Attribute-Based Access Control Utilizing Verifiable Credentials for Multi-Tenant IoT Systems

C.D. Nassar Kyriakidou
Mobile Multimedia Laboratory
Department of Informatics
AUEB, Greece
dnassar@aueb.gr

A.M. Papathanasiou
Mobile Multimedia Laboratory
Department of Informatics
AUEB, Greece
sissypapathanasiou@aueb.gr

I. Pittaras
Mobile Multimedia Laboratory
Department of Informatics
AUEB, Greece
pittaras@aueb.gr

N. Fotiou
Mobile Multimedia Laboratory
Department of Informatics
AUEB, Greece;
ExcID P.C.
Athens, Greece
fotiou@excid.io

Y. Thomas
Mobile Multimedia Laboratory
Department of Informatics
AUEB, Greece
thomasi@aueb.gr

G.C. Polyzos
Mobile Multimedia Laboratory
Department of Informatics
AUEB, Greece
School of Data Science
CUHK-Shenzhen, China
polyzos@acm.org

2024 IEEE 4th International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB) | 979-8-3503-6072-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICEIB61477.2024.10602646

***Abstract*—Many *Internet of Things* (IoT) applications are considering *multi-tenancy* to support for multiple entities sharing access to the same IoT devices. The challenge of ensuring IoT security and privacy is exacerbated in multi-tenant environments accommodating "guest" users, i.e., opportunistic users that the system has not encountered. Thus, there is a need for novel access control mechanisms capable of addressing the complexities introduced by the opportunistic nature of the users who create complex trust relationships within the IoT ecosystem. In this study, we proposed a solution that leverages *Verifiable Credentials (VCs)* to implement *Attribute-Based Access Control (ABAC)* for multi-tenant IoT environments and we integrate it with W3C's *Web of Things (WoT)* standards, enhancing interoperability. Through the utilization of VCs, the solution provides secure verification and efficient revocation of user attributes, enabling access control decisions based on the enclosed attributes. Additionally, the proposed system ensures privacy, since users can selectively disclose the necessary attributes to gain access to resources through the utilization of *Zero Knowledge Proofs* (ZKPs). Finally, the solution does not require users to have any "pre-existing" trust relationships with the protected system.**

Keywords—ABAC, ZKPs, VCs, DIDs, Multi-tenancy, IoT

I. Introduction

The proliferation of the *Internet of Things (IoT)* applications has enabled a variety of different devices, ranging from household appliances to industrial machinery, to be integrated into interconnected networks. There are many different, and often competing IoT protocols and standards, and diverse manufacturers of IoT devices. Thus, ensuring interoperability is crucial. To address the aforementioned problem, the *Web of Things (WoT)* is used for the integration and communication between heterogeneous IoT devices by providing a standardized interface and protocol translation, enabling efficient data exchange and interoperability across the IoT ecosystem. According to the WoT W3C working group [1], WoT builds on well-known Web protocols and enables IoT device discovery and access using REST-based APIs, over popular application layer protocols, such as HTTP(s).

In the context of IoT, multi-tenancy refers to an architectural approach where a single IoT platform or system serves multiple users or entities. This presents a significant challenge in terms of ensuring security and privacy, particularly when accommodating guest users, meaning individuals, businesses, or organizations with whom the system has no prior interaction.

This is because each tenant's or guest user's data must be isolated from, and invisible to, the other users sharing access to the IoT resources, ensuring data security and privacy for everyone. Thus, in multi-tenant IoT environments, the need for robust access control mechanisms becomes paramount. Traditional approaches and legacy systems often struggle to address the dynamic and opportunistic nature of guest users, who may lack pre-existing trust relationships within the IoT ecosystem. Moreover, to ensure the privacy of such users, while maintaining efficient access control, another layer of complexity is introduced [2].

In response to the aforementioned challenges, we extended the previous results [3] to a novel solution that leverages *Verifiable Credentials (VCs)* to implement *Attribute-Based Access Control (ABAC)* in multi-tenant IoT environments with support for opportunistic users. The developed system in this study comprises a central WoT gateway responsible for access control, IoT devices, and their corresponding IoT gateways that protect the devices from direct user interaction. *Decentralized Identifiers (DIDs)* are utilized for the authentication of guest users within the system, while user attributes are encoded as VCs, and we employed *Zero Knowledge Proofs* (ZKPs) and Boneh-Boyen-Shacham (BBS+) to selectively disclose the necessary attributes for each device, while maintaining others as secret. By utilizing VCs, the solution offers secure verification and efficient revocation of user attributes, enabling the implementation of access control policies directly based on these attributes. The proposed system's architecture offers the following contributions.

