The ECC is selected here due to its enhanced security with higher-speed encryption. But, the ECC has the vulnerability to exploitation of public parameters. Thus, to avoid this problem, the Montgomery Curve and Master Key (MCMK) are introduced in the ECC algorithm.

Basepoint generation: For the key generation in the MCMK-ECC, a base point is selected from the Montgomery curve. The Montgomery curve [46]over a field $\Im$ is given as,

$$M.u^2 = v^3 + v^2 + \mathrm{v} \tag{2}$$

While $M, N \in \Im$ is a constant parameter, v, u represents the u and v-axes, respectively. From the Montgomery curve equation, a base point b is selected for the key generation process.

Key generation: Initially, two private keys Field are randomly selected for the key generation. These private keys are prime integers kept confidential between the subscriber manager and the eSIM user. Then, with the base point and the private keys, the sharable public keys are generated on both ends as,

$$P_1 = K_{1.}.b \tag{3}$$

$$P_2 = K_{2.}.b \tag{4}$$

The field P_1, P_2 depicts the public keys generated at the eSIM user and subscriber manager side.

4.6. *Blockchain integrated secure zero-touch eSIM IoT provisioning*

Blockchain-based eSIM management for IoT provisioning is a decentralized approach to eSIM management that uses blockchain technology to provide secure storage, tracking, and authentication of eSIMs. Each eSIM is registered on a blockchain network, which allows for secure and tamper-proof storage and monitoring of the eSIM throughout its lifecycle. The eSIM provisioning process can be divided into eSIM registration and eSIM activation. During the eSIM registration phase, the eSIM is registered on the blockchain network, which provides a unique identifier and public key for the eSIM. The private key is stored securely on the eSIM hardware, while the public key is stored on the blockchain network. During the eSIM activation phase, the eSIM is activated by the network operator or service provider. The activation process involves sending a request to the blockchain network, which verifies the authenticity of the eSIM using its public key. Once the eSIM is authenticated, it is activated and ready for use. Fig. 9 displays the bootstrapping procedure of devices in the Registration/Provisioning Phase.

As shown in Fig. 10, the initial bootstrapping of all smart objects (IoT devices) involves authenticating and attesting each device in the deployment domain using the manufacturer-specific eSIM/IoT device profiles. Attestation protocols must be used to stop leaking secrets, identities, and data. A new IoT device, system, or equipment gets certified as legitimate when onboarded into the network. It will determine whether this new gadget is suitable. The Blockchain Provisioning Manager and local domain policy manager produce the SxC contract. For instance, to be eligible for participation in a trusted cluster of IoT devices, each vendor could need to successfully execute an attestation exchange and get a licensed/SxC smart contract and profile. The “eSIM-signature” is extracted from the profile by the provisioning manager.

To provide authentication to the registered users, blockchain-based security is provided. A hash code is created and stored for authentication in the blockchain, which is connected to the subscription manager. The hash code is made with the Keccak Parallelism-based Argon 2 (KPA2) to enhance security and avoid brute force attacks. Argon 2 is a password hashing technique that provides better security than simple hashing algorithms. But, the absence of parallelism may lead to continuous iteration, which increases the hash code generation time. Thus, to avoid this problem, the Keccak Parallelism is used in the Argon 2 hashing technique.

Input: Argon2 takes primary and secondary input to produce a hashcode. The primary inputs are the message field (W) of length $t - bit$ also known as password, which is given as,

$$\mathrm{W} =$$

\langle$I, E, RI.b$\rangle I, E, RI depicts the IMSI number, enrolment key, and registration ID. The secondary input (ζ) contains nonce salt for

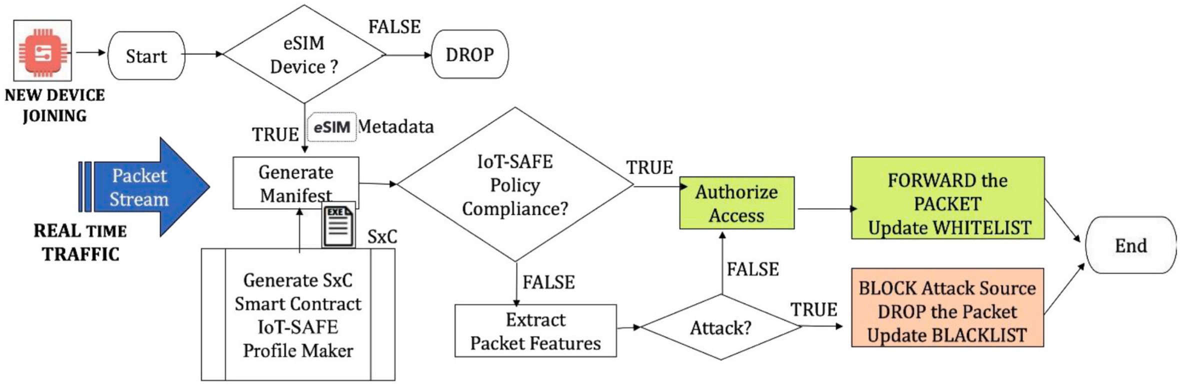

Fig. 9. Bootstrapping procedure of devices in IoTs

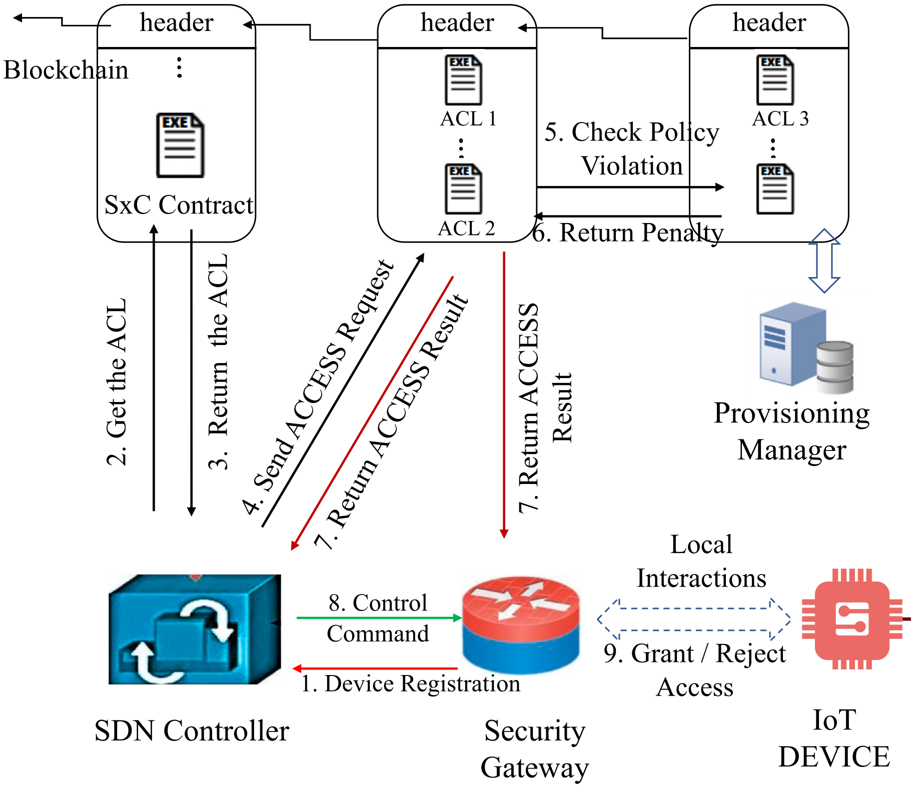

Fig. 10. eSIM Device Registration in the Blockchain Registry.

password hashing. The primary inputs are given by the user, which can have a length of 0 to 2^{32}-1 bytes

Operation: KPA2 uses an internal compression function (Θ) with two 1024-byte inputs, a 1024-byte output, and an internal hash function ($\hat{\varpi\lambda}()$) of BLAKE2 is applied. Where λ depicts the output hash length, KPA2 follows the extract-then-expand concept. First, entropy from the message and nonce are produced by hashing it. The compression function in the KPA2 is applied after the keccak parallelism.

