A Survey on Secure Network Device Identity

Qilin Chen c.qilin@wustl.edu (A paper written under the guidance of Prof. Raj Jain) Download 

Abstract:

The success in miniaturization of digital components, such as chips, sensors, and circuits, has promoted the proliferation of Internet of Things (IoT) devices, which are smaller devices with sensors connected to the Internet. The surge in machine-to-machine (M2M) traffic not only created the need for the design of new protocols but also urged the development of new security infrastructure and protection mechanisms to better serve constrained devices. Many researchers have covered correlated topics in the field. However, given the broad landscape and the abundant topics involved, a comprehensive survey paper is sparse. Thus, we aim to conduct a comprehensive survey from different perspectives, focusing on both the coverage and depth. We will introduce the background knowledge in IoT and secure device identity, and how they can be addressed or resolved from 3 vantage points, public key infrastructure (PKI), device identity techniques, and identity and access management (IAM).

Table of Contents:

---

1 Introduction

This section will first introduce IoT layer architecture and the technologies involved in section 1.1. We then analyze the existing protocols, aiming to identify potential security challenges in section 1.2, leading to the emergence of secure network device identity. Section 1.3 will cover some important concepts in the area, attempting to provide basic knowledge for the discussion in the following paper.

1.1 IoT layer architecture and protocols

Based on the complexity, IoT systems can be split into 3 to 7-layer architectures, which still lack standardization today. In practice, most of the models can be represented in a 4-layer architecture, which will be divided as follows: Sensing/perception layer, Network/transport layer, Data processing layer, and application layer (figure 1).

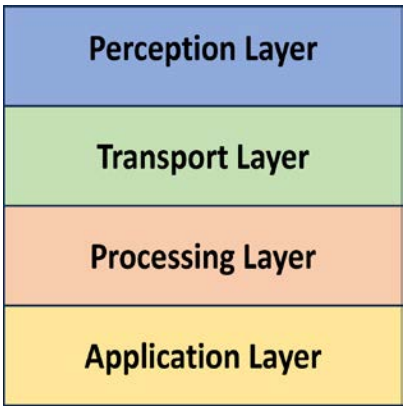

Figure1 IoT 4-layered Architecture

The first layer, the sensing/perception layer is also known as the physical layer, where the sensors and devices are located. It is responsible for data collection. The second layer is the network/transport/communication layer, in charge of end-to-end communication between devices. The main components are data transmission protocols, such as routing, WiFi, Bluetooth, 6LowPAN, MQTT, etc. The third layer is the data processing layer, where data will be stored and analyzed to generate useful insights and predictions. Various data storage and data abstraction techniques can work here. Modern data analysis is also commonly aided by machine learning. At last, it comes the application layer. It is responsible for providing graphical user interfaces (GUI) for users to control and interact with IoT devices and showing the insights generated through the

analysis in a human-readable way. Technologies involved include machine learning algorithms, visual analytics, and human-computer interactions.

1.2 Layer-wise challenges and overall security challenges

[Malik2019] proposed that key bootstrapping was not fully addressed in IoT since it is a cross-layered process. For instance, IEEE 802.15.4 was widely used in the perception layer. However, this protocol only provides hop-to-hop security rather than end-to-end security. In the transport layer, 6LoWPAN does not have a security counterpart whereas Routing Protocol for Low-Power and Lossy Networks (RPL). Public key infrastructure (PKI) has been one popular solution for safe key bootstrapping, however, using the current features of PKI is still not the perfect solution, which will be further discussed in Section 2. The reason is that asymmetric cryptography has high computation and energy requirements, controverting to the limited resources IoT devices possess.

Considering the whole IoT ecosystem, challenges can be classified into 4 categories, constrained devices, device identification, security, and interoperability [Ayoub2023]. They are correlated with each other and can be the different consequences caused by some shared reasons. One of the main reasons shared by the three categories is the lack of standardization in the area [HaddadPajouh2021]. Specifically, we can see the chaos in the identification of devices as numerous manufacturers exist in the market, all utilizing different identifiers. Popular ones include IP address, Digital Object Identifier (DOI), Electronic Product Code and Object Identifier. Besides, the interoperability problem was also attributed to the over-abundant standards problem by [RFC8477], making it hard to efficiently communicate and enforce a universal security protection practice.