- Support multi-tenancy in IoT environments by facilitating guest user interactions with IoT gateways

through a WoT gateway, serving as a relay for multi-tenant IoT environments.

- Utilize VCs to provide an interoperable way to perform ABAC.
- Access rights for opportunistic users can be easily modified without requiring any changes to the WoT gateway or the device-specific IoT gateway, thus enhancing scalability and adaptability.
- Ensure the privacy of sensitive user information by leveraging ZKPs to enable only necessary attributes to be revealed to each IoT device.

The remainder of the paper is organized as follows. In Section II, we present background information about the technologies utilized in the system. Section III provides a summary of the related work in the area. Section IV introduces the design of the access control mechanism, while in Section V, we discuss the properties and the challenges of our proposed system. Finally, Section VI concludes the article.

II. Background

A. Decentralized Identifiers and DID Authentication

A DID is a new type of identifier that is used to uniquely identify a subject in a decentralized system, such as a distributed ledger or blockchain [4]. When a user creates a DID, they have to utilize a public-private key pair. Users can possess and manage multiple DIDs and prove ownership of them by associating them with a public key on the ledger and governing access to them through the corresponding private key. DIDs can be resolved to DID documents. The content of a DID document is cryptographically authenticated, providing a high degree of certainty regarding its authenticity. Through the use of a DID document, individuals can determine how much information is made public, when, and to whom information is shared, as well as the preferred methods of communication. The DID document serves as an expression of these preferences, allowing for greater control and privacy in online interactions.

DID documents can be used for authentication (DID Auth) which entails the demonstration of control over the DID by the user that owns it [5]. A simple scenario of the DID Auth interaction involves the challenge-response process, where a relying party verifies the DID of an identity owner. Following the challenge, the identity owner creates a response to demonstrate control over their DID, typically using a cryptographic signature or other forms of proof mechanisms. The relying party then validates the response by resolving the identity owner's DID and verifying its validity against the prior challenge, such as verifying the response signature with the public key object specified in the DID document.

B. VC

VCs are a digital version of physical credentials, such as identity documents, passports, diplomas, and driver's licenses that utilize asymmetric cryptography to enable the verification of a set of claims regarding the credential subject [6]. Conventional credentials, which are issued by governments or organizations, suffer from several issues such as susceptibility to forgery and counterfeiting, loss or damage, high cost of issuance, and poor scalability in various situations. Additionally, they frequently mandate the disclosure of excessive personal information beyond what is essential for the specific use case. For these reasons, they are not suitable for the digital world. On the other hand, VCs address the aforementioned problems.

C. BBS+ Signatures

BBS+ signatures [7] rely on the Strong Diffie Hellman assumption with pairing-based elliptic curve cryptography and are typically utilized in privacy-preserving protocols. This signature scheme offers strong privacy guarantees such as unforgeability and unlinkability and requires much shorter keys and signatures to achieve the same level of security compared to the Camenisch and Lysyanskaya (CL) signatures [8], which are also utilized in the context of privacy-preserving credential ecosystems. Blind signatures and ZKPs can be constructed from BBS+, providing the necessary components for enhancing privacy in VC ecosystems. More specifically, when utilizing blind signatures, the issuer signs a list of messages, without learning the actual values, but only their commitments. In this way, the real messages remain confidential even from the signer resulting in privacy enhancement. Moreover, ZKPs [9] allow one entity to demonstrate knowledge of a specific piece of information to another party without revealing the actual information. In order for a holder to present a credential in a privacy-preserving manner, ZKPs are utilized to prove knowledge of the issuer's signature without revealing the actual values that were signed.

D. ABAC

ABAC is an access control model utilized to grant access to resources or services within systems, by leveraging attributes associated with the requesting entities [10]. In contrast to other access control models that rely solely on the users' identities or predefined roles, ABAC evaluates a set of rules against their attributes, as well as contextual factors, thus allowing enhanced precision and flexibility in access control decisions. ABAC comprises the following four key components as other access control models: the Policy Decision Point (PDP), the Policy Enforcement Point (PEP) [11], the Policy Administration Point (PAP), and the Policy Information Point (PIP). The PEP is responsible for inspecting the access request and generating an authorization request, which is sent to the PDP. The PDP evaluates access requests against defined policies, which are made available through the PAP. Access control decisions are made based on the attributes of the requester, the resource being accessed, and the environmental conditions. The PDP may utilize the PIP to retrieve missing metadata, as it provides access to external sources of attributes, such as databases.