Keccak parallelism: The Keccak function has the initialization, absorption, and squeezing stages. In the absorption phase, the $t-$ bit input message blocks are XORed with the first $t - bit$ of salt value, which is given as,

$$KP = W_{\mathrm{t}} \oplus \xi_t \tag{6}$$

The resultant *KP* is interrelated with the function. After the entire input message is processed, the compression takes place.

Compression: The hash block compression is built on the Blake2 round function. ϑ operates on 128-byte input, which is viewed as 16-byte registers,

$$\vartheta(B_0, B_1, \ldots..B_7) = (F_0, F_1, \ldots..F_7) \tag{7}$$

Where B, F depicts the input and output of the Blake round function. The compression function is $\Theta(E, C)$. For compression, the registers (Re) of 16-byte $(\mathrm{Re}_0, \ldots., \mathrm{Re}_{63})$ are computed with,

$$Re = E \oplus C \tag{8}$$

The $\vartheta()$ is applied row-wise at first and then column-wise to get the compressed output. This process is given as,

$$\Theta(E, C) \rightarrow^{\vartheta} Re \rightarrow^{\vartheta} v \rightarrow^{\vartheta} J \rightarrow J \oplus Re \tag{9}$$

Where Re depicts the row-wise resultant of Blake rounding, υ is the resultant of column-wise Blake rounding. Then, the compressed resultant is given as Field.

Resultant hash code: As the Keccak parallelism is introduced, the compression is iterated fewer times than the argon hash. The final hashcode generated is given as,

$$\varpi[Bl_{nn}] = J \tag{10}$$

Where Bl_{nn} signifies the hashcode generated at the nn^{th} block.

Blockchain: This hashcode J is stored in the blockchain as a transaction. Thus, the hashcode is verified whenever the eSIM user initiates the process. Other methods can be performed if the hashcode presented in the blockchain matches the hashcode generated on the user side. If the hashcode is unmatched with the hashcode in the blockchain, the process initiated using the eSIM credentials will be declined. By doing this process, eSIM hijacking will be avoided, as the malicious user cannot get the profiles of the registered users.

5. Evaluation

To evaluate the proposed mechanism, we conducted simulations and experimental studies. Fig. 11 illustrates the complete end-2-end software-to-hardware stack implemented to realize the SIeSIM architecture described in detail in the previous section.

Hardware

- iSIM, IoT SAFE, Java app integrated SoC in device platform (smart devices, gateway switches, routers, cellular modems)
- eSIM, SoC- Chipset/modules for partners/device vendors/network operators/service providers
- 5G, NB- IoT and LTE-M RAN options are packed in a single IP Core/ design.

Software

- OS - iSIM OS
- SIM Management -Remote SIM provisioning solution
- IoT Middleware API to support interactions with IoT Safe Applet on a SIM.
- Applets – IoT SAFE stack, applications
- SDK/API for implementing/customizing the Applets, tracking, Filters, Profiles

5.1. Network setup

The simulations were conducted using the COOJA simulator, which is a network simulator that enables the evaluation of IoT networks. The experimental studies were performed using a set of AIoT devices and a server. We've built a bespoke IoT gateway that interacts with Microsoft Azure's IoT cloud services. Our SIeSIM services interact with Azure's core application services and ensure policies are followed at the gateway level. Fig. 12 shows the lab setup.

5.2. Threat model

Components need to be evaluated for specific threat types [41,42] and analyzed using DFDs ("Data Flow Diagrams") for identifying and mitigating threats. Recent vulnerabilities in Glibc, OpenSSL, and log4j logging libraries (popular Java applications) illustrate how components could expose entire systems. Using data flows, processes, and definitions in DFDs, the proposed SIeSIM solution is analyzed on STRIDE [43] framework. It also includes specific firewall rules at perimeters of deployments (to prevent external exploitations) and router rules in SIeSIM to protect against insider threats, administration errors, and misconfigurations.

5.3. Evaluation methodology

Given that the duration of the provisioning process (time-to-provision, TTP) is the single most important KPI. We evaluated and compared the efficacy of our advanced SIeSIM provisioning framework with the IEEE 802.15.4 baseline [44,49,50] fairly and objectively. ZigBee or ZigBee/IEEE 802.15.4 protocols are wireless networking specifications encompassing hardware/software standard designs for wireless sensor networks (WSN), requiring high levels of reliability, lowered costs and power, scalability, and decreased data rates.

5.4. Performance analysis

This section will present the efficacy metrics of our proposed solution. The function of pre-condition and post-condition policy(ies) configuration, as defined by the end-user or IoT application/middleware, will add some delay in the provisioning process. We ran a series of experiments and test tools to measure the following key performance

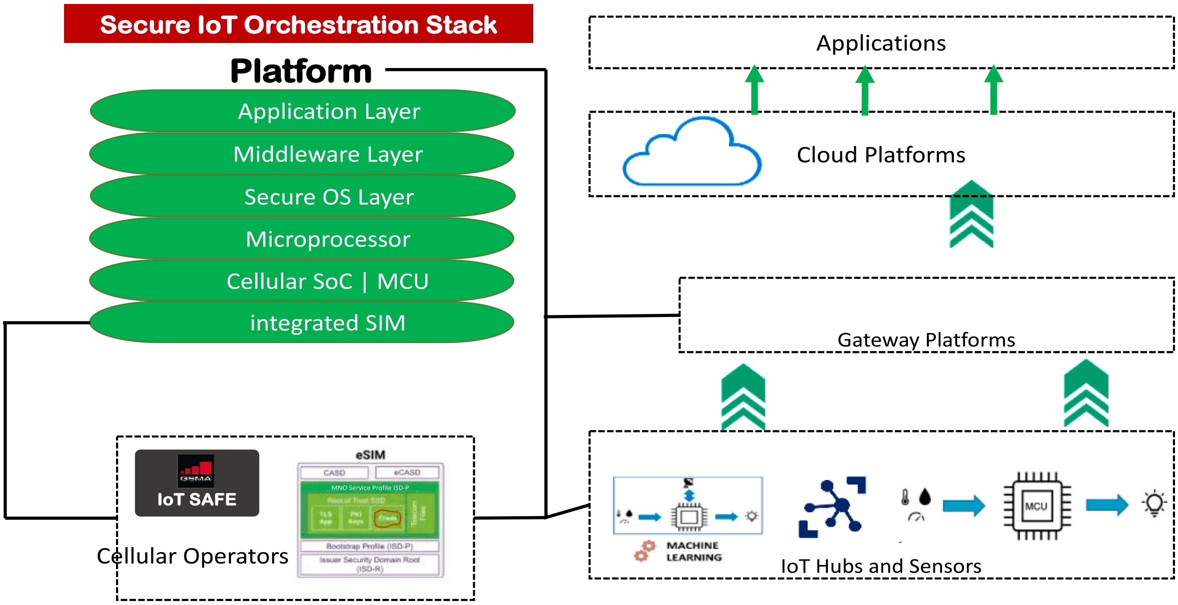

Fig. 11. SIeSIM solution stack.

