DOI: 10.1561/9781638285076.ch12

Chapter 12

Cybersecurity Challenges and Pitfalls in 6G Networks

By Aristeidis Farao, Vaios Bolgouras, Apostolis Zarras and Christos Xenakis

The transition from 5G to 6G networks aims to improve connection speeds and intelligence levels. 6G is expected to support machine-type communications and ultra-reliable low-latency communications while enhancing mobile broadband services by integrating cutting-edge technologies. These advancements can potentially transform sectors, including healthcare and autonomous transportation systems; however, they bring security challenges. The open, distributed, and user-centric nature of 6G—marked by numerous connected devices, decentralized networks, and complex interactions between systems—makes traditional centralized security models inadequate. This shift introduces a broader attack surface with increased vulnerability to threats like API exploitation, data privacy violations, interception risks, and insider attacks. Applying blockchain and Self-Sovereign Identity (SSI) technologies is a promising approach to addressing the security concerns associated with 6G. These technologies provide decentralized and cryptographically secure systems that match the changing requirements of 6G. Blockchain technology ensures immutability, transparency, and tamper-proof record-keeping

across the network. Through smart contracts, it enforces security measures and validates API communications while safeguarding data integrity among the distributed nodes of 6G. In parallel, SSI supports managing identities where users possess authority over their verified identities, ensuring privacy protection and secure access control, diminishing the likelihood of identity theft or unauthorized access. The combination of blockchain and SSI addresses security issues in 6G. Incorporating blockchain and smart contracts can minimize the risks associated with API vulnerabilities. This integration allows only authorized users and devices to interact with APIs, while SSI provides verifiable credentials that confirm users' identities and prevent unauthorized access to APIs. Although the 6G distributed architecture expands the attack surface, it can be protected using the blockchain's decentralized security enforcement mechanisms, where nodes can effectively verify each other's settings and activities. Moreover, the immutability feature provided by blockchain and the selective disclosure capabilities offered by self-sovereign identity help protect the privacy and integrity of data, ensuring that confidential information remains secure even when there are risks of interception. This chapter explores how blockchain and self-sovereign identity can tackle the security issues in 6G, analyzing how these technologies can shape a secure 6G infrastructure.

12.1 Introduction

The advent of the 6G marks a significant leap forward in telecommunications, promising to reshape how industries, devices, and individuals connect and communicate. Building on top of 5G, 6G aspires to offer ultra-high speeds, ultra-low latency, and ubiquitous connectivity, driving the development of futuristic applications (e.g., autonomous vehicles). At this transformation's backbone lies a sophisticated and user-friendly Service-Based Architecture (SBA), which is open, distributed, and user-centric, enabling seamless integration of devices and services into a unified network. The open and distributed nature of the 6G network represents a paradigm shift from the relatively centralized architecture of previous generations. While this shift benefits flexibility, scalability, and support for a vast array of use cases, it also exposes the network to new cybersecurity threats. By increasing interconnectivity among network functions, services, and third-party applications, the 6G SBA amplifies the risk of vulnerabilities across various network layers. Particularly, 6G networks will rely on Application Programming Interfaces (APIs) to enable communication between disparate services and functions, opening up more potential attack vectors. Thus, misconfigured or insecure APIs may be gateways for attackers, allowing unauthorized access to sensitive data and critical network infrastructure. Works on 5G SBA have already demonstrated the vulnerability of

APIs [1–3], a risk that is expected to grow as 6G becomes more complex and interconnected significantly [4].

Beyond the inherent API vulnerabilities, the openness of 6G also raises concerns about data privacy and interception [5, 6]. In this new architecture, data flows more freely between network nodes, users, and third-party service providers. Without robust encryption protocols and strict access controls, sensitive information could be susceptible to interception by malicious actors through man-in-the-middle (MitM) attacks or unauthorized access points [7]. As more entities access different components of the 6G network, the potential for data breaches and privacy violations rises. Another critical challenge that 6G's distributed nature introduces is expanding the network's attack surface. Unlike 4G and 5G, which rely on centralized core networks, 6G distributes core network functions across multiple edge nodes, cloud environments, and virtualized infrastructure. This decentralization is crucial for delivering low-latency services and optimizing network efficiency, but it also creates numerous potential points of vulnerability [8, 9]. Each edge node, cloud server, or virtualized function becomes a cyberattack target. One of the most pressing threats in this environment is the risk of Distributed Denial of Service (DDoS) attacks. In such attacks, malicious actors flood specific nodes or network functions with excessive traffic, causing widespread disruptions or even complete network outages.

Moreover, the distributed nature of the 6G SBA complicates the enforcement of consistent security policies across the network. In centralized architectures, security protocols could be more easily implemented and managed from a single location. However, each node or service may require individual security configurations in a distributed environment. The shift toward a user-centric model in 6G also introduces novel security concerns. With 6G, users will gain unprecedented control over network resources and services, customizing configurations and privacy settings to suit their needs. While this empowers users and enhances the overall user experience, it also increases the likelihood of misconfigurations. Improperly configured network slices, insufficient security settings, or weak authentication practices can create significant vulnerabilities [10]. In addition, 6G will significantly increase the amount of sensitive personal data being transmitted and processed across the network, raising critical privacy concerns. As more industries adopt 6G technology—particularly sectors like healthcare, finance, and transportation—user data will include highly sensitive information, such as health records and financial transactions. This data must be adequately protected from unauthorized access or misuse, requiring the implementation of cutting-edge privacy-preserving technologies such as blockchain and Self-Sovereign-Identity (SSI). Balancing robust privacy protections with the seamless user experience that 6G promises will significantly challenge network designers and regulators.