1.3 Secure Network Device Identity

Secure network device identity is a broad topic, involving hardware, software, and management concepts, aiming to design and implement a secure network system. Here, to address the aforementioned challenges in IoT, we narrowed our scope into three main aspects, the implementation of public key infrastructure, the identification techniques of IoT devices, and the identity and access management in IoT.

---

2 Public Key Infrastructure (PKI) in IoT

This section is going to discuss the utilization of Public Key Infrastructure (PKI) in IoT and its pertaining challenges, as well as some explored mitigation approaches. A PKI is a comprehensive system including hardware, software, policies, and standards designed to enhance security and trust in digital communication and information exchanges. In short, PKI implemented the idea of asymmetric cryptography, involving generating a pair of public key and private key. The mathematical relationship between two keys is intractable in a way that deriving the private key from the public key is computationally infeasible. Public keys are disseminated widely for the encryption of the data and verification of digital signatures, which are certified by some trusted certificate authorities (CA). Whereas the private keys are kept secret on the client side, and used

for decryption and creating digital signatures. The most commonly used format of PKI is defined in the X.509 standard, thus the technology is also referred to as PKI X.509 (PKIX) [X.509]. Three major merits brought by PKI are the confidentiality, integrity, and authenticity of information. However, this requires users to place trust in CAs, which can also be compromised, and trigger security problems.

The section is organized as follows: section 2.1 surveys the landscape of PKI implementation in IoT, and the current limitations entailed by the traditional architecture of PKI. The following potential mitigation approaches are discussed in section 2.2 to section 2.6. Specifically, section 2.2 attempts to conduct a comparison of different implementations of PKI to identify the best practices. Section 2.3 introduces the concept of Domain Name System (DNS) and sheds light on how the combination of DNS-based Authentication of Named Entities (DANE) and DNS Security Extension (DNSSEC) can be deployed as a complementary for PKI in IoT. To have a better knowledge of this topic, a comprehensive evaluation of different DNS-related technologies is carried out at the end of this part, opening up a wider horizon for future research. It also illustrates the impact on DNS infrastructure, in turn, from the deployment of IoT. Section 3.4 offers another standpoint to address security problems by taking advantage of the decentralized nature of blockchain technology.

2.1 PKI Implementation in IoT and Related Challenges

[Diaz-Sanchez2019] proposed that one of the commonly used standards to provide end-to-end security in IoT traffic management is Transport Layer Security (TLS), which is highly dependent on PKI. As mentioned in the starting part of Section 2, CAs in traditional PKI each have a list, including trusted domains, that need to sign, manage, revoke, and verify digital certificates to ensure security. While assumptions have been made that CAs should benignly finish these tasks, nevertheless, this is not always the case. Therefore, any security breaches in these trusted parties can exert wide effects. Several drawbacks and challenges of using PKI in this scenario are highlighted as follows.

Firstly, users have to trust manufacturers-generated certificates while the certifying process is costly and time-consuming [Singla2018]. The trust in CAs is also concerning given their global localization all over the world. Jurisdictions and regulations in these countries can vary; thus, their discrepancies can leave space for attacks. The situation is only worse by knowing that non-commercial groups, including governments, and special interest groups, control over 74% of trusted certificates [Diaz-Sanchez2019].

Secondly, not willing to be restricted to a single CA, the attempt to create a single root structure for interoperability failed. Additionally, aiming to intercept and accelerate SSL/TLS traffic on behalf of the customers, network operators allow companies to introduce intermediate CAs, originating from a trusted CA. This will create a large tree-like hierarchy where certificates can be verified to different independent roots but not a unified one, which makes it hard to maintain an up-to-date hierarchical trusted CA list in the root [Diaz-Sanchez2019], [Balakrichenan2022].

Thirdly, another great security concern arises from the fact that PKI certificates can be issued to any domain without the domain owner's consent, given that the voucher entity and the owner of the service do not have a bidirectional and verifiable relationship [Diaz-Sanchez2019].

Fourthly, "clicking through" security, is an easy breach of the good security practice approach that the browser allows users to interact with unauthenticated entities when the verification of certificates fails.

