Chapter 3
Access Control and Authentication in IoT

Bhaskara Santhosh Egala and Ashok Kumar Pradhan

3.1 Introduction

The IoT devices are broadly classified as constrained and non-constrained based on their processing capabilities. The constrained devices are limited in computational resource capabilities and have minimal network connectivity. These devices come with pre-coded static operational instruction sets and less scope for the user or dynamic configurations. For example, smart lights, door and window sensors, temperature and humidity sensors come under this category. Because of limited processing capabilities, these devices mainly depend on a third-party computational service such as cloud computing for their data analysis. Moreover, they depend on intermediate gateways for secure communications with the remote cloud. In order to communicate with other devices, a variety of networking mediums such as wireless fidelity (Wi-Fi), short-range wireless technologies (Bluetooth and near-field communication (NFC)), and cellular networks are employed. The non-constrained devices, on the other hand, or self-reliant and have the necessary data storage and processing capability. They perform basic data operations to make primary decisions for actuators. Further, they communicate with the cloud for high computational and data storage operations. Though these devices are more capable, they still depend on manual configurations to operate. At the same time, the improper configurations and default devices configurations lead to cyber-attacks. Also, both category devices do not have whole-level security mechanisms by default and come with limited configurations. In order to protect these devices from cyber-attacks, we need more specific and lightweight mechanisms. Most of these mechanisms point to the need for identity management and access control. Deploying device-specific security mechanisms is not worthy if we need to maintain a vast number of IoT devices. One compromised device weakens total system security. In 2016, a complex distributed denial of service (DDoS) attack was initiated on a well-known security service provider's

B. S. Egala · A. K. Pradhan (✉)
SRM University, Amaravati, Andhra Pradesh, India
e-mail: ashokkumar.p@srmap.edu.in

B. S. Egala
e-mail: bhaskara_santhosh@srmap.edu.in

S. Saxena and A. K. Pradhan (eds.), *Internet of Things*, Transactions on Computer Systems and Networks, https://doi.org/10.1007/978-981-19-1585-7_3

website using the Mirai IoT botnet (Antonakakis et al. 2017). The recent security breaches highlight the necessity of multilayer security for IoT devices to guarantee their security and privacy levels to combat future attacks. This layer filters most of the cyber-attacks and minimizes the effect on the IoT system operations. We can use intermediate gateways and public cloud computing to deploy these layers. In this chapter, the primary security breach surface vectors and identity management mechanisms are highlighted in Sect. 3.2. Authentication mechanisms to support privacy features in the IoT ecosystem are discussed in Sect. 3.3. We have given a brief introduction to the access control mechanism in Sect. 3.4.

3.2 Identity Management in IoT

Every device in the IoT ecosystem requires a unique identity in order to implement security rules. Devices can use strong identity management to identify themselves before establishing a secure connection with other devices and users. A typical device life cycle of activities includes identity formation at the design device, device registration at manufacturing, assigning deployment certificates for field deployment, identity parameter maintenance, and revoking or terminating identity parameters of the device.

- **Identity at Designing-Stage**: The initial stage in the identity creation and management of IoT devices starts with the designing stage itself. Every device gets an essential identity in the development stage and flashes to its ROMs for future deployment. The identity is mainly related to manufacturing and device unique manufacture identity and essential certificates for secure operations. Since most IoT devices are not updated with security patches throughout their lifetime, the design stage places a more significant role in device identity management. Besides the heterogeneous nature of manufacture designing policies, it becomes too challenging to use manufacture given identity to control the IoT ecosystem.
- **Deployment**: The primary identification of the device is used to register it locally, and a secondary identity is produced. In addition, depending on the deployment, devices are classed as Brownfeaild or Greenfeaild. A single corporation or organization can only use the secondary identity. A set of specialized cryptography settings is also included in the deployment. When a device enters a live state, these values are utilized to send or receive data from other devices. It streamlines the organization's auto-identification procedure.
- **Manage**: To extend their life and functionality, deployed devices are subjected to continual monitoring or device management. The credentials and crypto parameters are renewed or revoked at this step, depending on the circumstance. Any device's identity gets extended or destroyed as a result of this. Furthermore, secure over-the-air (OTA) updates are sent regularly to ease device administration and enable automation. This step includes ownership transfer, certificate renewal, reporting, and logging.

- **End of Device life**: An IoT device's last step likewise serves as the final stage of its identification. The gadget is zeroed when the identification has been received. To reduce the attack surface, it is critical to revoke certificates and security credentials. Attackers have been known to utilize the revoked or fabricated identities of zeroization devices in the past. As a result, the revocation and identity management system should be designed to identify and prevent counterfeit identities. Figure 3.1 illustrates the normal identity management life cycle in IoT ecosystem.