12.2 Security Constraints and Vulnerabilities in 6G SBA Core Network

The security constraints and vulnerabilities of the 6G SBA core network are vast and multifaceted. This stems from the shift toward a more open, distributed, and user-centric architecture, which introduces numerous complexities and risks. As 6G becomes more advanced and interconnected, the potential attack surface expands significantly, creating opportunities for cyber threats to exploit weaknesses in the system. In analyzing these challenges, examining how API vulnerabilities, distributed architecture, data privacy, and user misconfigurations contribute to the overall security risks facing 6G networks is crucial.

12.2.1 API Vulnerabilities

The development of 6G introduces significant advances in network architecture, but with it comes an increased reliance on APIs [11], which presents opportunities and security challenges. APIs are critical for enabling the open and distributed nature of 6G, allowing different services, applications, and network functions to communicate seamlessly [12]. However, this openness also makes APIs prime cyberattack targets [13].

API vulnerabilities can arise from weak authentication mechanisms, inadequate encryption, or insecure communication channels. The consequences of API attacks include but are not limited to data exposure, compromised authentication mechanisms, and service interruptions [14]. In the context of 5G and beyond, works have already revealed that insecure APIs have been a point of exploitation [1, 4, 15], and with 6G, these vulnerabilities are expected to be even more pronounced [16, 17]. In particular, as APIs will serve as interfaces within the network and with third-party services, the security challenges multiply, necessitating stringent security protocols at every layer. API attacks can take various forms, such as MitM attacks, where an attacker intercepts data during transmission between services, or API injection attacks, where malicious code is inserted into the API request to manipulate data or compromise the system. These threats underscore the importance of implementing robust encryption, authentication, and access control measures. End-to-end encryption is essential to ensure that data transmitted through APIs is protected from eavesdropping or tampering, while strong authentication mechanisms, such as OAuth or mutual TLS, can help prevent unauthorized access. Moreover, API vulnerabilities can become even more concerning in distributed network environments like those seen in 6G, where services are spread across multiple edge nodes and cloud infrastructures. Each API call made between services represents a potential point of failure.

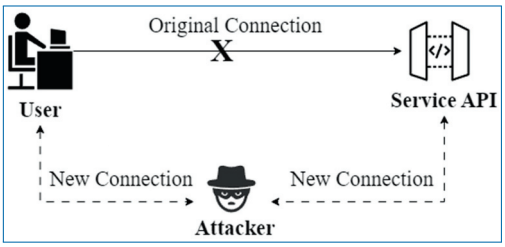

Figure 12.1. Cybersecurity attack in API.

The following are the most common cybersecurity attacks that can exploit APIs (see Figure 12.1) in 5G and beyond networks [4, 19]:

- MitM Attacks: the attacker intercepts the data transmitted between different network components, such as between the core network and third-party applications. This can lead to data breaches, manipulation of messages, or session hijacking. In 5G and beyond networks, as APIs are more widely used for communication between network slices, edge computing, and other services, MitM attacks can be more prevalent without proper encryption.
- API Injection Attacks: an attacker inserts malicious data or code into API requests, leading to unintended behavior or compromising network services. With the growing complexity of APIs in 6G, particularly those managing real-time data flows and edge computing services, injection attacks could lead to critical infrastructure disruptions.
- DoS and DDoS Attacks: an API is overwhelmed with a large volume of requests, causing it to slow down or crash, making the service unavailable to legitimate users. In a DDoS attack, multiple compromised devices (e.g., a botnet) are used to flood the API. Given that networks support many devices, including IoT and edge devices, APIs are particularly vulnerable to DDoS attacks that target the availability of network functions. Unprotected APIs can serve as easy entry points for such attacks, leading to disruptions in service.
- Broken Authentication and Session Management: APIs often manage authentication and session tokens to verify users and services. If attackers gain access to session tokens due to insecure APIs, they can hijack user sessions, impersonate legitimate users, and gain unauthorized access to sensitive network services. Broken authentication can occur if APIs fail to manage user credentials and tokens securely or if session expiration is not handled properly. Where there are diverse and distributed access points across devices, the risk of broken authentication increases.
- Cross-Site Scripting (XSS): attackers inject malicious scripts into an API response, which can then be executed in the user's browser. In scenarios where APIs serve web applications or user interfaces, an attacker can exploit

vulnerabilities in API responses to inject malicious code. This can lead to session hijacking, redirection to malicious websites, or stealing sensitive data. XSS is especially dangerous when APIs are exposed to third-party services, a common feature in 6G networks.

- Replay Attacks: an attacker intercepts valid API requests and resends them to the server, attempting to replicate valid actions or requests. Without mechanisms like timestamps or nonce (a random number used only once), replay attacks can exploit API sessions, such as resubmitting a payment request or gaining repeated access to services. Replay attacks can be especially dangerous in 6G environments where real-time data transfers, such as autonomous vehicle communication, rely on API exchanges.

12.2.2 Distributed Architecture and Increased Attack Surface

The distributed architecture of 5G and 6G networks significantly widens the attack surface, presenting new cybersecurity challenges [5]. 5G and 6G adopt a decentralized approach where core network functions are distributed across various edge nodes. This transformation introduces operational advantages like lower latency, enhanced scalability, and more flexible service deployment. However, it also opens up many potential entry points for cyberattacks. As each node, server, and API becomes a critical network component, attackers have more opportunities to exploit vulnerabilities, disrupt services, or steal data [20].