E. WoT

WoT [12] organises established Web protocols and tools to simplify the connection of IoT devices to the Web. In the communication structure of the WoT architecture, IoT devices can be reached via REST-based APIs, allowing users to engage with device functionalities, initiate actions, and receive notifications for device-generated events. To improve

interoperability across IoT platforms, the WoT model employs a standardized format called *Thing Description (TD)* [13], which is readable by machines and contains metadata about the IoT device. TD includes its identification, title, and security specifications, as well as the device's properties, actions, and events that can be accessed or triggered through Web links and forms.

III. Related Work

Several solutions have been proposed to enable efficient and secure access control in IoT environments, most of which propose *Capability-based Access Control* (CapBAC) or ABAC to represent users' access rights. *Distributed Ledger Technologies* (DLTs) and VCs are important in security and transparency. Moreover, multi-tenancy has also been discussed in the context of IoT and the proposed schemes address the challenges regarding security and scalability that opportunistic users may introduce. ABAC has also been proposed as an access control mechanism for IoT environments to model device characteristics as attributes, which are utilized to perform access control decisions. ABAC is used to implement a framework in the SmartThings IoT platform, in an attempt to tackle issues that may occur in real-world constrained IoT environments [14]. Zhang et al. [15] proposed an ABAC method, in which an access tree is constructed to make authorization decisions. In this system, DLTs are utilized to record final access control information using the authorization results.

In [16], the authors proposed an IoT access control mechanism called fabric-IoT based on the Hyperledger Fabric blockchain and ABAC. By leveraging DLTs and ABAC, fabric-IoT provides a decentralized and dynamic access control solution applied in constrained IoT devices. Nonetheless, the aforementioned approaches cannot be used in multi-tenant IoT environments, where guest users must be handled in a privacy-preserving manner and therefore enhanced security practices are required. Furthermore, other solutions that leverage DLTs have been proposed to enable access control in IoT environments. In particular, a CapBAC model is proposed by DLTs and DIDs to achieve both identity management and access control. Their protocol leverages smart contracts and the overall system's security is based on the system's interactions and the transparency that smart contracts offer [17]. Similarly, in [18], an IoT access control and authentication mechanism for IoT devices with smart contracts for managing access rights is designed and implemented. Blockchain technology is used to record the distribution of attributes to avoid single-point failure [19]. The proposed scheme uses ABAC and offers a lightweight and scalable solution for constrained devices. However, there is a need for a privacy-preserving solution to handle opportunistic users without compromising the system's security.

A combination of VCs and OAuth 2.0 has also been proposed along with CapBAC to model access control policies in a privacy-preserving manner. As described in [20] and [21], a CapBAC technique based on VCs and OAuth 2.0 is utilized to handle VC attributes as capabilities related to access control policies. The main objective is to enable sharing of Web resources, by integrating VCs into the OAuth 2.0 authorization flow, while the latter includes an efficient and privacy-preserving proof of possession mechanism and supports revocation. The aforementioned tools enhance the system's security and preserve privacy regarding access rights. Therefore by utilizing ZKPs in the proposed solution, we aim to build such schemes and create privacy-preserving protocols suitable for IoT multi-tenant environments.

Another solution for access control in IoT environments, proposed by Pittaras *et al.* [22], leverages DLTs such as Ethereum blockchain and smart contracts. In this solution, a smart contract acts as the PDP, while other smart contracts are responsible for creating and managing *Access Control Tokens* (ACT), enabling fine-grained access control management for various entities, including municipal governments, citizens, and police departments. Through predefined mappings and token ownership verification, the system ensures secure and efficient access management for IoT devices and services. This architecture provides increased transparency, automation, and decentralization, addressing key security and privacy concerns in IoT ecosystems.