All these challenges in the current implementation of PKI in IoT suggest that traditional PKI itself is not enough to fulfill baseline security requirements. Alternative certification methods and attack detection mechanisms are needed to support sufficient protection. Several mitigation methods will be discussed in the sections afterward.

2.2 Different key bootstrapping protocols of PKI in IoT

In the scope of IoT, key bootstrapping, consisting of key generation and key exchange, is the prior process before any operation to establish association and trust between devices. Being a cross-layered security challenge and given that protocols in normal IoT layers only provide enhancement to certain aspects of communications or security, PKI is used as the solution pervasively. However, traditional PKI is by nature energy and computation-inefficient and is not fully compatible with constrained devices, for instance, IoT devices. [Malik2019] presented a holistic evaluation of several different key bootstrapping methods with different authentication schemes, involving raw public key, certificate-based key (traditional PKI), identity-based key, self-certificated key, and certificateless key. The pros and cons of each will be discussed below.

In terms of traditional PKI, namely the certificate-based key bootstrapping, the implicit certificate is favorable over the explicit certificate since it can provide smaller footprints, and the absence of an explicit certificate saves storage, making it faster for IoT devices to process. One of the most commonly used methods of this type is the Elliptic Curve Qu-Vanstone (ECQV).

In identity-based authentication, users' identities (e.g. phone numbers, email addresses) are used to replace digital certificates for verification purposes. It simplifies key generation and management processes, and effectively reduces the running overheads, making it more scalable in the IoT ecosystem.

Another improvement that can be made to traditional certificate-based authentication is through self-certification. Self-certification is done by excluding the separate certificate and only having implicit certificates on the keys. This is beneficial as the storage and computation burdens are lighted on the constrained devices. Moreover, this scheme transcends the previous method, ID-based authentication, as users can also have an anonymous private key to the authority. However, in turn, the weakness of using this scheme is the repudiability of the private keys.

Regarding certificate-less authentication, despite the strengths mentioned for previous methods, privacy is further enhanced as this certificate-less authentication does not require linking device identifiers to certificates. On the other hand, the absence of certificates and reduction in identifiers also leads to degradation in security, that is, hard to verify the authenticity of devices.

2.3 DNS Infrastructure in PKI

To discuss how Domain Name System (DNS) infrastructure can function in PKI, basic knowledge of DNS is needed and will be covered in this section. In short, a Domain Name System is a system that translates human-readable domain names. Domain Name System Security Extensions (DNSSEC) is a set of extensions to DNS that adds a layer of security, which provides data origin authentication and data integrity, verified using digital signatures. DNS-Based Authentication of Named Entities (DANE) is an extension of DNSSEC that focuses on enhancing the security of internet communication by binding digital certificates to domain names, and by allowing websites and services to publish their TLS/SSL certificates in DNS records. Generally, a normal network will create a domain name space, consisting of a tree data structure. Each node or leaf in the tree has a label and zero or more resource records (RR), which hold information associated with the domain name [DNS].

[Diaz-Sanchez2019] aimed to address some of the aforementioned TLS/PKI-related problems by utilizing different certificate pinning techniques, including CT, SK, TACK, CAA, HSTS-HPKP, and DANE. Certificate pinning is a concept that allows clients to obtain a better certainty that a certificate used by a server is not compromised. Comparison over 9 metrics showed that DANE is preferable as it requires no extra side channel and can maintain frequent certificate updates and instant key recovery. It is also superior in its convergence time plus the decentralized security for no involvement of third parties.

[Balakrichenan2022] illustrated the proximity of DNS and PKI and demonstrated its feasibility to implement PKI using DNS and its extensions. Specifically, data integrity and authentication can be guaranteed by DNSSEC whereas the hierarchy of trust list in PKI can be implemented using the DNSSEC chain of trust, against which the public key can be verified. The attack surface and security level are better augmented using DANE, by enabling dynamic certificate signing and verification against self-chosen root CA by each institution. These features demonstrated the advantages of DNS and DANE, including a single trust anchor and lightweight authentication scheme to be a feasible and robust complement to PKIX, as well as being more scalable on IoT devices.