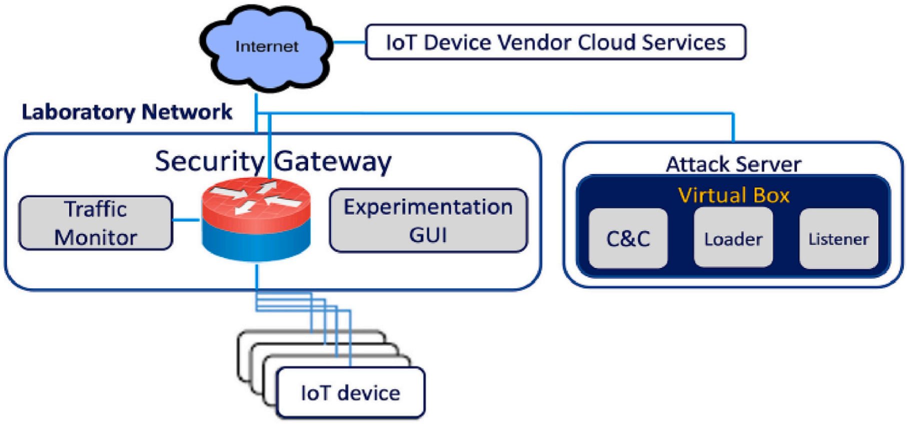

Fig. 12. Laboratory system components.

indicators of our solution. They are (1) Provisioning speed or latency, (2) network bandwidth/throughput consumed, (3) resource usage (CPU/RAM), (4) Authentication efficacy, (5) eSIM provisioning Workflow overhead, (6) runtime monitoring, and (7) anomaly detection (7), blockchain processing overhead. We connected multiple gateways to the cloud during each experiment and provisioned Internet of Things (IoT) devices to each gateway. These measurements are highly context-dependent and may vary in other environmental contexts.

5.4.1. *Latency and device provisioning speed*

Latency incurred to Device provisioning is the total time required to autonomously establish connectivity and attest the allowed IoT devices into IoT edge networks and clouds. The procedures involve authentications, linking, and authorizations. There might be modest delays in overall device provisioning processes because of the implementation of precondition policies to improve authentications. Fig. 13 displays latency/provisioning times as functions of device counts and necessary policies of authentications. The provisioning time for devices was measured without SIeSIM, where it was found that it grew linearly with device counts. SIeSIM increased provisioning latency logarithmically due to the executions of parallel threads inside its software architecture.

Manual: For 100 devices, it takes 240s and increases to 2650s with 1000 devices.

With SIeSIM: Activating the Zero-touch automated provisioning services, the provision time increases slightly due to the processing check, authentication, and blockchain overhead. With 100 devices, the overhead is 120s; for 1000 devices and 400 pre-condition policy entries, the provisioning delay is 1300 s. This result demonstrates that the proposed architecture is feasible and can effectively reduce end-to-end delay relative to the baseline.

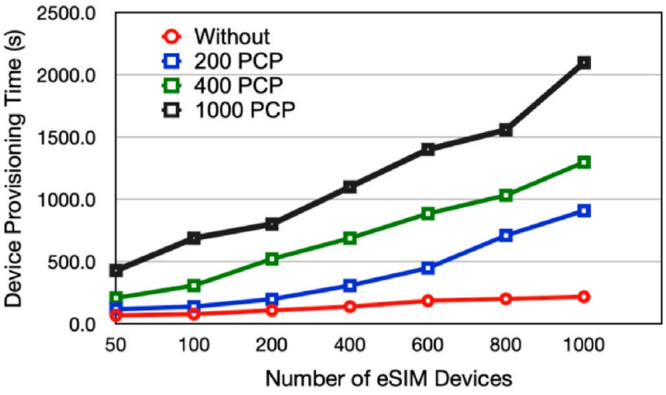

Fig. 13. Device Provisioning Scaling vs. Pre-Condition Policies (PCP).

5.4.2. *Throughput*

Fig. 14 compares throughput with and without the SIeSIM service operating on the IoT network. We used iPerf to monitor the network's throughput while varying the number of postcondition policies (Blockchain contracts). The increase in postcondition policies is mirrored in the bar graph by a corresponding decrease in throughput. As an example, the throughput is 480 Mb/s with 400 policies. In contrast, throughput drops to 960 Mb/s when PCP is disabled.

5.4.3. *Resource (CPU/memory) utilization*

We will only consider CPU and heap memory usage to describe the system's resource utilization by the SIeSIM services on the hardware platform. Resource consumption depends most on system configuration and execution environment. Thus, this is a prototype system demonstration, not a standard representation. We conducted ten experiments with average resources. Fig. 15 shows that the number of policies (pre- and post-condition) affects CPU and heap memory consumption. The application used 1250 MB of heap memory and 89 % CPU with 400 policies. IoT network gateway hubs use 35 % CPU and 127 MB heap memory without SIeSIM services.

5.4.4. *Time-to-provision (manual/zero-touch)*

When evaluating automated provisioning systems, we average the results of 18 evaluation tests to determine TTP performance for the following situations (see Table 2). Furthermore, the manual provisioning scenario is divided into two cases: i) a single expert makes provision across four evaluations, and ii) provisioning is done manually by an expert human operator, with each operator doing a single evaluation test. The second option is desirable since a non-expert can master the provisioning rules and become an expert by the end of the assessment tests. As a result, we implemented this countermeasure to ensure the validity of the evaluation.

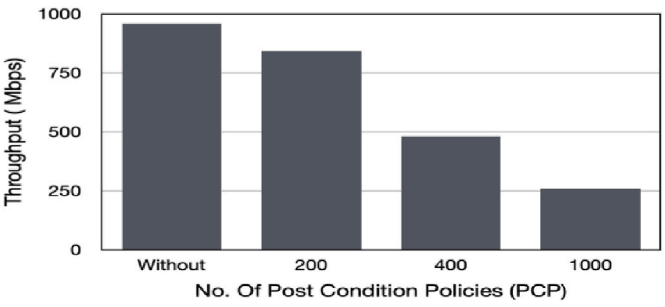

Fig. 14. Throughput vs. PCP scaling.

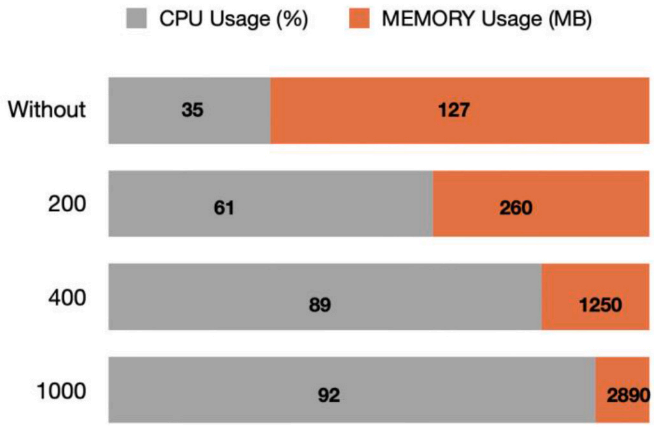

Fig. 15. Pre/post condition policies vs. Resource usage (CPU, RAM).

Table 2
Time-to-provision (TTP) evaluation results.

Evaluation Scenarios	Manual Provisioning		Zero-Touch SIeSIM
	Expert	Non-Expert	
Average TTP [sec]	41	143	11
Best-Effort TTP [sec]	38	124	9
Worst-Effort TTP [sec]	52	187	14

- **Manual Provisioning***:* The device will be provisioned by one expert familiar with the provisioning procedures and by four non-experts who have no prior knowledge of the provisioning procedures, following the detailed provisioning guide. In addition to the guidelines, we provided each non-expert with a few introductory remarks before beginning the provisioning process.
- **Automated SIeSIM:** To evaluate the SIeSIM- Zero Touch automated Provisioning solution with security procedures considered for exemplifying interoperability.