Although the solutions offer effective approaches to access control presented [20−22], we employed a WoT gateway, which not only facilitates interoperability but also serves as a centralized access control point, streamlining access management for multiple tenants sharing IoT resources. Similarly, VCs enable a more flexible and tailored approach to access permissions, accommodating the different needs of guest users. Furthermore, ZKPs ensure privacy, thereby encouraging guest users to engage with the system. confidently.

Finally, there have been solutions to address multi-tenancy in IoT environments. Most of the proposed architectures are generic and do not refer explicitly to access control, such as [23], in which the authors propose an architecture that provides multi-tenant capability of IoT decentralization and the sharing of objects between users. A notable reference regarding access control in IoT multi-tenant environments is [24], in which the authors implement an IoT-based solution that utilizes OAuth 2.0, while also allowing the complete delegation of authorization. The multiple tenancy property is also enabled by application-scoped authorization policies. The aforementioned solution is open-source and has been extensively validated in the scope of FIWARE. The main objective of this study was to design an access control model suitable for multi-tenant IoT environments and not an application-specific access control mechanism as a service.

IV. System Design

The proposed system architecture is illustrated in Fig. 1, as a typical use-case scenario. Specifically, the system comprises a WoT gateway serving as the central access control point, IoT devices, and the corresponding IoT gateways that protect the devices from direct user interaction. In the system's architecture, the WoT gateway plays the role of the PEP and the PDP. User attributes are encoded as VCs, and we employ ZKPs using BBS+. With the aforementioned design, the proposed system has the following characteristics:

- Guest users interact with the IoT gateways through a WoT gateway, which serves as a relay for multi-tenant IoT environments.
- VC attributes are modeled as access rights, enabling an efficient and secure way to perform ABAC.
- Access rights of guest users, which are transparent to gateways, can be altered, while gateways do not have to be modified.
- By leveraging ZKPs, the necessary attributes that correspond to each IoT device are disclosed, thus enhancing the system's security and preserving the users' privacy.

From a high-level perspective, the system works as follows. Upon a guest user's initial request, the system generates a public-private key pair, to create the DID for authentication. The owner is tasked with assigning access rights encoded as VC attributes and subsequently signing the relevant credentials. When a user initially enters the system and wants to request access to a resource, the system securely transmits her DID to the owner, through the WoT gateway. The DID is then registered with a secure DID registry, which is trusted and accessible by owners and WoT gateways but remains inaccessible to users to ensure privacy. Each DID can be resolved to a DID document, which contains service endpoints, the public key, and the authentication methods. The authentication phase follows the DID Auth process, during which the user receives a DID Auth challenge—a random cryptographic challenge—to prove ownership of her DID. The system responds to the challenge using her private key, for instance by encrypting a message, and then uses the owner's public key to encrypt it again, thus creating the DID Auth response. Once received by the owner, the system accesses the DID registry, decrypts the response using his private key, and then decrypts it again using the user's public key. If the process is successful, the authorization phase concludes, allowing the user to proceed with her request to access a specific IoT resource, including her attributes.

This initiates a new phase in the proposed protocol, where the PEP inspects the user's request and generates an authorization request for the PDP. The DID is included in the VC as a unique identifier. Subsequently, the user utilizes ZKP from BBS+ to selectively disclose the appropriate attributes for the WoT gateway that performs access control decisions for accessing the IoT devices. The PDP evaluates the user's request against the policy and determines whether access should be granted. This decision is then relayed back to the PEP, which can subsequently either allow or deny access to the requester.