[Ayoub2023] moved one step further by considering on a wider range of DNS-related technologies and how DNS can contribute to IoT at a wider degree not only for PKI. For instance, the security extensions of DNS, that is, DNSSEC, can be leveraged to resolve IoT secure name resolution problems and IoT interoperability problems. Plus, DNS over CoAP can mitigate the communication security between constrained devices. The obstacles in detecting malicious activity can also be tackled using DNS traffic analysis etc. In conclusion, DNS-related solutions can be applied to various aspects of IoT and have a promising future.

In turn, the author of [Ayoub2023] also emphasized the impact of IoT on DNS infrastructure where DNS infrastructure may be more vulnerable to DDoS attack and DDoS amplification since the proliferation of the number of connected devices and the complex coding in IoT layers is prone to errors.

2.4 Blockchain-based PKI

It is discussed in the paper that PKI architecture is prone to error and failure based on its centralized design. Blockchain, originally invented by Satoshi Nakamoto for cryptocurrency, can be leveraged as a potential solution considering its decentralized nature. Blockchain functions as a linked list of blocks, where each block contains a hash of the previous block, a timestamp, and transaction data. The blocks are append-only and cannot be modified once added. It is peer-to-peer and enables independent verification of transaction authenticity to support its decentralization.

[Singla2018] delivered an evaluation on three blockchain-based PKIs, including Emercoin Name Value Storage (NVS), Ethereum and Smart Contracts, and Ethereum Light Sync mode, and demonstrated blockchain-based PKI's feasibility and their superiority over conventional CA-based PKI. Observed advantages include centralized CA, as well as separate monitoring, which is unnecessary so that there will be no single-point failure. Blockchain-based PKIs can have quick addition and removal of certificates while being resistant to DDoS attacks. Storage capabilities are also facilitated, for instance, Ethereum allows storing of more complex data structures created by smart contracts.

2.5 Summary

To sum up, section 2 discussed the implementation of PKI in IoT, exploring different key bootstrapping protocols and pertaining challenges. It also provided insights on how current infrastructure can be improved by incorporating DNS and blockchain, making PKI more scalable and accessible on constrained devices. On the other hand, PKI cannot provide enough protection to devices that are not equipped with cryptographic infrastructures. In this scenario, device identification comes in to help.

---

3 IoT Device Identification Techniques

Section 3 covers the identification techniques for IoT devices. Contents include the underlying reasons why device identification is crucial in IoT security and machine learning-based identification techniques. An overview of the landscape and comparisons of performances of various techniques will then come at last. Section 3.1 first introduces the threat models and challenges faced in IoT device identification. Section 3.2-3.4 will cover different aspects of ML-based identification techniques, whereas Section 3.5 explores the idea of abnormal detection, which is the direct extension of device identification. Section 3.6 summarizes the whole section and provides insights from comparisons.

3.1 Threat models and Challenges

[Chowdhury2023] proposed that IoT is suffering increasingly complex management issues given the proliferating numbers of devices and the heterogeneous functionalities of each device. In traditional network infrastructure, devices communicate with each other and report their identifiers

to the server to get verified. However, implementing this method in IoT can be challenging as IoT devices are designed with limited computation capabilities and storage [Aksoy2019]. The situation degrades given the heterogeneity of protocols used in devices, as well as the devices that are frequently on and off in the systems [Liu2021b], [Fan2023]. Therefore, correctly identifying IoT devices becomes a crucial part of IoT security, which also acts as the very first level of protection. One widely used approach of identity verification is cryptographic identification, examples include using digital certificates, which is mentioned above in Section 2. However, many constrained devices do not support cryptographic identification as well and cryptographic approaches are impotent to already compromised devices. This brings up the need for a supplementary approach, that is noncryptographic, that is, to utilize signal patterns or behavioral characteristics to identify and distinguish devices [Liu2021b]. All the techniques discussed in the rest of the sessions fall into this category. The comparison of techniques is listed in Figure 2, which will be explored in detail in follow-up subsections.