5.3.5. *Energy consumption and delay*

Routing devices—generally speaking, networking components—consume significant energy during data transmission. In particular, the device's energy consumption is directly correlated with the amount of data it transmits (i.e., the more bits it transmits, the more energy it uses). We compare the IEEE 802.15.4 protocol [58] with the suggested SIeSIM in order to assess its energy usage. From Fig 16 a), It is evident that compared to the IEEE 802.15.4 protocol, our suggested algorithm uses less energy and can efficiently select the edge server. Additionally, the suggested technique has a higher efficiency in energy utilization with increasing simulation time despite both algorithms having similar energy-utilization profiles.

Because IoT applications are employed in real-time systems, all processes must be completed as quickly as feasible. Fig 16 b) shows graphs that show the end-to-end delay versus the elapsed simulation time when the IEEE 802.15.4 protocol and the suggested SIeSIM technique are simultaneously executed for 30 s. While the suggested technique consistently exhibits a shorter end-to-end delay than the IEEE 802.15.4 protocol, we can observe that the end-to-end delays of both approaches converge with the simulation time. As a result, our concept offers adequate performance and effective communication between the routing devices.

5.4.6. *Authentication and bootstrapping*

Fig. 17 a) demonstrates the delay for COAP-EAP bootstrapping (authentication/provisioning) per IoT device. The average overall authentication delay for eSIM + Blockchain processing involves getting an eSIM profile from the IT server, translating it to IoT-SAFE policies, confirming Blockchain compliance, and enforcing policy under normal and attack scenarios. The defense mechanism must process more when the attack ratio increases from 0.1 to 0.9. The average provisioning time for a new node is around 1/9 of the open-source traditional IoT provisioning strategy. Device authentication takes 4300 ms with the basic classical IEEE 802.15.4 scheme [44].

Our SDN-based remote-SIM provisioning approach at the IoT gateway reduces overhead to 240–2000 ms for an exact number of packet exchanges. Our IoT-SAFE-based scheme can handle complex network configurations using the Over-The-Air (OTA) GSMA IoT-SAFE protocol through cellular operators and advanced Cellular-IoT Gateway hubs. The traditional IoT provisioning scheme (over CoAP/EAP) uses a slower DSA signature generation method. We investigated IoT-SAFE and Blockchain-based contract compliance verification overhead with cellular IoT networks and eSIM devices utilizing comparable credential/access restrictions. The JSON-based tokens implemented in the SIeSIM authentication protocol reduced metadata size by 25 % in Fig. 17 b.

5.4.7. *Workflow overhead*

IoT Device Enrollment: Cloud-IoT protocols like MQTT and CoAP are used at the network's periphery, known as the Edge. The time and effort put into the smart contract development and verification procedure did not appear to impact the system's scalability, as shown inFig. 18 a.

Policy Violation Detection: Policy violation detection in IoT security is critical for ensuring the integrity and safety of connected devices. When policies are violated, it can lead to various risks, including data breaches, unauthorized access, and potential damage to the IoT

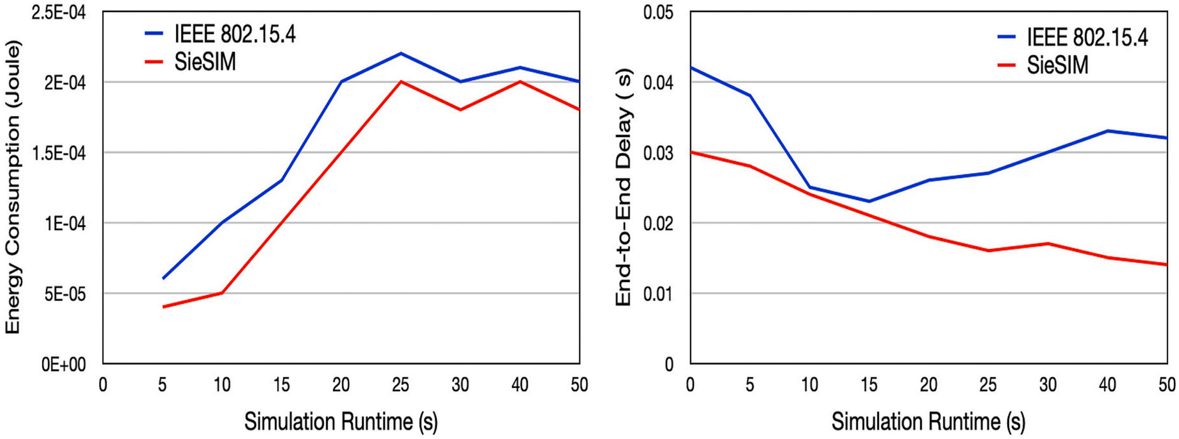

Fig. 16. a) Energy Consumption b) End-to-End delay.

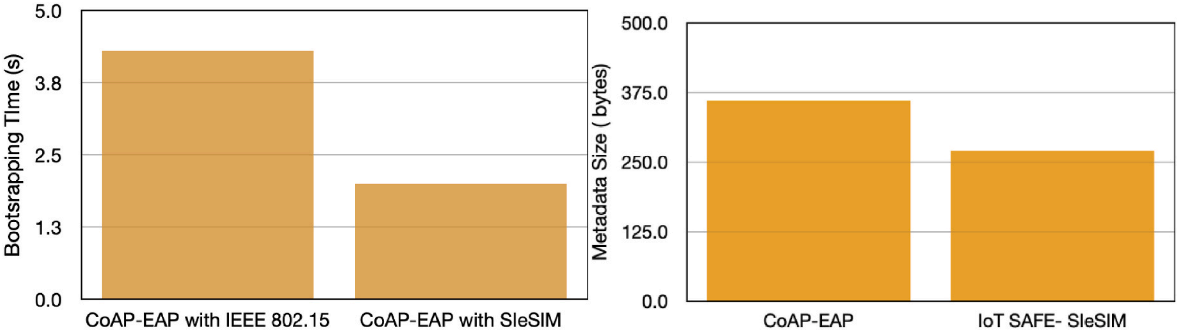

Fig. 17. eSIM-based Provisioning b) Blockchain Contract Registration.

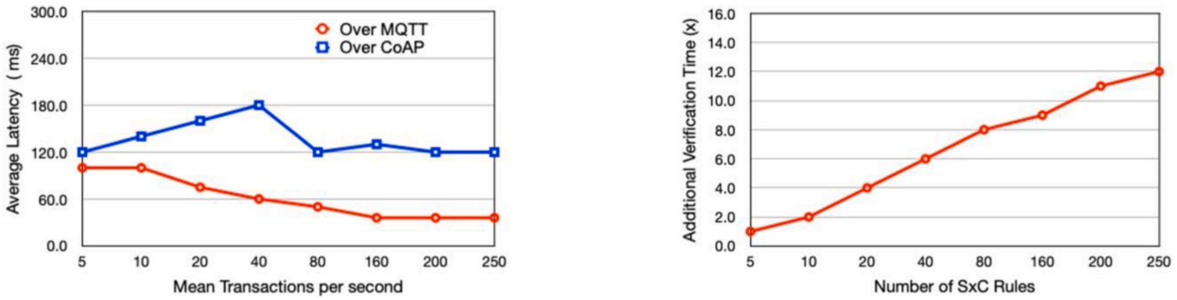

Fig. 18. a) eSIM Enrollment delay b) Blockchain Policy Verification Scalability.

ecosystem.