In 6G, where services are widely distributed across edge nodes and cloud environments, a DDoS attack targeting a key node could cause significant disruptions to critical network services. As 5G and 6G networks rely heavily on edge computing to deliver low-latency services, particularly for various applications [21] (e.g., autonomous driving), the impact of a DDoS attack could be devastating. By targeting the edge, attackers can disrupt data flow between devices and the cloud, degrade service performance, or cause complete service outages [22]. Moreover, 6G will further increase reliance on edge infrastructure, meaning that the attack surface for DDoS attacks will continue to expand. It has already been emphasized that 5G/6G networks need robust DDoS protection mechanisms, including AI-driven traffic filtering, anomaly detection, and adaptive firewalls [23, 24]. These technologies can help detect malicious traffic patterns early and mitigate the effects of DDoS attacks. AI and machine learning can analyze network traffic in real time, identifying anomalies that may indicate an ongoing attack [25, 26].

Moreover, the distributed edge computing environment, which brings network services closer to the user, also increases the number of potential targets for attackers. The more edge nodes that exist, the more points of vulnerability an attacker can target [27]. Unlike a centralized system where security can be more easily managed,

distributed architectures create a challenge in implementing and enforcing consistent security policies across every node. Edge nodes may not have the same level of security or processing power as centralized cloud systems, making them more vulnerable to attacks. If an edge node is compromised, an attacker could access sensitive data, disrupt services, or even infiltrate the broader network. Securing edge nodes requires ensuring each node is properly configured, regularly updated, and equipped with strong access control measures [28].

Implementing consistent security policies across a distributed architecture is a significant challenge. In a 5G/6G network, different nodes and servers may be owned or operated by different entities, each with its own security protocols. Ensuring that security policies are enforced uniformly across these disparate infrastructures is crucial to maintaining the integrity of the overall network. This challenge is compounded by the fact that 6G networks will support various services with varying security requirements [29]. Some services, like those handling sensitive data, will require stringent security measures, including strong encryption, while others may prioritize low-latency or high-throughput performance over security. Therefore, orchestration tools are essential in ensuring that the right security policies are applied to each part of the network, depending on the service it delivers [30]. Automated orchestration and management tools powered by AI can help address this challenge by dynamically configuring and enforcing security policies across the network. These tools can ensure that security measures such as encryption, authentication, and access control are consistently applied across different network slices, cloud environments, and edge nodes.

Finally, in 6G networks, many core network functions will be virtualized and deployed as Virtualized Network Functions (also known as VNFs). On the one hand, this approach offers greater flexibility and scalability; on the other hand, it introduces new cybersecurity risks. Virtualization layers can become targets for attackers who may attempt to compromise the hypervisor or exploit vulnerabilities in VNFs to gain access to underlying network resources. This risk is particularly pronounced in 6G, where VNFs are expected to handle increasingly complex tasks (e.g., managing AI-driven services). Ensuring the security of VNFs requires robust isolation mechanisms to prevent attackers from moving laterally within the network and continuous monitoring for vulnerabilities at the virtualization layer [31].

12.2.3 Data Privacy and Interception Risks

In 5G and 6G networks, data privacy and interception risks are key concerns due to the scale and complexity of the infrastructure. As mobile networks evolve to accommodate a massive number of connected devices and the diverse services that characterize 6G, ensuring the protection of user data becomes more challenging.

The transition to SBA introduces new vulnerabilities and opens up various points where sensitive data can be intercepted or exposed. These risks require comprehensive security measures, as increased network nodes and distributed services magnify the potential attack surface.

One of the primary privacy concerns in 6G networks is the sheer volume of personal data transmitted and processed across the network [32]. As 6G enables more advanced applications (e.g., autonomous vehicles), the data generated from these services grows exponentially. Much of this data is personal or sensitive [33]. If improperly secured, malicious actors can intercept this data during transmission or be compromised at storage points across the network. In 6G, a distributed architecture shifts much of the data processing to the network's edge—closer to the end-user devices [34]. While this reduces latency and enhances performance, it also introduces more points of vulnerability. Each edge node becomes a potential target for attackers looking to intercept data as it moves between devices and the core network. In addition to edge nodes, network slices pose privacy risks if not properly secured [35]. Network slicing allows operators to allocate virtualized resources to different services or customers based on their needs, enabling faster, more tailored service delivery. However, with multiple network slices running simultaneously, each tailored for a specific use case, a security flaw in one slice could expose data traversing the entire network. Attackers could potentially exploit vulnerabilities in a low-security slice to gain access to more sensitive slices, compromising user data or even intercepting critical information such as authentication credentials.

Beyond malicious attacks, data interception can also occur due to poorly implemented security protocols or weak encryption standards. As more data flows across diverse and distributed infrastructure, it is crucial that strong encryption protocols are applied consistently [36]. Another layer of risk comes from quantum computing, which, although not yet widely available, could eventually break many of the encryption algorithms currently in use. As 6G networks are expected to be operational well into the future, the post-quantum security of encryption methods must be considered. Quantum computers could theoretically decrypt intercepted previously thought secure data, posing a significant future risk. The evolving nature of 6G networks also means that traditional identity and access management strategies may not be sufficient to protect against data interception. As the number of devices and users connecting to the network increases, ensuring that only authorized entities access data and services becomes more complex.

12.2.4 User Misconfiguration and Insider Threats

The introduction of 6G networks, with their advanced capabilities such as ultra-low latency, high-speed data transfer, and massive connectivity, presents transformative

potential for various industries. However, the complexity of these networks also creates numerous security vulnerabilities that must be addressed. While much attention is paid to external threats (see above), user misconfigurations and insider threats remain significant and often underestimated risks. The aftermath of such a threat includes but is not limited to unintentional data breaches. In the context of 6G, the challenges posed by user misconfigurations and insider threats will likely grow.