Device Identification Approaches	Techonology branch	Feature requirement	Model explainability	Continuou learning	Anc
Feature based device identification	Supervised learning	High	Strong (KNN)/Median (SVM)	Easy (KNN) / Median (SVM)	Low
Deep learning enabled device identification	Supervised learning	Low	Weak	Hard	High Me
Unsupervised device detection & identification	Unsupervised learning	High	Strong	N/A	

Figure2 Comparison of device identification techniques

Challenges in device identification originate from two major areas [Fan2023], namely, identification accuracy and high overhead generated by labeled data. Identification accuracy may fluctuate due to many factors, which require comprehensive consideration of various aspects. Meanwhile, the overhead of the algorithm is hard to cope with as the accuracy and overhead are commonly viewed as a trade-off. That is, to achieve a better performance in ML algorithms needs a larger amount of data and therefore entails more overhead.

3.2 Feature-based identification

Features under this scenario can be defined as raw signals in data transmission and hardware imperfections. Commonly used features include persistent patterns, transient patterns, channel status features, cross-domain features, and hybrid approaches. While these features are by nature unique for the device they are hard to forge, which can be highly accurate identifiers. They are also fragile and prone to interferences as they are intercepted from the physical world, for example, human movements or device location changes [Liu2021b]. Practically, the hybrid approaches that use the combination of previous feature sets outperform others. This can be attributed to the implementation of an automatic feature selection algorithm, promoting the hybrid approaches to have the optimal feature sets.

3.3 DL-based identification

DL-based identification methods received great interest and are widely deployed. It is known for its estimated high accuracy but requires a large amount of data to converge. Recent research showed its progress in the reduction of manual feature engineering and robustness to complex environments. [Aksoy2019] is the first to integrate automation into the IoT device identification process, whereas previous studies were human resources demanding, which requires much feature engineering. A GA algorithm was leveraged to perform automatic feature selections, which thus empowered the model to automatically perform data reprocessing and feature re-extraction without expert supervision once the test beds were changed. Later, [Liu2022a] greatly reduced the number of features by proposing an IoT device identification method combined using the directions and lengths of packets in a sequence as the feature. It achieved over 99% accuracy, recall, precision, and f1 score yet still suffers from latency in processing data since the feature sequences consist of 500 consecutive packets. [Chowdhury2023] addressed the latency problems by conducting a supervised ML approach that required only 4 features from 5 consecutive packets. While a new function to classify IoT and non-IoT devices is also added to the model in [Chowdhury2023], it sacrifices accuracy compared to the model in [Liu2022a].

Some frequently discussed open issues in DL-based techniques that may or may not be covered in these papers are hyperparameter settings and neural network architecture settings. Both greatly impact the performances of the model, but no perfect solution has been seen so far and thus can be future directions.

3.4 Unsupervised learning-based identification

Unsupervised learning-based identification is called into usage when the exact information of devices is not directly available. The underlying idea of it is to map device signals and activities into latent space to discover clusters or probability distributions. It is categorized into two types based on its focus, including device behavioral modeling and signal propagation pattern modeling. [Fan2023] is an example of the formal one, as it inspiringly developed a heterogenous graph representation learning algorithm incorporating with attention mechanism with macro F1 13.58% and 12.77% higher than other approaches on average.

3.5 Summary

In summary, this section first presented the threat models and challenges in device identification. It then provided a comprehensive overview of existing identification techniques, details of comparison from different characteristics are covered in Figure 2.

---

4 Identity and Access Management (IAM)

As the number of users and devices continues to grow rapidly, it is crucial for manufacturers that not only implement separate identification or authentication approaches but also have IAM

solutions. IAM stands for identity access and management, which acts as a self-sufficient system contributing to user/device authentication, access control, identity management, etc, offering great convenience and efficiency for both the users and network management. This section will discuss the usage of IAM in the IoT area, starting by first introducing important terminologies and concepts of IAM in section 4.1. Section 4.2 will then explore challenges faced by the current implementation of IAM in IoT, followed by the discussion of how blockchain-based IAM can mitigate the situation in section 4.3. The whole section will be summarized in section 4.4.

4.1 IAM structure and concepts

IAM consists of three parts: identity management (IdM), access control (AAC), and monitoring & logging. IdM is an administrative process to create and maintain user accounts to be used for authentication and identification in online services, comprising registration, identification, authentication, issuance, and verification. The four subsections included in identity management are registration/identification, authentication, data management, and verifiable claims. In terms of modern authentication methods, there are four popular categories, knowledge-based, possession-based, inherence-based, and multi-factor authentication [Ghaffari2022].