The impact of policy violation detection on IoT security is multifaceted:

1. Risk Mitigation: Detecting policy violations helps mitigate risks by identifying potential security breaches or unauthorized access in real-time.
2. Prevention of Compromise: It assists in preventing the compromise of sensitive data or device functionalities, ensuring the overall integrity of the IoT network.
3. Compliance: Maintaining compliance with industry standards and regulations is crucial. Detection of policy violations helps ensure adherence to these standards.

The relationship isn't necessarily linear regarding resolution time scaling with the number of rules. The time required for resolution can increase with the number of rules due to the complexity of analyzing and addressing multiple violations simultaneously. Efficiently managing a larger rule set may require more sophisticated algorithms and computational power, potentially leading to increased resolution times.

To detect rule violations efficiently and accurately in real-time sensor data, IoT gateways employ Rule-Based Monitoring. Implementing a rule-based system for monitoring and analyzing incoming data against predefined policies can efficiently detect violations. However, managing a vast number of rules might impact processing speed. The gateway checks real-time sensor data for rule violations. We determined the time required for policy verification by altering the number of rules (beginning with a configuration of 5 rules). Resolution time scales linearly with policy count (Fig. 18 b).

5.4.8. *Blockchain processing overhead*

Ethereum's unit gas represents computational work—Fig. 19 a shows contract/transaction gas consumption. Transactions increase gas use. Our method improved transaction throughput by 30 % and transaction time by 85 %. Gas consumption and processing time are similar (up to 27 s) for transactions under 200. As transactions increase, gas consumption increases linearly while processing time remains constant. Our system is scalable since an SDN controller's processing time is lower than the gas needed for a Blockchain transaction. Thus, our concept combines high safety (Blockchain technology) with efficiency (optimized SDN-eSIM IoT-SAFE architecture).

Fig. 19 b shows the performance in terms of overall end-to-end delay

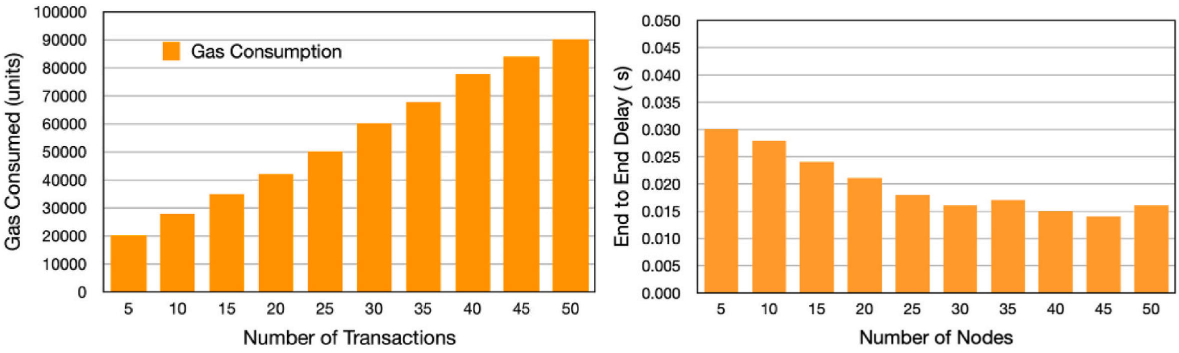

Fig. 19. a) Blockchain Energy Consumption b) Delay with Number of Nodes.

(in *seconds*). In detail, we compute the overall end-to-end delay in terms of workloads and time delay by varying the number of nodes, notably, with a small number of nodes (i.e., ≤10), the end-to-end delay of our proposal, and increasing the number of nodes, both end-to-end delays show a linear increasing trend, with our proposal constantly outperforming the baseline method.

5.5. Security analysis

In the following sections, we'll review different attack scenarios and discuss the security properties. Finally, we will detail how our proposed SIeSIM safeguards endpoints and the underlying network infrastructure by adapting attack case studies to real-world attack scenarios. Information security analysis data is also presented.

1) Security Properties, Defense Mechanisms and Attack Studies

In this section, we present the results of an empirical evaluation of SIeSIM's security features. In this article, we described SIeSIM's security features. We provided case examples that illustrate those features in action. We conducted these case studies in real-time assault scenarios to show how an adversary can easily compromise a device that is either about to be supplied or that has already been provisioned and how the SIeSIM system can protect against such attacks by employing pre- and post-condition criteria.

- *Case 1—"Device Sending a Single Malicious Packet":* An adversary obtains access to the device via a stolen set of credentials and then attacks the IoT gateway. An authentication system is required to counter this assault.
- *Case 2—"Device Sending several Malicious Packets": This simulation uses A gadget to overwhelm the Internet of Things gateway with sham data.* The purpose of this assault is to examine the security of the authentication mechanisms.
- *Case 3—"Compromised Device Injecting Malware":* Only authenticated and already supplied devices can access the smart network. For instance, malware like Mirai infects devices. We will manufacture such attacks to put our authorization policies through their rules.
- *Case 4—"State Change of a Device Due to External Manipulation":* The SIeSIM allows device monitoring based on its condition and events. This test case aims to validate SDN Security Monitoring during runtime. Here, we'll conduct assaults against IoT gadgets to induce state transitions in those devices. These transitions in the state are difficult for authorization policies to detect. Our SDN Controller's event-driven state monitoring services pick up on these shifts as they occur.

2) Resilience to Malicious eSIM devices

In an increasingly mobile world, malicious cellular IoT devices can significantly influence the security and functionality of the communication system. SIeSIM's capacity to distinguish between legitimate and malicious devices is paramount. SIeSIM security controller can't re-authenticate the device until it receives the entire sequence of messages. With our authentication technique, we can significantly minimize the calculation and communication requirements for detecting malicious users/rogue IoT devices in the network. The computing costs of SIeSIM and the conventional method in the case of an attack scenario due to rogue IoT devices present in the network are compared in Table 3. For simplicity's sake, the vertical axis of Fig. 20 is depicted as a log scale, which shows the computational delay.

Table 3
Overhead in Malicious eSIM Devices Scenario.

Scheme	Computation Cost (ms)
P.G [22]	0.10
A.I [28]	0.14
S.J [36]	0.18
SIeSIM [Proposed]	0.04

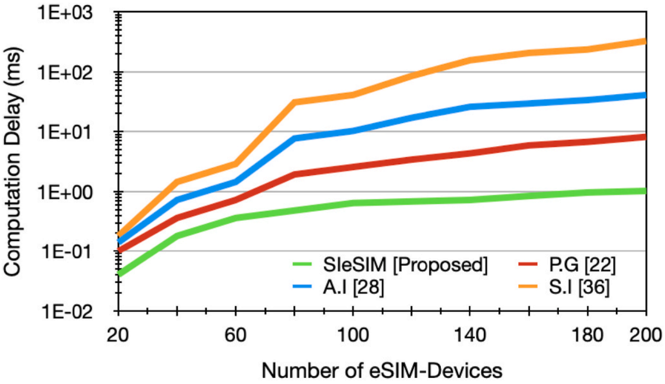

Fig. 20. Consumption delays vs. Devices.

3)Informal Security Analysis

At the outset of this part, we demonstrate that our proposed authentication/registration protocol in SIeSIM architecture is resistant to several standard security attack models intrinsic to 3GPP protocols and other related techniques. The gist of the strengthening is that even when the long-term private key is compromised in the future, it does not allow the attacker to compute any current active session key. Perfect forward secrecy is thus achieved. This is done by ensuring that the compromise of the private key reveals no information on the session key used in the computation of the long-term key. Furthermore, SIeSIM also achieves leakage resilience because of the structure of the multi-signature it operates, in that even though the stored secret key leaks out from the signature Si, the attacker cannot obtain any constant non-session-dependent function of the long-term secrets. This is assured due to the hardness of the discrete logarithm problem, i.e., given y = Gx mod N for some public parameters g and N, it is infeasible to recover the discrete logarithm x.