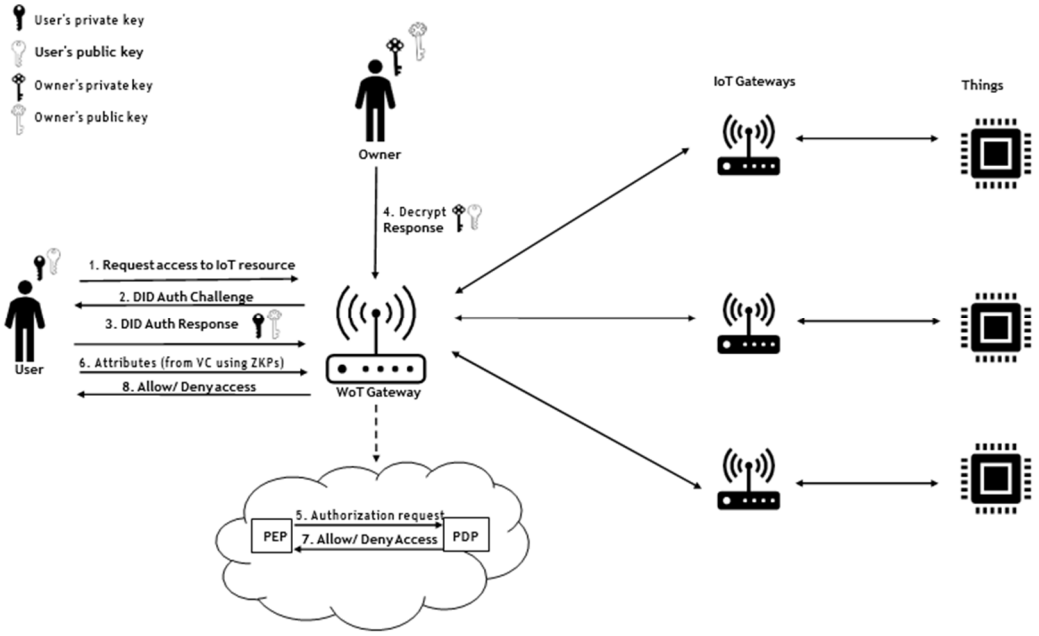

Fig. 1. Overview of system architecture

A. Use Case

Suppose a smart home scenario with multiple IoT devices with different capabilities that require a common management approach. In this case, we assume that there exists one owner and guest users that require access to the IoT devices in the smart home. These devices, ranging from sensors to surveillance cameras, have different capabilities and access control policies. For instance, a guest user may wish to access an IoT device, such as a temperature sensor, to regulate environmental conditions within the home. In this example, the user does not have previous relationships with the system and thus cannot be considered trusted. For this purpose, authentication is required along with the appropriate access control policies.

V. Discussion

Resource-constrained IoT devices are vulnerable to various security threats targeting their limited processing capabilities and susceptible to unauthorized access, thus

robust access control measures are required. The utilization of WoT gateways as relays for user interactions with the IoT gateways offers an additional layer of security to the proposed system. This approach enhances the system's resilience against malicious intrusions by providing a controlled entry point for user requests. Additionally, WoT gateways implement robust access control measures by serving as centralized hubs for enforcing authentication and authorization policies. Through this centralized approach, access rights can be carefully managed and dynamically adjusted based on user attributes stored within the VCs, which is important for multi-tenant systems, where guest users have not previously established trust relationships with the system. VCs also enable a standard and interoperable way to handle users' attributes and thus can easily be integrated into ABAC protocols.

The proposed solution is resilient against various types of attacks. By binding VCs to a user's DID, the system is not affected by attacks that involve the interception of communication between a client application and a device. Any attacker, who obtains a user's authentication account information can solely utilize it to request new VCs, without affecting the previously issued VCs. Additionally, the implementation of access control policies is decoupled from the IoT devices and their owners, since granting or revoking access rights does not require any communication with the actual devices. Moreover, the utilization of VCs enables selective disclosure through ZKPs, allowing users to present only the necessary attributes that correspond to their requests, while accessing the IoT resources. This not only mitigates privacy risks associated with multi-tenancy, but also holds significance for opportunistic users, as it enhances their trust and confidence in the IoT ecosystem. As a result, guest users are more likely to engage with the system, knowing that their privacy is protected and that they retain control over the information they reveal.

While the proposed system demonstrates strengths in terms of privacy, security, and scalability, the calculation of BBS+ signatures may introduce computational overhead. The average time required to sign and verify subitems is relatively low with values of 0.07 and 0.055 ms, which coincided with [25]. Nevertheless, further optimization and efficiency improvements may be necessary to address potential performance bottlenecks and ensure smooth operation, particularly in environments with large numbers of IoT devices and guest users.

Revocation can be implemented in the system by leveraging simple and efficient revocation lists by the W3C as described in [26]. In this approach, a simple bitstring list is used to store the status of the credentials. In each credential, a unique identifier that represents the position of the credential in the list is included. The list contains a single bit in each position, with 0 representing non-revoked credentials and 1 representing revoked credentials. When a credential needs to be revoked, the owner simply adds bit 1 in the position that is described in the credential. Nonetheless, this approach may introduce privacy concerns due to the use of unique credential identifiers, which allow gateways to correlate users to the specific credential.