Regrading access control, it is a security technique that regulates who or what can do which action (e.g., use, read, write, execute, view) on specific resources in a computing environment [Ghaffari2022]. Discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), and attribute-based access control (ABAC) are four commonly implemented methods with different focus of control levels. One note to be aware of is that most of the existing AAC solutions are centralized and suffer from single point of failure and low scalability. The details of the structure can be seen in Figure 3.

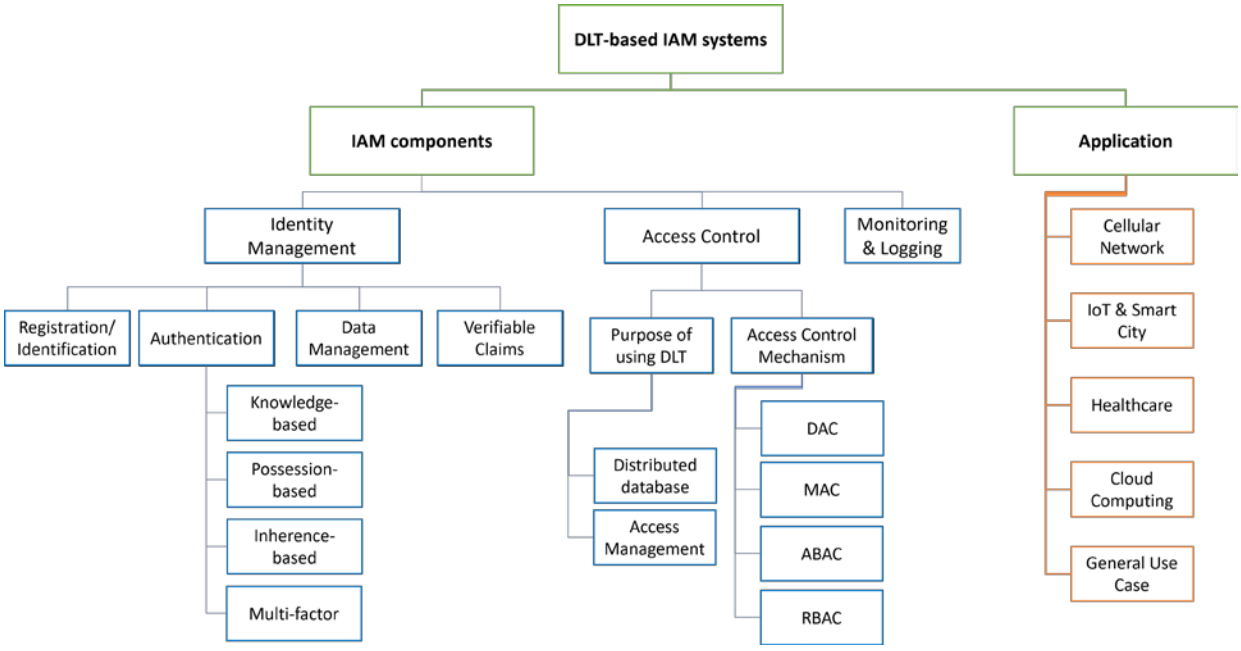

Figure3 Taxonomy of existing DLT-based IAM structure

4.2 Current challenges of IAM in IoT

As mentioned above, urgent needs for decentralized access control and management can be observed throughout the IoT landscape because of its large scale and heterogeneity [Pal2022]. In other words, traditional centralized mechanisms were less favorable given its prone to single point of failure, high cost, duplication, and complexity to the users [Ghaffari2022]. While the ABAC access control method assigns more responsibilities to users and slightly alleviates the problem, it is still not compatible with the distributed landscape of IoT. Thus, to promote self-sovereign identity which enhances privacy and security, blockchain, a by nature decentralized technology, and blockchain-based IAM can be a highly potential alternative [Ghaffari2022].

4.3 Blockchain-based solutions

[Liu2020c] evaluated three popular blockchain-based IdM systems, namely, Sovrin, Uport and Shocard. By comparing them against Cameron's Laws of Identity [Cameron2005], the paper showcased that all three models can fulfill most of the requirements, indicating the superiority and feasibility of implementing blockchain-based solutions as alternatives for traditional IAM. The paper also provided a comprehensive list of literature reviews on other blockchain-based solutions, viewing authentication, privacy, and trust as three central pillars for distributed IAM.