The most common vulnerability in modern networks is human error, often misconfigurations [37]. This risk is heightened in complex, decentralized networks like 6G because the architecture requires multi-layered configurations, each with its own set of protocols and security mechanisms. Misconfigurations can occur when settings related to network access, data encryption, or firewall rules are incorrectly applied, inadvertently creating backdoors for cyberattacks [38–42]. In addition, The SBA and network slicing inherent to 6G present additional risks. In SBA, individual services are separated into microservices, each requiring its own configuration and security settings [43]. The entire network's security posture may be compromised if any of these services are misconfigured. Additionally, network slicing, which allows for creating multiple virtual networks on top of a single physical infrastructure, requires precise configuration to ensure each slice is properly isolated and secure. A single misstep in the configuration process [43] can expose sensitive data across different network slices or grant access to unauthorized entities, causing potentially widespread damage. Cloud misconfigurations [44] account for 15% of initial attack vectors in security breaches—the third most common initial attack vector in breaches. On average, these types of data breaches take 186 days to identify and yet another 65 to deal with. Misconfigurations like this cost companies around 3.86 million dollars in total costs [45]. Besides the unintentional misconfigurations, insider threats pose a serious risk to 6G networks. These occur when individuals with authorized access to the network misuse their privileges, either intentionally to cause harm or unintentionally through negligence [46]. The potential for insider threats is substantial in 6G, where millions of devices and users will be connected. Insider threats are particularly dangerous because they often come from trusted individuals with legitimate access to sensitive areas of the network, making detection more difficult.

12.3 Candidate Technologies

At this point, we present the technological pillars that jointly can provide a robust solution for the 6G network ecosystem. The proposed solutions have been designed on the grounds of well-established technologies (i.e., Blockchain, Smart Contracts, and SSI) with proven security properties.

12.3.1 Blockchain

Blockchain [47] is a decentralized, distributed ledger technology that enables secure, transparent, and immutable record-keeping of transactions across multiple participants without the need for a central authority or intermediary. Blockchain networks can be public, private, consortium, or hybrid. Public blockchains are decentralized and open to anyone, with no central authority, where anyone can participate in the consensus process. On the other hand, private blockchains are restricted and governed by a single organization, making them more centralized and suitable for enterprise use where control over participants is needed. Consortium blockchains are semi-decentralized, where a group of organizations collectively manage the blockchain, offering a balance between openness and control, often used in industries like finance or supply chains. Finally, hybrid blockchains combine elements of both public and private models, allowing certain data to be publicly accessible while keeping sensitive information private, enabling flexibility and control in specific use cases like healthcare or government services.

Blockchain's security is underpinned by cryptographic techniques such as hashing and digital signatures. Every participant on the blockchain network has a pair of public and private keys used to sign and verify transactions. These digital signatures ensure that only the rightful owner of a private key can authorize a transaction, providing a robust form of authentication. In addition, blockchain networks rely on consensus mechanisms [48] to validate transactions. These mechanisms ensure that only legitimate transactions are added to the blockchain and that the network is resilient to attacks. For 6G networks, which are expected to handle vast amounts of data and devices, blockchain's security features can help authenticate devices, secure data exchanges, and ensure that communication between network nodes remains tamper-proof. The consensus mechanism is the process by which blockchain networks agree on the ledger's state. These mechanisms are critical to ensuring that the blockchain remains decentralized and secure. Consensus mechanisms ensure that all nodes in the network agree on the transactions being added to the blockchain, thus maintaining the system's integrity.

Blockchain [49] works by creating a chain of blocks, each containing a list of transactions. Every block is cryptographically linked to the previous block, forming an unalterable chain of records. This cryptographic linkage, combined with the distributed nature of blockchain, provides enhanced security, transparency, and trust. The most defining feature of blockchain is its decentralized nature. Unlike traditional centralized databases that rely on a single entity to manage and validate transactions, blockchain networks operate on a peer-to-peer basis. Each node in the network maintains a copy of the entire blockchain, ensuring that the system remains operational even if some nodes go offline or attempt to manipulate

data. Decentralization removes the need for intermediaries, reducing costs and the potential for manipulation or fraud. Another critical feature is the use of smart contracts [47, 49]. These are self-executing contracts with the terms of the agreement directly written into code. They automatically execute and enforce the contract's terms when predefined conditions are met. Smart contracts enable automation of transactions and processes, reducing the need for intermediaries and enhancing efficiency. In 6G networks, smart contracts could manage resource allocation, automate service provisioning, or enforce network security policies, providing real-time, trustworthy execution without human intervention.

Another critical feature is immutability, which refers to the fact that once data is recorded on the blockchain, it cannot be altered or deleted. This is achieved through the use of cryptographic hashing. Each block in the chain contains a unique cryptographic hash of the previous block, linking them together to ensure any attempt to alter the data in a block would require changing all subsequent blocks. Such a task would require controlling more than 50% of the network's computing power [50] This feature is critical for applications that require reliable and tamper-proof records (e.g., supply chain management, where tracking the origin and authenticity of products is mandatory). In 6G networks, immutability could be used to maintain accurate logs of data exchanges, device authentication, or even service provisioning. In addition, Blockchain promotes transparency by making all transaction data visible to every participant in the network. Each node maintains a complete copy of the ledger, and the transactions are verified by the consensus of the network participants before being added to the blockchain. While public blockchains are fully transparent, where all transaction details are viewable, permissioned blockchains used in enterprises can restrict access to certain information, allowing for a more controlled form of transparency. This transparency builds trust between participants, even when they do not know or fully trust one another. In telecommunications and 6G, blockchain can create a transparent environment for managing decentralized resources, such as network slices, or for enabling seamless, trust-based interactions between devices in IoT ecosystems.