One alternative is to utilize more privacy-preserving methods, such as dynamic accumulators [27], in which all non-revoked credentials are stored in an accumulator and a witness value is computed and distributed in the other entities. When a user wishes to prove that a credential has not been revoked, he needs to compute a ZKP that the credential belongs to the accumulator. These structures offer a higher level of privacy, as they do not disclose any information about the credential itself or the other members of the accumulator, however they may introduce computational overhead due to their complexity.

Another approach is to utilize *Selective Disclosure JSON Web Tokens* (SD-JWTs) [28] instead of BBS+ signatures. In the proposed solution with ZKPs using BBS+, while selective disclosure is achieved, the unlinkability is not guaranteed, since DIDs are included in the VCs. While the attributes possessed by users remain hidden during transactions, DIDs can potentially be correlated with specific users, compromising their anonymity. These tokens provide a mechanism for sharing only a subset of the claims included in a JWT, instead of releasing all claims to every verifier. When an SD-JWT is issued, it is accompanied by an *SD-JWT Salt/Value Container* (SVC), which contains a mapping between the raw claim values in the SD-JWT and corresponding salts. This mapping facilitates the selective disclosure of specific claim values to verifiers. The issuance process involves an issuer, who creates the SD-JWT and SVC, and a holder, who receives the tokens. Once issued, the holder can present an *SD-JWT Release* (SD-JWT-R) to verifiers. An SD-JWT-R contains a subset of the claim values from the original SD-JWT in a verifiable format. Verifiers, upon receiving the SD-JWT-R, use the salts provided in the SVC to compute hash digests of the claim values and compare them with the corresponding values in the SD-JWT, thus verifying the authenticity of the claims disclosed. Verifiers only salt for the values that the holder wishes to disclose, and they must validate the JWT, including the signature of the issuer, to ensure its authenticity.

VI. Conclusions and Future Work

We proposed a system that addresses the complexities and challenges of ensuring security, privacy, and efficient access control in multi-tenant IoT environments. Specifically, we leveraged VCs and ZKPs to develop a robust ABAC mechanism that enables the secure verification and revocation of user attributes, modeled as access rights in a multi-tenant IoT system. This approach enhances the scalability of IoT ecosystems that require dynamic access control policies and support for guest users who have not previously established a trust relationship with the system. To enhance the system's security, we also utilize a WoT gateway as a controlled entry point for user requests and enforce authentication and authorization policies. It is still necessary to integrate a VC wallet to further empower users to securely store and manage their VCs within the multi-tenant IoT ecosystem. This offers users enhanced control and flexibility over their attribute data. Additionally, the potential of SD-JWTs needs to be considered in the solution to achieve selective disclosure, since ensuring unlinkability in the proposed system remains a challenge. While the attributes possessed by users remain

hidden during transactions, DIDs can potentially be correlated with specific users, compromising their anonymity. Therefore, integrating SD-JWTs offers a complementary approach to address this limitation and enhance user privacy within our multi-tenant IoT environment.

REFERENCES

[1] World Wide Web Consortium (W3C), "W3C web of things," https://www.w3.org/WoT/, accessed: April 2, 2024.

[2] C. D. Nassar Kyriakidou, A. M. Papathanasiou, and G. C. Polyzos, "Decentralized identity with applications to security and privacy for the internet of things," *Computer Networks and Communications*, pp. 244– 271, 2023.

[3] N. Fotiou, I. Pittaras, V. A. Siris, and G. C. Polyzos, "Enabling opportunistic users in multi-tenant iot systems using decentralized identifiers and permissioned blockchains," in *Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things*, 2019, pp. 22–23.

[4] World Wide Web Consortium (W3C), "Decentralized Identifiers (DIDs) v1.0," World Wide Web Consortium (W3C), Tech. Rep., July 2022. [Online]. Available: https://www.w3.org/TR/did-core/

[5] M. Sabadello, K. Den Hartog, C. Lundkvist, C. Franz, A. Elias, A. Hughes, J. Jordan, and D. Zagidulin, "Introduction to did auth," in *Rebooting the Web of Trust VI*, July 2018.

[6] M. Sporny, D. Longley, and D. Chadwick, "Verifiable credentials data model 1.0," *W3C Candidate Recommendation, March*, 2019. [Online]. Available: https://www.w3.org/TR/vc-data-model/

[7] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Annual international cryptology conference*. Springer, 2004, pp. 41–55.