[Pal2022] had a detailed exploration of the advantages of blockchain and investigated how these features can be leveraged to resolve the dilemma of centralized IAM for large-scale IoT. Additionally, it also introduced five key features for the evaluation of access control for IoT. These include resource management, access rights transfer, permission enforcement, attribute management, and scalability. Using this proposed framework, the researchers exhibited the pros and cons from the results of the comparison among 3 traditional access control mechanisms and blockchain-based mechanisms. Results can be found in the Figure 4 [Pal2022]. Based on the observations, the paper stated the advantages of blockchain include the elimination of centralized controllers and the enrichment of IoT security features with immutability, auditability, and accountability.

AC Mechanisms	Advantages	Disadvantages
RBAC	Provides stronger security by enforcing effective policy management.	Policy management and their informants are highly centralised. It typically requires explicit user assignment to specific roles and supports only pre-defined and static policies which do not support the scale of an IoT system.
ABAC	Provides flexibility as the access control decision is performed based on attributes. It helps to enforce fine-grained access control policies in real-time.	In an IoT context, the use of ABAC raises important questions of the number of policy requirements, the policy evaluations, storage of attribute policy base, and the associated cost of applications.
CapBAC	Considers the resource-constrained characteristics of the IoT devices simplifies the distribution of permissions, and allows fine-grained access control. It is decentralised by nature.	Management of the number of capabilities that are required in a realistic IoT system and the issues of capability propagation and revocation are two common challenges when employing it for IoT systems.
Blockchain	Provides high security to prevent unauthorised data access. It is a distributed database of verifiable records.	Scalability remains an open issue for blockchain management. For instance, blockchain ledgers can expand large over time that raises the issue to download and store the ledger.

Figure 4. Pros and cons of different access control mechanisms used in IoT [Pal2022]

[Ghaffari2022] carried out a holistic survey on the usage of distributed ledger technology, which is the parent domain of blockchain, and pointed out some drawbacks of blockchain-based IdM. Specifically, one major drawback is that a central server or intermediaries for data storage and key revocation are still relied upon in decentralized solutions, creating another possible single point of failure instance.

4.4 Summary

Though not perfect, blockchain-based IAM solutions still outperform all other current centralized IAM implementations by offering beneficial characteristics such as being decentralized, scalable, audible, non-repudiable, and permanent.

---

5 Conclusion

This paper provided a survey on how secure network device identity can mitigate the challenges in IoT mainly from three angles, the PKI implementation, different device identification techniques, and the identity and access management process. Being a fundamental infrastructure for network security, PKI has played a crucial role in existing IoT. The combined implementation of PKI and DNS can enhance the current security level and show a promising future. Device identification techniques have exhibited advantages in different domains based on their features. Future researchers can take this as a reference and select proper methods to best fit the situations. In terms of IAM, the current trend is toward decentralization and self-management due to the explosion of M2M traffic as these approaches are more efficient and effective. Blockchain-based IAM is a powerful candidate and has already shown its merits. However, the limitations of blockchain including scalability remained as future research topics.

List of Acronyms

IoT	Internet of Things
M2M	machine-to-machine
GUI	graphical user interfaces
RPL	Routing Protocol for Low-Power and Lossy Networks
PKI	Public Key Infrastructure
DOI	Digital object identifier
CA	Certificate authorities
PKIX	Public Key Infrastructure using X.509
DNS	Domain name system
DANE	DNS-based Authentication of Named Entities
DNSSEC	DNS Security Extensions

TLS	Transport layer security
ECQV	Elliptic Curve Qu-Vanstone
DL	Deep Learning
IAM	Identity and access management
IdM	Identity management
AAC	Access control
DAC	Discretionary access control
MAC	Mandatory access control
RBAC	Role-based access control
ABAC	Attribute-based access control