12.3.2 Self-Sovereign-Identity

Self-Sovereign Identity [47], also known as SSI, is an example of a decentralized identity management system. Thanks to this, individuals or organizations can take ownership of and control their digital identities. As an additional benefit, SSI makes it easier to engage in selective attribute disclosure, a method for minimizing the disclosure of personal information. Additionally, it provides features that protect users' privacy, such as anonymity and the inability to be linked to an individual. With SSI, no central authority keeps ownership of users' data, which eliminates the

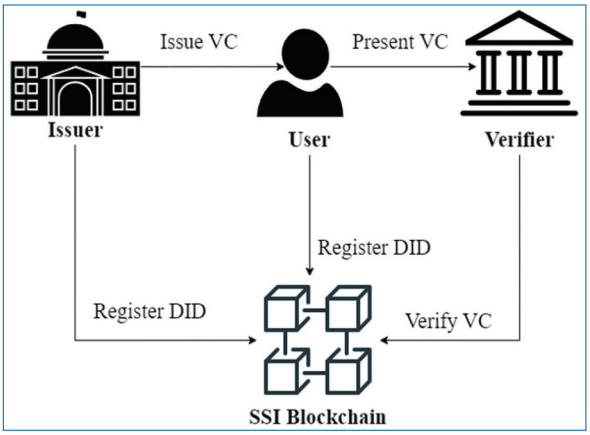

Figure 12.2. SSI functionalities.

requirement to provide it to other people when they request it. The user is the one that carries their data, and because of the encryption and distributed ledger technology that underpins it, the user can make assertions about its identity, which other entities can verify with cryptographic certainty. With the help of SSI, stakeholders in the 6G networks can exchange verified data in a way that is both automated and respectful of their privacy. This technique eliminates the need for manual data verification processes, which not only helps to prevent the disclosure of confidential information but also saves time. SSI is built on the foundation of Verifiable Credentials, also known as VCs. VCs were defined by the World Wide Web Consortium (W3C) as tamper-evident credentials with authorship that can be cryptographically confirmed [51]. This proposal was published as a formal recommendation. VCs can enhance interoperability and selective disclosure of information pertaining to its holders.

An issuer, a user, and a verifier are the three types of participants actively involved in the SSI framework (see Figure 12.2). Two fundamental features constitute the SSI: *(i)* the issuance of VC and *(ii)* the verification of VC. VC Issuance is the initial functionality that allows the user to obtain a VC from the issuer while acting in the holder's role. VC consists of tamper-evident claims and information that provide cryptographic proof of the authenticity of its issuer. *Claims* are statements a holder makes, such as the holder's birth year. Every VC is issued on the Decentralized Identifiers (DIDs) of its holder and issuer, serving as a public key within the blockchain ecosystem. A DID is a globally unique identifier. It is made up of a string of letters and numbers and is directly associated with a pair of public and secret keys simultaneously. Using the private key, the holder can access and manage their data. The holder is the only entity who should be aware of the private key, and its information should never be disclosed to any other individual. Concerning DIDs, the

private key enables holders to demonstrate ownership and authorize authorization to share particular data. Blockchain, on the other hand, is a distributed ledger that maintains the public key that is connected with the DID of the VC's issuer public key. This public key can be safely shared with anybody to send and receive data. VCs that have been issued are stored in a secure manner in a digital identity wallet. This wallet is the location (for example, a mobile app) where holders maintain their VCs [52]. It is not possible to host these just within cell phones; rather, certain implementations permit their hosting within trusted computers.

The second functionality is VC Verification, in which the holder (acting as the prover) must demonstrate to the verifier that he holds accurate attributes without necessarily exposing the values included within those attributes. Establishing that the corresponding user is, in fact, in control of the provided identity is how this objective is accomplished through the utilization of zero-knowledge proofs. The verifier must check the Blockchain to view the VC's issuer (i.e., the DID of the VC's issuer) to validate the legitimacy of the venture capital. This can be done without the need to contact the issuer. When presenting a VC, the prover has the ability to choose which claims to reveal and which to keep hidden. An additional benefit of SSI is that it can accomplish unlinkability because the user uses a unique DID for each presentation.

12.4 Facing the Challenges

Blockchain and SSI technologies hold tremendous potential in addressing the cybersecurity challenges faced by 6G networks. These next-generation networks bring unprecedented speed, connectivity, and automation but also present new vulnerabilities, including identity management, data privacy, and system integrity. Security becomes an essential concern as 6G networks aim to create an open, distributed, and user-centric environment. In this section, we will explore how blockchain and SSI can be used to tackle the key cybersecurity challenges inherent in the evolving landscape of 6G networks.

12.4.1 Addressing the API Vulnerabilities

API vulnerabilities have been a persistent security issue in modern networks and are expected to pose even greater risks in 6G. APIs are essential communication bridges between applications, devices, and services in highly interconnected and distributed environments. As 6G networks introduce more open and decentralized interfaces, poorly secured APIs could become prime targets for attackers, enabling them to intercept sensitive data, manipulate services, or execute malicious code.