[8] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in *Security in Communication Networks: Third International Conference, SCN 2002 Amalfi, Italy, September 11–13, 2002 Revised Papers 3*. Springer, 2003, pp. 268–289.

[9] U. Fiege, A. Fiat, and A. Shamir, "Zero knowledge proofs of identity," in *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, 1987, pp. 210–217.

[10] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, 2015.

[11] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone *et al.*, "Guide to attribute based access control (abac) definition and considerations (draft)," *NIST special publication*, vol. 800, no. 162, pp. 1–54, 2013.

[12] M. Kovatsch, R. Matsukura, M. Lagally *et al.*, "Web of things architecture," https://www.w3.org/TR/wot-architecture/, 2017, accessed: March 29, 2024.

[13] S. Kaebisch, T. Kamiya, M. McCool *et al.*, "Web of things thing description," https://www.w3.org/TR/wot-thing-description/, 2017, accessed: March 29, 2024.

[14] G. Goyal, P. Liu, and S. Sural, "Securing smart home iot systems with attribute-based access control," in *Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*, 2022, pp. 37–46.

[15] Y. Zhang, B. Li, B. Liu, J. Wu, Y. Wang, and X. Yang, "An attribute-based collaborative access control scheme using blockchain for iot devices," *Electronics*, vol. 9, no. 2, p. 285, 2020.

[16] H. Liu, D. Han, and D. Li, "Fabric-iot: A blockchain-based access control system in iot," *IEEE Access*, vol. 8, pp. 18 207–18 218, 2020.

[17] Y. Liu, Q. Lu, S. Chen, Q. Qu, H. O'Connor, K.-K. R. Choo, and H. Zhang, "Capability-based iot access control using blockchain," *Digital Communications and Networks*, vol. 7, no. 4, pp. 463–469, 2021.

[18] A. Z. Ourad, B. Belgacem, and K. Salah, "Using blockchain for iot access control and authentication management," in *Internet of Things–ICIOT 2018: Third International Conference, Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA, June 25- 30, 2018, Proceedings 3*. Springer, 2018, pp. 150–164.

[19] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for iot," *IEEE Access*, vol. 7, pp. 38 431–38 441, 2019.

[20] N. Fotiou, V. A. Siris, and G. C. Polyzos, "Capability-based access con- trol for multi-tenant systems using oauth 2.0 and verifiable credentials," in *2021 International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2021, pp. 1–9.

[21] N. Fotiou, V. A. Siris, G. C. Polyzos, Y. Kortesniemi, and D. Lagutin, "Capabilities-based access control for iot devices using verifiable credentials," in *2022 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2022, pp. 222–228.

[22] I. Pittaras and G. C. Polyzos, "Multi-tenant, decentralized access control for the internet of things," in *2023 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)*. IEEE, 2023, pp. 28–34.

[23] S. Cherrier, Z. Movahedi, and Y. M. Ghamri-Doudane, "Multi-tenancy in decentralised iot," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. IEEE, 2015, pp. 256–261.

[24] A´ . Alonso, F. Ferna´ndez, L. Marco, and J. Salvachu´a, "Iaacaas: Iot application-scoped access control as a service," *Future Internet*, vol. 9, no. 4, p. 64, 2017.

[25] N. Fotiou, I. Pittaras, S. Chadoulos, V. A. Siris, G. C. Polyzos, N. Ipiotis, and S. Keranidis, "Authentication, authorization, and selective disclosure for iot data sharing using verifiable credentials and zero-knowledge proofs," in *Emerging Technologies for Authorization and Authentication*, A. Saracino and P. Mori, Eds. Cham: Springer Nature Switzerland, 2023, pp. 88–101.

[26] M. Sporny and D. Longley, "Revocation list 2020: a privacy-preserving mechanism for revoking verifiable credentials," Available from: https://w3c-ccg.github.io/vc-status-rl-2020/, 2021, accessed: 2023-09-15.

[27] J. Camenisch and A. Lysyanskaya, "Dynamic accumulators and application to efficient revocation of anonymous credentials," in *Annual International Cryptology Conference*. Springer, 2002, pp. 61–76.

[28] D. Fett and J. Bradley, "Oauth 2.0 authorization with selective disclosure: Jwt secured authorization request (jar)," https://www.ietf.org/archive/id/draft-fett-oauth-selective-disclosure-jwt-02.html, 2020.