5.6. Comparison with related works

There is a paucity of resources to install and manage the expanding eSIM-based Autonomous-IoT ecosystem, and its workflow standards still need to be improved. These issues have received scant attention from academics. Due to these considerations, we introduced a novel and efficient provisioning algorithm and a distributed monitoring technique that guarantees network consistency and security within the Blockchain-enabled software-defined IoT ecosystem. Our framework's layered design supports several SDN domains for mobile carriers to improve IoT ecosystem availability, secrecy, and integrity. Secure device provisioning is our primary goal. Our method differs from others in this field in four ways. First, eSIM-Blockchain's granular device and context-specific precondition regulations provide security checks to device authentication during provisioning. Second, SIeSIM precondition policies cross-check device operation during runtime (authorization). We established a security feature-focused blockchain registry to evaluate provided device security. Third, SIeSIM evaluates device security during provisioning and runtime. For instance, if the gadget is running malware or has outdated firmware. Finally, the SIeSIM service can prevent rogue devices from entering the network infrastructure and thwart attacks.

5.7. Key findings and result discussions

The system's security was built from the ground up with standardized and trusted components. This study focused on the most pressing issues surrounding IoT-based infrastructure security [45], including provisioning, secure registration of autonomous IoT devices, and attacks on these systems. Inadequate security configuration, unprotected data transmissions, suspicious behavior, malicious hardware, and security lapses.

- IoT security application, compliant with GSMA IoT SAFE
- Server for credential life cycle management, compliant with GSMA IoT SAFE.
- Hardware root of trust through IoT SAFE-based eSIM-enabled security enclave = end-to-end.
- IoT SAFE eSIM enabled IoT devices = zero-touch provisioning/re-provisioning of credentials.
- Blockchain-based registration and Identity Management
- Intelligent field gateway, hub, microcontrollers, SoCs, things
- IETF Enrolment over Secure Transport (RFC 7030) with Public Key Infrastructure
- SDN Orchestration, IoT Life cycle Monitoring, and dynamic provisioning System

Our research shows a need for improvement in the technology components, such as incorporating IoT, Blockchain, eSIM provisioning, and SDN management standards into smart and secure autonomous IoT applications. The TTP evaluation tests are comprehensive and average, best-effort (to potentially reveal how much time is required for manual provisioning by an expert with advanced knowledge compared to the automated ZTP solutions) and worst-effort (to potentially reveal how much time is needed for a non-expert without technical background compared to the expert counterpart case and the automated ZTP solutions). Section E exhibits TTP performance. Manual provisioning's best-effort TTP (44.83 s) beats all automated provisioning's worst-effort TPP (48.80 s) by 9 %. Automated ZTP solutions surpass manual TTP by at least 154 %. In summary, our suggested ZTP solution surpassed previous closely related and comparable ZTP solutions, particularly in the best circumstances, where the SIeSIM performs roughly 120 % better TTP than the [40]. Table 4 below enumerates the summary and salient findings from the experiments.

Table 4
Summary of the key findings.

ASPECTS EVALUATED	DISCUSSION
Device Provisioning **Section V.E 1)**	Activating the Zero-touch automated provisioning services, the provision time increases slightly due to the processing check, authentication, and blockchain overhead. With 100 devices the overhead is 120s, for 900 devices, and 450 precondition policies, the provision time is 1300 s.
Throughput **Section V.E 2)**	We assessed SIeSIM's overall network processing capacity with a specific network traffic load. This test measures the total provisioning and authentication workloads in a fixed time slot. The result illustrates a decrease in throughput with increasing postcondition policies. For example, with 450 policies, the throughput is 480 Mb/s. While without the SIeSIM, the throughput is 960 Mb/s. In SIeSIM, multi-threaded processing and network communication are faster than in the IEEE 802.15 baseline.
Resource Usage **Section V.E 3)**	The evaluation shows that the CPU and heap memory usage increases with the higher number of policies (both pre and post-condition). With 450 policies, the CPU usages become 89 %, and the software utilized 1250 MB of heap memory. On the other hand, without the SIeSIM services running on the IoT network hubs, they utilize on average 35 % of the CPU and 127-MB heap memory.
Provisioning Time **Section V.E 4)**	We evaluate the Time-to-Provision (TTP) performance for the various scenarios (automated provisioning with SDN + Blockchain based SIeSIM and manual provisioning with IEEE 802.15 baseline.
New Device Registration **Authentication** **Section V.E 5)**	With cellular IoT network, with eSIM device, we tested the overhead for the IoT-SAFE and SxC Blockchain-based contract compliance verification using similar credential/access policies. Our solution reduced the metadata size by 9 % (24 bytes) with JSON-based token. The total time for the device authentication process is in the order of 4300 ms. But, with our design, since we deploy the SDN-based Remote-SIM provisioning protocol at the IoT gateway level, for a similar count of packet exchanges, the overhead is reduced to 240–2000 ms.
Blockchain Processing **Section V.E 7)**	The gas consumption increases with the number of transactions. Our scheme outperformed current strategies by up to 30 % in overall transaction throughput and improves the time between transactions by up to 85 %. With a lower number of transactions (i.e. < 200), the gas consumption and processing time assume similar values (up to ≈ 27 *s*). Our proposal is able to combine high safety (provided by Blockchain technology) with efficiency (provided by SDN-eSIM IoT-SAFE architecture).
Security Properties **Section V.F.1**	We conducted these attack case studies in real-time attack scenarios and demonstrate how an adversary can easily compromise an about-to-be-provisioned device or an already-provisioned device. SIeSIM can defend against such attacks using pre/post-condition policies.
Resilience to Malware **Section V.F.2**	With our authentication technique, we can significantly minimize the calculation and communication requirements for detecting malicious users/IoT devices.

6. Limitations and future work

While the proposed architecture for eSIM-based secure provisioning of IoT devices provides many benefits, there are still open problems. While this research has proven the value of integrated approaches by producing improved outcomes across various performance indicators and security posture, it has its limitations and problems, briefly discussed below.

- ***Interoperability***: Different manufacturers and providers may use different eSIM technologies, which can create interoperability issues. Standardization efforts should be made to ensure interoperability across different eSIM management platforms and IoT devices.
- ***Scalability***: As the number of IoT devices and the volume of data they generate increases, scalability becomes a significant challenge. Efficient provisioning, management, and communication between devices and cloud services must be addressed to ensure the architecture can handle large-scale deployments.
- ***Security***: While eSIMs provide an additional layer of security for IoT devices, they are not entirely immune to attacks. Robust security measures should be implemented to prevent unauthorized access, data breaches, and other cybersecurity threats.
- ***Cost***: The cost of implementing eSIM technology in IoT devices can be high, which may make it difficult for smaller companies to adopt the technology. Efforts should be made to reduce the cost of eSIMs and associated hardware to make them more accessible to a broader range of users.
- ***Regulation***: The use of eSIM technology in IoT devices is still relatively new, and more regulation in this area needs to be done. Governments and regulatory bodies must develop policies and regulations to ensure the security and privacy of data generated by IoT devices with eSIMs.
- ***Cloud service vulnerabilities:*** Cloud services have intricated pieces of software that can have security holes. Current cloud systems must

correct the assumption that all distributed cloud services can be trusted. Thus, an unpatched component version or misconfiguration in one cloud service may let adversaries disseminate attacks to other cloud services, putting any user's cloud resources at risk. SIeSIM protects communications between services, hosts, nodes, and mechanisms. However, a compromised cloud service can still misbehave or spread attacks. We will examine current defenses carefully and qualitatively against cloud service vulnerabilities and mobile operators' misconfigurations.