On the one hand, Blockchain's inherent decentralization and transparency can significantly enhance the security of API interactions in 6G networks. By using a distributed ledger, Blockchain can verify and record every API transaction, ensuring that each interaction between devices or services is cryptographically signed and time-stamped. This means that unauthorized modifications to API requests and responses can be easily detected, as all interactions are recorded in an immutable ledger accessible to network participants. Blockchain also offers the potential for smart contract-based APIs. Smart contracts can enforce predefined rules and security policies on API transactions. These contracts can automatically ensure that only authorized devices, applications, and users can access certain APIs. This would eliminate many common API vulnerabilities, such as unauthorized access, excessive data exposure, and parameter tampering, often exploited in traditional networks.

On the other hand, SSI is crucial in securing API access by providing a decentralized approach to identity management. In an SSI model, users and devices control their own cryptographically verified identities without needing a central authority. In the context of APIs, SSI can ensure that only authenticated and authorized entities gain access to the network's APIs. By integrating SSI, 6G networks can ensure that each API request is associated with a verifiable, cryptographically secure identity. This eliminates the risk of unauthorized devices or users accessing sensitive APIs, as each API request must be accompanied by verifiable credentials stored in decentralized identity wallets. Furthermore, since users have complete control over their identity data, the risk of identity theft or impersonation through compromised API endpoints is minimized.

12.4.2 Securing Distributed Architecture and Mitigating Increased Attack Surface

One of the defining characteristics of 6G networks is their distributed architecture, which significantly expands the network's attack surface. With numerous devices, edge nodes, and services distributed across the network, traditional security models that rely on centralized control are ineffective.

In a blockchain-based system, there is no single point of failure; instead, security is enforced collectively by all participants in the network. This decentralized security model is particularly effective in environments like 6G, where data and devices are spread across multiple nodes. Each 6G device or edge node could participate in the blockchain network, where security policies, configurations, and access controls are transparently managed and enforced through consensus. Using Blockchain's peer-to-peer validation, network participants can collectively verify the authenticity of each device, transaction, and service in real time, ensuring that no compromised device can subvert the network's integrity.

In traditional networks, a central authority manages identity verification, which becomes a bottleneck in decentralized environments. However, SSI can eliminate this bottleneck by giving each user and device control over their own VCs, which can be securely stored and shared without relying on a centralized authority. In 6G networks, SSI enables decentralized authentication across all devices and nodes, ensuring that only verified participants can access network resources and perform transactions. As SSI credentials are cryptographically secure, they can be validated by any party in the network, preventing unauthorized access. SSI also allows for granular access control, where devices and users can selectively share specific credentials to gain access to particular services. This reduces the attack surface, as entities only expose the minimal necessary information to perform a transaction, making it harder for attackers to exploit the system.

12.4.3 Addressing Data Privacy and Interception Risks

Data privacy and interception risks are heightened in 6G networks due to the sheer volume of sensitive data being transmitted across the network. In addition to the potential for data breaches, there is the risk of eavesdropping, where attackers intercept data as it moves between devices, edge nodes, or applications. Given the reliance on edge computing and multi-access edge networks, data no longer resides in centralized data centers but is processed closer to the user, increasing its vulnerability to interception.

Blockchain's immutability and encryption mechanisms offer strong guarantees for ensuring the integrity and confidentiality of data in 6G networks. By recording each data transaction in an immutable ledger, Blockchain ensures that any attempt to modify or tamper with data is immediately detectable. This is particularly valuable in 6G environments where data might traverse multiple edge nodes before reaching its final destination. Furthermore, Blockchain can facilitate data encryption, ensuring that only authorized entities can access the transmitted information. Even if an attacker intercepts the data in transit, they cannot decrypt it without the proper cryptographic keys, which are securely managed through blockchain-based key distribution systems.

Next, one of the key features of SSI is its focus on data minimization and user control over personal information. In an SSI framework, users can selectively share only the necessary attributes required to perform a transaction, minimizing the risk of data exposure. This feature is invaluable in the context of 6G networks, where personal data is constantly being transmitted between devices, applications, and services. SSI allows users to control what information is shared and with whom, using cryptographically verifiable claims. This ensures that even if an attacker gains access

to the transmitted data, they cannot infer sensitive information, as only minimal and necessary data points would be revealed.

As 6G networks introduce unprecedented connectivity, speed, and decentralization, they also bring cybersecurity challenges. Blockchain and SSI technologies offer powerful solutions to address these issues by providing decentralized, cryptographically secure frameworks for managing identities, securing data, and enforcing security policies. Blockchain's immutability, transparency, and distributed consensus mechanisms make it an ideal solution for securing API interactions, enforcing decentralized security policies, and maintaining data integrity in 6G networks. Meanwhile, SSI empowers users and devices with control over their identities, reducing the risk of unauthorized access and protecting personal data through selective disclosure and cryptographic proofs. Together, these technologies offer a robust, decentralized security architecture that aligns with the distributed, open nature of 6G networks. By integrating Blockchain and SSI, 6G networks can become more resilient, secure, and privacy-preserving, laying the foundation for a safer and more trustworthy digital future.

Acknowledgments

This Chapter has received funding from the European Commission's Horizon Europe programs under grant agreements No. 101131292 (AIAS) and No. 101139031 (SAFE6G).

References

[1] Tang, Q., Ermis, O., Nguyen, C. D., De Oliveira, A., & Hirtzig, A. (2022). A systematic analysis of 5g networks with a focus on 5g core security. IEEE Access, 10, 18298–18319.

[2] Dolente, F., Garroppo, R. G., & Pagano, M. (2023). A Vulnerability Assessment of Open-Source Implementations of Fifth-Generation Core Network Functions. Future Internet, 16(1), 1.