The different identity management coupling methods are depicted in Fig. 3.2. The coupling of identity in the same domain is simpler and more manageable, whereas different domains with weak identities are challenging.

Furthermore, the sort of protocols and services that the device uses to interact on the Internet may generate the device's identity. We may further divide identity into two types: physical identity and virtual identity. Physical identity refers to the hardware characteristics that distinguish devices, such as the media access control (MAC) address and defined communication settings. Radio frequency identification (RFID) is an example of a radio wave system to show its identification. The constrained application protocol (CoAP) is intended to allow HTTPS-based restful IoT apps. The current IoT devices are not self-protective from identity theft attacks; moreover, they depend highly on physical identity than virtual identity in industry 4.0 use-cases. These are inconvenient and unsuitable for IoT ecosystem privacy and security in real time. As a result, keeping one's identity hidden from the outer world is essential. A defined namespace is a superior choice for hiding a device's existence on the internet. Identity lifecycle design also includes establishing extensible identity management, identifying the needed security methods, and clearly defining privacy policies for various data species. The deployment procedure should begin

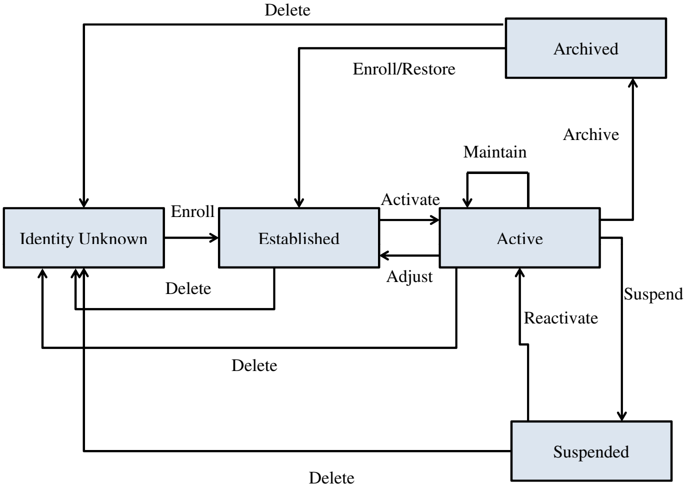


Fig. 3.1 Identity management life cycle in IoT ecosystem

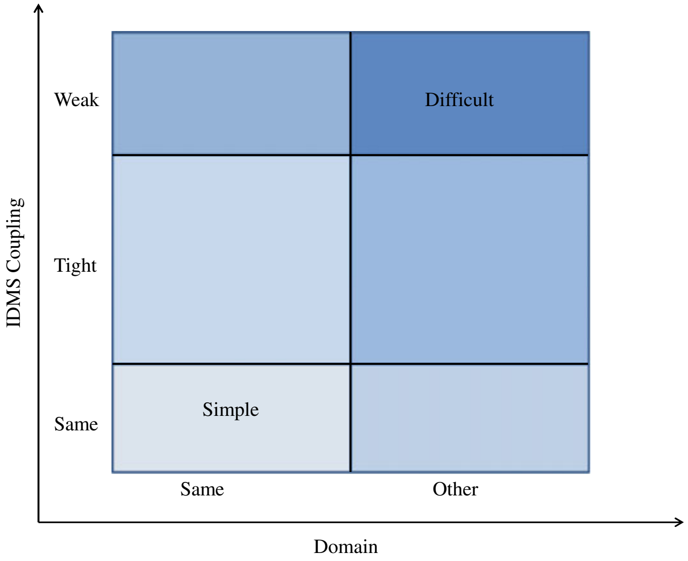


Fig. 3.2 Identity management systems coupling in IoT ecosystem

with resetting the default passwords to protect devices against assaults. In multicasting use-cases, an identity might refer to a collection of devices and an entity can have several identities (Dib and Toumi 2020).

3.2.1 *Inter-domain Identity Management Architectures*

IoT virtual identity management is a particularly significant operation in inter-domain identity management architectures. Figure 3.3 shows an inter-domain identity network operation structure in which individual identity management systems are collectively accountable for directing a specific network-level identity. The structure may be improved by incorporating scale scenarios with intermediate coordinating identity management subsystems (IDMSS).

Figure 3.4 showcases an alternate standard structure in which various IDMSS collaborate on a peer-to-peer basis. In this architecture, not every IDMSS system will interact with others in the network to form the network-level identity. Only one peer takes responsibility for formulating the identity using the remaining IDMSS systems information.