7. Conclusions

eSIM-based secure identity and provisioning provide a viable solution for the requirements of the IoT ecosystem. It enables secure, flexible, and remote management of IoT devices, eliminating the need for physical SIM cards and simplifying the supply chain. eSIM-based identity and provisioning can help address the challenges associated with IoT security, such as authentication and data privacy. However, eSIM technology faces several challenges, such as standardization and OTA management. Despite these challenges, eSIM-based identity and provisioning present several opportunities for innovation and growth in the IoT ecosystem. This paper proposed using the GSMA standardized IoT-SAFE protocol-based eSIM for secure zero-touch service provisioning in autonomous IoT. The proposed solution enables devices to be provisioned securely and automatically without human intervention, ensuring the network is protected from vulnerabilities. The solution has been evaluated using simulations and experimental studies, demonstrating its effectiveness in enabling secure zero-touch service provisioning in AIoT networks. In conclusion, eSIM is a rapidly developing area of research in IoT. Future research must focus on creating solutions to these challenges and exploring new applications for IoT eSIM and integrated SIM (iSIM) with System-on-Chip in the emerging AI-based 5G/6G and beyond networks.

CRediT authorship contribution statement

Prabhakar Krishnan: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Resources, Methodology, Investigation, Data curation, Conceptualization. **Kurunandan Jain:** Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Resources, Methodology, Investigation, Formal analysis, Conceptualization. **Shivananda R. Poojara:** Writing – review & editing, Validation, Supervision, Software, Resources, Methodology, Investigation, Formal analysis, Conceptualization. **Satish Narayana Srirama:** Writing – review & editing, Visualization, Software, Resources, Methodology, Formal analysis. **Tulika Pandey:** Writing – review & editing, Visualization, Validation, Software, Methodology, Formal analysis. **Rajkumar Buyya:** Writing – review & editing, Visualization, Validation, Supervision, Software, Formal analysis, Conceptualization.

Declaration of competing interest

The paper entitled, "eSIM/Blockchain Integrated secure Zero-Touch Provisioning for Autonomous Cellular-IoTs in 5G Networks" has been submitted to Special Issue: "Zero-touch Service Provisioning for Autonomous IoT". The authors and Co-Authors have no conflicts of interest and the paper is not been submitted to any other Journals.

Data availability

No data was used for the research described in the article.

References

[1] Y. Lu, L. Da Xu, Internet of Things (IoT) cybersecurity research: a review of current research topics, IEEE Internet Things J. 6 (2018) 2103–2115.

[2] S. Nižeti′c, P. Šoli′c, D.L.D.I. González-de, L. Patrono, Internet of Things (IoT): opportunities, issues, and challenges towards a smart and sustainable future, J. Clean. Prod. 274 (2020) 122877.

[3] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes, in: Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, 2018, pp. 1–8. October 2018.

[4] M. Adil, M. AminAlmaiah, A. Omar Alsayed, O. Almomani, An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks, Sensors 20 (8) (2020) 2311.

[5] M.T. Hammi, B. Hammi, P. Bellot, A. Serhrouchni, Bubbles of Trust: a decentralized blockchain-based authentication system for IoT, Comput. Secur. 78 (2018) 126–142 [CrossRef].

[6] Praveen Kumar Donta, Satish Narayana Srirama, Tarachand Amgoth, Chandra Sekhara Rao Annavarapu, Survey on recent advances in IoT application layer protocols and machine learning scope for research directions, Digital Communications and Networks 8 (Issue 5) (2022), https://doi.org/10.1016/j.dcan.2021.10.004, 727-744, ISSN 2352-8648.

[7] P. Hosein, G. Sewdhan, A. Jailal, Soft-Churn: Optimal Switching between Prepaid Data Subscriptions on E-SIM Support Smartphones. 2021 IEEE 8th International Conference on Data Science and Advanced Analytics, 2021, https://doi.org/10.1109/DSAA53316.2021.9564163. DSAA 2021.

[8] S. Yadav, R. Rishi, Secure and authenticate communication using Softsim for intelligent transportation systems in smart cities, J. Phys. Conf. 1767 (1) (2021) 1–11, https://doi.org/10.1088/1742-6596/1767/1/012049.

[9] M. Aazam S. u. Islam S. T. Lone and A. Abbas, "Cloud of things (CoT): cloud-fog-IoT task offloading for sustainable internet of things," in IEEE Transactions on Sustainable Computing, vol. 7, no. 1, pp. 87-98, 1 Jan.-March 2022, doi: 10.1109/TSUSC.2020.3028615..

[10] R. Borgaonkar, I. Anne Tøndel, M. ZenebeDegefa, M. Gilje Jaatun, Improving smart grid security through 5 G-enabled IoT and edge computing, Concurrency Comput. Pract. Ex. 33 (18) (2021) 1–16, https://doi.org/10.1002/cpe.6466.

[11] K. Oztoprak, Y.K. Tuncel, I. Butun, Technological Transformation of telco operators towards seamless IoT edge-cloud continuum, Sensors 23 (2) (2023) 1–16, https://doi.org/10.3390/s23021004.

[12] A.S. Ahmed, A. Peltonen, M. Sethi, T. Aura, Security Analysis of the Consumer Remote SIM Provisioning Protocol, Annals of Telecommunications1, 2022. http://arxiv.org/abs/2211.1532.

[13] B. Abazi, 5G new radio evolution towards enhanced features, Thesis 38p (2023).

[14] C. Silva, J.P. Barraca, R. Aguiar, ESIM suitability for 5G and B5G enabled IoT verticals. Proceedings - 2021 International Conference on Future Internet of Things and Cloud, 2021, pp. 210–216, https://doi.org/10.1109/FiCloud49777.2021.00038. FiCloud.

[15] Istabraq Mohammed Alshenaifi, Emad UlHaq Qazi, AbdulrazaqAlmorjan, IoT forensics: machine to machine embedded with SIM card. ITNG 2023 20th International Conference on Information Technology-New Generations, Springer International Publishing, Cham, 2023.

[16] Surabhi Thatte, eSIM on IoT: an Innovative Approach towards Connectivity, 2020, https://doi.org/10.17577/IJERTCONV8IS05053.

[17] R. Kawamura - Future Of eSIM. https://www.soracom.io/blog/the-future-of-esim/. (Accessed 14 August 2019).

[18] Apilo, Olli, PekkaKarhula, Jukka Mäkelä, eSIM-based inter-operator mobility for advanced smart products, IEEE Internet of Things Magazine 5 (2022) 120–126.

[19] Alex R. Mathew, Threats and protection on E-sim: a prospective study, Novel Perspectives of Engineering Research 8 (2022) 76–81.

[20] Chrystel Gaber, Pierrick Kaluza, "eSIM adoption: essential challenges on responsibilities repartition.". International Conference on 6G Networking (6GNet), IEEE, 2022, 2022.

[21] Y. Gao et al. "Blockchain-based IIoT data sharing framework for SDN-enabled pervasive edge computing," in IEEE Trans. Ind. Inf., doi: 10.1109/TII.2020.3012508..

[22] Jianli Pan, et al., EdgeChain: an edge-IoT framework and prototype based on blockchain and smart contracts, IEEE Internet Things J. (2018) 4719–4732.