[3] Wehbe, N., Alameddine, H. A., Pourzandi, M., & Assi, C. (2024). Empowering 5G SBA security: Time series transformer for HTTP/2 anomaly detection. Computers & Security, 104114.

[4] Porambage, P., Gür, G., Osorio, D. P. M., Liyanage, M., Gurtov, A., & Ylianttila, M. (2021). The roadmap to 6G security and privacy. IEEE Open Journal of the Communications Society, 2, 1094–1122.

[5] Nguyen, V. L., Lin, P. C., Cheng, B. C., Hwang, R. H., & Lin, Y. D. (2021). Security and privacy for 6G: A survey on prospective technologies and challenges. *IEEE Communications Surveys & Tutorials*, *23*(4), 2384–2428.

[6] Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S., & Zhou, W. (2020). Security and privacy in 6G networks: New areas and new challenges. *Digital Communications and Networks*, *6*(3), 281–291.

[7] Kazmi, S. H. A., Hassan, R., Qamar, F., Nisar, K., & Ibrahim, A. A. A. (2023). Security concepts in emerging 6G communication: Threats, countermeasures, authentication techniques and research directions. *Symmetry*, *15*(6), 1147.

[8] Kehelwala, J., Siriwardhana, Y., Hewa, T., Liyanage, M., & Ylianttila, M. (2024, June). Decentralized Learning for 6G Security: Open Issues and Future Directions. In *2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)* (pp. 1175–1180). IEEE.

[9] Ferrag, M. A., Friha, O., Kantarci, B., Tihanyi, N., Cordeiro, L., Debbah, M., ... & Choo, K. K. R. (2023). Edge learning for 6G-enabled Internet of Things: A comprehensive survey of vulnerabilities, datasets, and defenses. *IEEE Communications Surveys & Tutorials*.

[10] Mao, B., Liu, J., Wu, Y., & Kato, N. (2023). Security and privacy on 6g network edge: A survey. *IEEE communications surveys & tutorials*, *25*(2), 1095–1127.

[11] Beyond bit-pipes – new opportunities on the 6G platform, Ericsson, Online: https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/6g-platform [Last access: 23/9/2024].

[12] 6G Security – drivers and needs, Ericsson White Papers, Online: https://www.ericsson.com/49c1cd/assets/local/reports-papers/white-papers/2024/6g-security-drivers-and-needs.pdf [Last access: 23/9/2024].

[13] Oliveira, D. S., Lin, T., Rahman, M. S., Akefirad, R., Ellis, D., Perez, E., ... & Brun, Y. (2018). {API} blindspots: Why experienced developers write vulnerable code. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* (pp. 315–328).

[14] Khan, M. S., Siam, R. S. F., & Adnan, M. A. (2024). A framework for checking and mitigating the security vulnerabilities of cloud service RESTful APIs. *Service Oriented Computing and Applications*, 1–22.

[15] Bjerre, S. A., Blomsterberg, M. W. K., & Andersen, B. (2022, October). 5G attacks and countermeasures. In *2022 25th International Symposium on Wireless Personal Multimedia Communications (WPMC)* (pp. 285-290). IEEE.

[16] Siriwardhana, Y., Porambage, P., Liyanage, M., & Ylianttila, M. (2021, June). AI and 6G security: Opportunities and challenges. In *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)* (pp. 616–621). IEEE.

[17] Je, D., Jung, J., & Choi, S. (2021). Toward 6G security: technology trends, threats, and solutions. *IEEE Communications Standards Magazine*, *5*(3), 64–71.

[18] Martin-Lopez, A., Segura, S., & Ruiz-Cortés, A. (2022, November). Online testing of RESTful APIs: Promises and challenges. In *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (pp. 408–420).

[19] Soltani, S., Shojafar, M., Amanlou, A., & Tafazolli, R. (2024). Intelligent Control in 6G Open RAN: Security Risk or Opportunity?. *arXiv preprint arXiv:2405.08577*.

[20] Ramezanpour, K., & Jagannath, J. (2022). Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Computer Networks*, *217*, 109358.

[21] Alotaibi, B. (2023). A survey on industrial Internet of Things security: Requirements, attacks, AI-based solutions, and edge computing opportunities. *Sensors*, *23*(17), 7470.

[22] Uddin, R., Kumar, S. A., & Chamola, V. (2024). Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. *Ad Hoc Networks*, *152*, 103322.

[23] Cunha, J., Ferreira, P., Castro, E. M., Oliveira, P. C., Nicolau, M. J., Núñez, I., ... & Serôdio, C. (2024). Enhancing Network Slicing Security: Machine Learning, Software-Defined Networking, and Network Functions Virtualization-Driven Strategies. *Future Internet*, *16*(7), 226.

[24] Karatisoglou, M., Farao, A., Bolgouras, V., & Xenakis, C. (2022, June). BRIDGE: BRIDGing the gap bEtween CTI production and consumption. In *2022 14th International Conference on Communications (COMM)* (pp. 1–6). IEEE.

[25] Petihakis, G., Farao, A., Bountakas, P., Sabazioti, A., Polley, J., & Xenakis, C. (2024, July). AIAS: AI-ASsisted cybersecurity platform to defend against adversarial AI attacks. In *Proceedings of the 19th International Conference on Availability, Reliability and Security* (pp. 1–7).

[26] Pantelakis, V., Bountakas, P., Farao, A., & Xenakis, C. (2023, August). Adversarial machine learning attacks on multiclass classification of iot network traffic. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (pp. 1–8).

[27] Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., & Lv, W. (2019). Edge computing security: State of the art and challenges. *Proceedings of the IEEE*, *107*(8), 1608–1631.