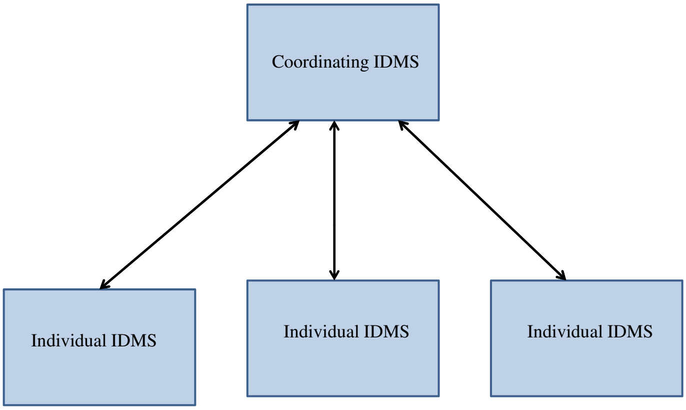


Fig. 3.3 Centrally coordinated IDMSS network

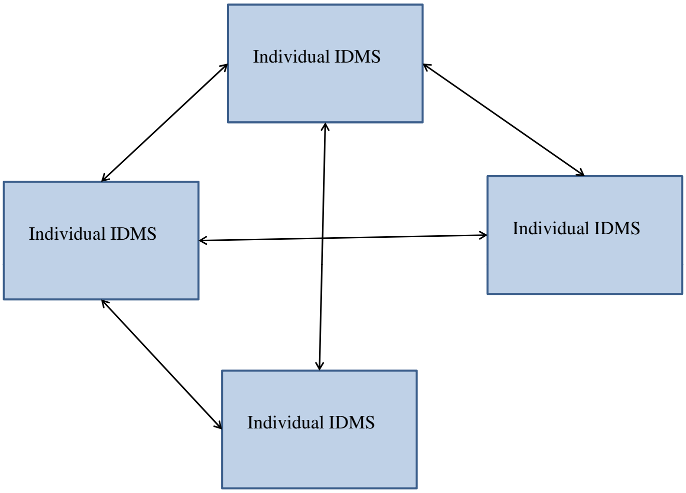


Fig. 3.4 Peer-to-peer coordination

3.2.2 Techniques to Build a Coordinating System

While developing a coordinating system for inter-domain identity management introduces technical and management issues because of ambiguity in IDMSS level operations. As shown in Figs. 3.3 and 3.4, every subsystem should share its local identity information over the TCP/IP layer with a central coordinating system. The network-level identity is an agreement between the subsystems and coordinating system to validate the new identity throughout the network (Jia et al. 2020).

3.2.3 Single Sign-On Identity Federation

When it comes to forming identity coalitions, single sign-on (SSO) (Teravainen 2020) is a frequently requested feature, especially when people are involved. SSO enables the use of a reality's identity in one sphere to authenticate a reality in another. SSO's purpose is to assist in dealing with individualities in two or more disciplines simultaneously. The identity confederation agreement has completely automated protocols and processes for data processing and interchange among disciplines. Enterprise and pall system designs can be seen using cryptography-based identity coalitions to offer SSO services. Some of the most widely used authentication protocols are SAML (Ferdous and Poet 2013), OpenID (Recordon and Reed 2006), and OAuth2.0 (Fett et al. 2016). The SSO protocols allow humans and IoT devices to consume digital services by maintaining identity and trust between multiple actors. It reduces the burden on people and devices by eliminating the requirement of remembering the credentials all the time. The simplified examples where we can use these methods are as follows.

3.2.3.1 Network-Level Service for Nodes Communication

A lightweight M2M (LWM2M) operation protocol is used to send and receive data to and from other service devices and operation services. Because the quantity of services utilized is largely constant during the lifespan of the IoT device, and there is no mortal convenience advantage, an SSO-able identity confederation is not required in this situation. Using business SSO protocols on tiny IoT devices, on the other hand, adds a tremendous amount of complexity to the device firmware. When SSO is required on an IoT device, Featherlight SSO protocols should be investigated instead. Mahkonen et al. (2013) is a mobile network technology that permits an identity from one province to be reused across many disciplines. Using mobile network subscribers' individualities, relevant key cryptographic material, and cryptographic algorithms, the GBA structure provides a transient, cryptographically secured link between an IoT device and a service in the operation layer. Before granting service access, the security association may conduct conditioning, such as authenticating the IoT device. For mobile networks, a GBA uses well-known identity information suppliers (IIPS). The IoT gadget operates with a GBA-compatible SIM such as a universal integrated circuit card (UICC)/embedded universal integrated circuit card (eUICC) (Smeets 2019). Despite the fact that the 3GPP identity and GBA are now connected with cellular networks, this technology may connect non-3GPP items to a network. In this case, attack-specific sequestration and protection methods may be utilized to safeguard the corresponding credential and supporting software, avoiding the use of UICC in IoT devices.