References

[X.509]	"X.509", https://en.wikipedia.org/wiki/X.509, [ITU standard for public key certificates]
[DNS]	"Domain Name System", https://en.wikipedia.org/wiki/Domain_Name_System, [Resource records for DNS]
[Malik2019]	M. Malik, M. Dutta, and J. Granjal, "A Survey of Key Bootstrapping Protocols Based on Public Key Cryptography in the Internet of Things," IEEE Access, vol. 7, pp. 27443-27464, 2019, doi: 10.1109/ACCESS.2019.2900957.
[Singla2018]	A. Singla and E. Bertino, "Blockchain-Based PKI Solutions for IoT," 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), Philadelphia, PA, USA, 2018, pp. 9-15, doi: 10.1109/CIC.2018.00-45.
[Diaz-Sanchez2019]	D. Diaz-Sanchez, A. Marin-Lopez, F. A. Mendoza, P. A. Cabarcos, and R. S. Sherratt. 2019. TLS/PKI Challenges and Certificate Pinning Techniques for IoT and M2M Secure Communications. Commun. Surveys Tuts. 21, 4 (Fourthquarter 2019), 3502-3531, doi: 10.1109/COMST.2019.2914453.
[Balakrichenan2022]	S. Balakrichenan, I. Ayoub and B. Ampeau, "PKI for IoT using the DNS infrastructure," 2022 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA), Bangalore, India, 2022, pp. 1-8, doi: 10.1109/PKIA56009.2022.9952253.
[Ayoub2023]	I. Ayoub, S. Balakrichenan, K. Khawam, and B. Ampeau, "DNS for IoT: A Survey," Sensors, vol. 23, no. 9, p. 4473, May 2023, doi: 10.3390/s23094473.
[HaddadPajouh2021]	H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements,

challenges, and solutions," Internet of Things, vol. 14, p. 100129, 2021, doi:10.1016/j.iot.2019.100129

[RFC8477] J. Jimenez, H. Tschofenig, and D. Thaler, Report from the internet of things (IOT) semantic interoperability (IOTSI) workshop 2016, IETF RFC 8477, Oct 2018, doi:10.17487/rfc8477

[Liu2022a] X. Liu, Y. Han, and Y. Du, "IoT Device Identification Using Directional Packet Length Sequences and 1D-CNN," Sensors, vol. 22, no. 21, p. 8337, Oct. 2022, doi: 10.3390/s22218337.

[Chowdhury2023] R. R. Chowdhury, A. C. Idris, and P. E. Abas, "Internet of things: Digital footprints carry a device identity," presented at the 8TH BRUNEI INTERNATIONAL CONFERENCE ON ENGINEERING AND TECHNOLOGY 2021, Bandar Seri Begawan, Brunei Darussalam, 2023, p. 040003. doi: 10.1063/5.0111335.

[Aksoy2019] A. Aksoy and M. H. Gunes, "Automated IoT Device Identification using Network Traffic," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-7, doi: 10.1109/ICC.2019.8761559.

[Fan2023] L. Fan et al., "GraphIoT: Accurate IoT Identification based on Heterogeneous Graph," 2023 IEEE/ACM 31st International Symposium on Quality of Service (IWQoS), Orlando, FL, USA, 2023, pp. 01-04, doi: 10.1109/IWQoS57198.2023.10188710.

[Liu2021b] Y. Liu, J. Wang, J. Li, S. Niu and H. Song, "Machine Learning for the Detection and Identification of Internet of Things Devices: A Survey," in IEEE Internet of Things Journal, vol. 9, no. 1, pp. 298-320, 1 Jan.1, 2022, doi: 10.1109/JIOT.2021.3099028.

[Liu2020c] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. Raymond Choo, "Blockchain-based identity management systems: A review," Journal of Network and Computer Applications, vol. 166, p. 102731, Sep. 2020, doi: 10.1016/j.jnca.2020.102731.

[Pal2022] S. Pal, A. Dorri, and R. Jurdak, "Blockchain for IOT Access Control: Recent Trends and Future Research Directions," Journal of Network and Computer Applications, vol. 203, p. 103371, 2022. doi:10.1016/j.jnca.2022.103371

[Ghaffari2022] F. Ghaffari, K. Gilani, E. Bertin, and N. Crespi, "Identity and access management using distributed ledger technology: A survey," International Journal of Network Management, vol. 32, no. 2, p. e2180, 2022, doi: 10.1002/nem.2180.

[Cameron2005] Cameron, K., 2005. The laws of identity. Microsoft Corp 12, 8-11.