[28] Ravidas, S., Lekidis, A., Paci, F., & Zannone, N. (2019). Access control in Internet-of-Things: A survey. *Journal of Network and Computer Applications*, *144*, 79–101.

[29] Zhang, Z., Xiao, Y., Ma, Z., Xiao, M., Ding, Z., Lei, X., ... & Fan, P. (2019). 6G wireless networks: Vision, requirements, architecture, and key technologies. *IEEE vehicular technology magazine*, *14*(3), 28–41.

[30] De Sousa, N. F. S., Perez, D. A. L., Rosa, R. V., Santos, M. A., & Rothenberg, C. E. (2019). Network service orchestration: A survey. *Computer Communications*, *142*, 69–94.

[31] Repetto, M. (2023). Adaptive monitoring, detection, and response for agile digital service chains. *Computers & Security*, *132*, 103343.

[32] Tripi, G., Iacobelli, A., Rinieri, L., & Prandini, M. (2024). Security and Trust in the 6G Era: Risks and Mitigations. *Electronics*, *13*, 2162.

[33] Hexa-X and data protection evolution in 6G, Ericsson Blog, Online: https://www.ericsson.com/en/blog/2023/10/hexa-x-and-data-protection-evolution-in-6g [Last access:23/9/2024].

[34] Ishtiaq, M., Saeed, N., & Khan, M. A. (2021). Edge computing in IoT: A 6G perspective. *arXiv preprint arXiv:2111.08943*.

[35] Singh, V. P., Singh, M. P., Hegde, S., & Gupta, M. (2024). Security in 5G Network Slices: Concerns and Opportunities. *IEEE Access*.

[36] Wang, Y., Kang, X., Li, T., Wang, H., Cheng, C., & Lei, Z. (2023). SIX-Trust for 6G: Towards a Secure and Trustworthy Future Network. *IEEE Access*.

[37] Petihakis, G., Kiritsis, D., Farao, A., Bountakas, P., Panou, A., & Xenakis, C. (2023, August). A Bring Your Own Device security awareness survey among professionals. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (pp. 1–10).

[38] Yungaicela-Naula, N. M., Sharma, V., & Scott-Hayward, S. (2024). Misconfiguration in O-RAN: Analysis of the impact of AI/ML. *Computer Networks*, 110455.

[39] Muñoz, A., Farao, A., Correia, J. R. C., & Xenakis, C. (2021). P2ISE: preserving project integrity in CI/CD based on secure elements. Information, 12(9), 357.

[40] Suciu, G., Farao, A., Bernardinetti, G., Palamà, I., Sachian, M. A., Vulpe, A., … & Xenakis, C. (2022). SAMGRID: security authorization and monitoring module based on SealedGRID platform. *Sensors*, *22*(17), 6527.

[41] Kalderemidis, I., Farao, A., Bountakas, P., Panda, S., & Xenakis, C. (2022, August). GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1–9).

[42] Farao, A., Panda, S., Menesidou, S. A., Veliou, E., Episkopos, N., Kalatzantonakis, G., … & Xenakis, C. (2020). SECONDO: A platform for cybersecurity investments and cyber insurance decisions. In Trust, Privacy and Security in Digital Business: 17th International Conference, TrustBus 2020,

Bratislava, Slovakia, September 14–17, 2020, Proceedings 17 (pp. 65–74). Springer International Publishing.

[43] Scalise, P., Boeding, M., Hempel, M., Sharif, H., Delloiacovo, J., & Reed, J. (2024). A Systematic Survey on 5G and 6G Security Considerations, Challenges, Trends, and Research Areas. *Future Internet*, *16*(3), 67.

[44] 40+ Alarming Cloud Security Statistics for 2024, strongdm, Online: https://www.strongdm.com/blog/cloud-security-statistics#:~:text=just%20internal%20mistakes.-,Cloud%20misconfigurations%20account%20for%2015%25%20of%20initial%20attack%20vectors%20in,another%2065%20to%20deal%20with. [Last access: 23/9/2024].

[45] PurpleSec, 2024 Cybersecurity Statistics, The Ultimate List Of Cybersecurity Stats Data, & Trends, Online: https://purplesec.us/resources/cybersecurity-statistics/ [Last access: 23/9/2024].

[46] Pandey, D., Goyal, S., Bhaumik, K., Suneja, S., Sharma, M., & Dadheech, P. D. (2024). A Systematic Review of Security Issues in 6G Networks and Communication. *Security Issues and Solutions in 6G Communications and Beyond*, 1–11.

[47] Farao, A., Paparis, G., Panda, S., Panaousis, E., Zarras, A., & Xenakis, C. (2024). INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain. *International Journal of Information Security*, *23*(1), 347–371.

[48] Bamakan, S. M. H., Motavali, A., & Bondarti, A. B. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. Expert Systems with Applications, 154, 113385.

[49] Voudouris, A., Farao, A., Panou, A., Polley, J., & Xenakis, C. (2024, July). Integrating Hyperledger Fabric with Satellite Communications: A Revolutionary Approach for Enhanced Security and Decentralization in Space Networks. In *Proceedings of the 19th International Conference on Availability, Reliability and Security* (pp. 1–8).

[50] Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied sciences*, *9*(9), 1788.

[51] World Wide Web Consortium (W3C).: Verifiable credentials data model v1.1. Online: https://www.w3.org/TR/vc-data-model/ [Last Access: 23/09/2024]

[52] Farao, A., Veroni, E., Ntantogian, C., & Xenakis, C. (2021). P4G2Go: a privacy-preserving scheme for roaming energy consumers of the smart grid-to-go. Sensors, 21(8), 2686.