[23] L. Gong, D.M. Alghazzawi, L. Cheng, BCoT sentry: a blockchain-based identity authentication framework for IoT devices, Information 12 (2021) 203.

[24] P. Krishnan, et al., SDN Framework for Securing IoT Networks, 218, Springer, Cham, 2018, https://doi.org/10.1007/978-3-319-73423-1_11.

[25] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.R. Sadeghi, S. Tarkoma, IoT SENTINEL: automated device-type identification for security enforcement in IoT, in: Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems, ICDCS), Atlanta, GA, USA, 5–8 June 2017, pp. 2177–2184.

[26] D. Wang, H. Wang, Y. Fu, Blockchain-based IoT device identification and management in 5G smart grid, EURASIP J. Wirel. Commun. Netw. 2021 (2021) 125.

[27] A. Dorri, C. Roulin, S. Pal, S. Baalbaki, R. Jurdak, S. Kanhere, Device identification in blockchain-based internet of things. Early Access, IEEE Internet Things J, 2022.

[28] B.K. Mohanta, A. Sahoo, S. Patel, S.S. Panda, D. Jena, D. Gountia, DecAuth: decentralized authentication scheme for IoT device using Ethereum blockchain, in: Proceedings of the TENCON 2019—2019 IEEE Region 10 Conference (TENCON), 2019, pp. 558–563. Kochi, India, 17–20 October.

[29] H. Yang, B. Bao, C. Li, Q. Yao, A. Yu, J. Zhang, Y. Ji, Blockchain-enabled tripartite anonymous identification trusted service provisioning in industrial IoT, IEEE Internet Things J. 9 (2022) 2419–2431. IoT Safe protocol.

[30] M. Gowtham, M. Banga, Mallanagouda Patil, Secured authentication systems for the internet of things, EAI Endorsed Transactions on Smart Cities 4 (2020) 11.

[31] Kersten Heins, Kersten Heins, Cellular IoT technology. NB-IoT Use Cases and Devices: Design Guide, 2022, pp. 17–44.

[32] J. Munilla, M. Burmester, R. Barco, An enhanced symmetric-key-based 5G-AKA protocol, Comput. Network. 198 (2021) 108373, https://doi.org/10.1016/j.comnet.2021.108373.

[33] E. Baccour, M.S. Allahham, A. Erbad, A. Mohamed, A.R. Hussein, M. Hamdi, Zero-touch realization of pervasive artificial intelligence as a service in 6G networks, IEEE Commun. Mag. 61 (2) (2023) 110–116, https://doi.org/10.1109/MCOM.001.2200508.

[34] C. Toma, M. Popa, C. Boja, C. Ciurea, M. Doinea, Secure and anonymous voting D-app with IoT embedded device using blockchain technology, Electronics 11 (12) (2022) 1–25, https://doi.org/10.3390/electronics11121895.

[35] J. Ma, Y. Guo, C. Fang, Q. Zhang, Digital twin-based zero-touch management for IoT, Electronics 11 (24) (2022) 1–17, https://doi.org/10.3390/electronics11244104.

[36] H. Choudhury, HashXor: a lightweight scheme for identity privacy of IoT devices in 5G mobile network, Comput. Network. 186 (2021) 107753, https://doi.org/10.1016/j.comnet.2020.107753.

[37] Y.D. Lin, D.T. Truong, A. Ali, C.Y. Li, Y.C. Lai, T.M.T. Dinh, Proxy-based federated authentication: a transparent third-party solution for cloud-edge federation, IEEE Network 34 (6) (2020) 220–227, https://doi.org/10.1109/MNET.011.2000136.

[38] J. Mamvong, G. Goteng, Y. Gao, Low-cost client-side encryption and secure Internet of Things (IoT) provisioning, Front. Comput. Sci. 16 (6) (2022) 1–3, https://doi.org/10.1007/s11704-022-1256-9.

[39] A.S. Ahmed, M. Thakur, S. Paavolainen, T. Aura, Transparency of SIM profiles for the consumer remote SIM provisioning protocol, Annales Des Telecommunications/Annals of Telecommunications 76 (3–4) (2021) 187–202, https://doi.org/10.1007/s12243-020-00791-2.

[40] P.R. Sousa, L. Magalhães, J.S. Resende, R. Martins, L. Antunes, Provisioning, authentication, and secure communications for IoT devices on fiware, Sensors 21 (17) (2021) 1–24, https://doi.org/10.3390/s21175898.

[41] M. Brandt, et al., Security analysis of software-defined networking protocols OpenFlow, in: OF-config and OVSDB in IEEE ICCE 2014, 2014.

[42] Markus Tasch, Rahamatullah Khondoker, Ronald Marx, Kpatcha Bayarou, Security analysis of security applications for software defined networks, Proceedings of the 10th Asian Internet Engineering Conference (AINTEC '14) (2014) 23–30, https://doi.org/10.1145/2684793.2684797. Association for Computing Machinery, New York, NY, USA.

[43] Applying a Threat Model to Cloud Computing – OSTI.Gov, 2022. https://www.osti.gov/servlets/purl/1594657, 02-01.

[44] N. Kushalnagar, G. Montenegro, C. Schumacher, 'IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals, '' Microsoft Corp., New York, NY, USA, 2007. Tech. Rep. 2007A4919.

[45] H.I. Ahmed, A.A. Nasr, S. Abdel-Mageid, H.K. Aslan, A survey of IoT security threats and defenses, Int. J. Adv. Comput. Res. 9 (2019) 325–350.

[46] C. Costello, B. Smith, Montgomery curves and their arithmetic, J Cryptogr Eng 8 (2018) 227–240, https://doi.org/10.1007/s13389-017-0157-6.

[47] M.C. Chow, M. Ma, A secure blockchain-based authentication and key agreement scheme for 3GPP 5G networks, Sensors 22 (2022) 4525, https://doi.org/10.3390/s22124525.

[48] A.E. Azzaoui, S.K. Singh, Y. Pan, J.H. Park, Block5GIntell: blockchain for AI-enabled 5G networks, IEEE Access 8 (2020) 145918–145935, https://doi.org/10.1109/ACCESS.2020.3014356.

[49] P. Krishnan, A.V. Prabu, S. Loganathan, S. Routray, U. Ghosh, M. AL-Numay, Analyzing and managing various energy-related environmental factors for providing personalized IoT services for smart buildings in smart environment, Sustainability 15 (2023) 6548, https://doi.org/10.3390/su15086548.

[50] M. Kasiselvanathan, Teresa V.V. Manikandan Rajagopal, Prabhakar Krishnan, Performance analysis of alternating minimization based low complexity detection for MIMO communication system, Automatika 64 (4) (2023) 748–755, https://doi.org/10.1080/00051144.2023.2209416.

[51] A. Balasundaram, S. Routray, A. V. Prabu, P. Krishnan, P. P. Malla and M. Maiti, "Internet of things (IoT) based smart healthcare system for efficient diagnostics of health parameters of patients in emergency care," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2023.3246065..

[52] N. Singh, K. Jain, Data security approach using blockchain mechanism and cryptography algorithms. 2023 11th International Symposium on Digital Forensics and Security, ISDFS), USA, 2023, pp. 1–6, https://doi.org/10.1109/ISDFS58141.2023.10131789. Chattanooga, TN.

[53] M. Kataria, K. Jain, N. Subramanian, Exploring advanced encryption and steganography techniques for image security, in: 2023 11th International Symposium on Digital Forensics and Security, ISDFS), USA, 2023, pp. 1–6, https://doi.org/10.1109/ISDFS58141.2023.10131890. Chattanooga, TN.