3.2.3.2 Mapping

The strength of SSO is entirely dependent on its cryptographic mechanisms; in SSO operations, no data about participant identity, security keywords, or cryptography methods are exchanged with other participants. Still, this is not the only way to create a confederation of identities. Another popular method for forming an identity federation is mapping. The identification of one field is counterplotted with the identity of another. The mapping can be carried out precisely as written or with slight changes. The mapping process contains adding redundant identity data to respective original identities in a synchronized passion from multiple locations in the entire day. A communication machine is a software structure used for communication and event exchange among IDMSS. Regardless of whether these two mapping methodologies are used, simultaneous changes to the counterplotted data in the linked disciplines must be addressed. By designating one field as the master for particular identity data, this may be prevented. Two distinct techniques of solving issues with tracking and syncing idenitities are three-way merging and differential synchronization. The IDMSS ecosystem might be modest or large, and it can contain a few or many different forms of identifying data. Figure 3.5 depicts four identity operation disciplines, each of which abstractly embodies the technological and organizational characteristics of an IoT system.

- **Service User Domain(SUD)**: The location where the Internet of things registrars identity and operates.
- **Service Management Domain(SMD)**: The location where the IoT device's operation or services are linked to business operation waiters who handle freight data.

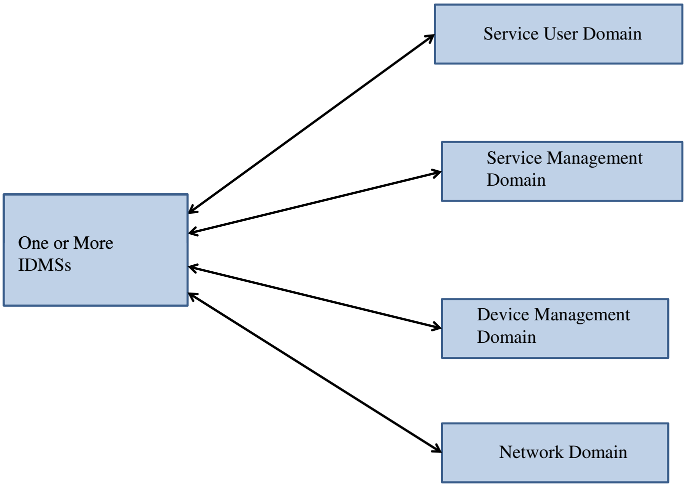


Fig. 3.5 IMDs in the IoT

- **Device Management Domain(DMD)**: Services based on the LWM2M protocol to manage essential device functions such as the device lifecycle and firmware or operating system.
- **Network Domain(ND)**: The network domain (ND) describes how IoT communication takes place, for as through a cellular network or another sort of wide area network (WAN) or a local area network (LAN). In the Internet of things, there are four distinct identity management domains (IMD) as represented in Fig. 3.5.

3.3 Authentication Mechanisms in IoT

Convention authentication and authorization approaches are ineffective due to many IoT heterogeneous nature and different machine-to-machine communication characteristics. For dispersed IoT settings, experimenters in Xu et al. (2018) presented a capability-grounded access control paradigm. It allows groups to participate in a single commemorative and uses IPsec to give end-to-end security. A panhandler can communicate with any device in a group using a single commemorative for group access. The network prefix unique original identifier is used to construct an access group identification (ULA). A ULA identifies each device in the group. The panhandler in a group access commemorative has its ULA and the network prefix of the access group. As a result, the commemorative's ULA and prefix may be used to authenticate the groups of objects. It can also provide admission if the panhandler has a ULA commemorative. Cruz-Piris et al. (2018) is an OAuth2.0 profile that allows vivid agents to have multiple access requirements, according to the Stoner-Managed Access paradigm. "SmartOrBAC," based on the OrBAC paradigm, was presented as a unique access control architecture for an IoT environment in Pasquier et al. (2015). Web services were employed to operate the security applications in this method. We have a variety of models based on parameters and operation style. In this part, just a few of them are examined in depth.

Though the classical OrBAC works best in a centralized system, it lacks collaboration capabilities and security conversion mechanisms. For that reason, a SmartOrBAC is introduced to get around these limitations. The work in Pereira et al. (2014) suggested a novel access control structure for power-constrained devices. It combines the principles of Kerberos and RADIUS access control systems to provide a dependable access control framework. In order to achieve low-power access control and authentication, it barrows and combines features of Kerberos and Constrained Application Protocol (CoAP). A lightweight, secure, and scalable IoT group authentication protocol named threshold cryptography grounded group authentication (TCGA) is introduced by Mahalle et al. Mahalle et al. (2014) to simplify the group authentication process. Group authentication reduces the handshake's outflow, resulting in lower resource use and energy savings. TCGA successfully eliminates man-in-the-middle attacks over IoT networks. Tomanek and Kencl (2016) demonstrated a method for ensuring the security of a smart home system using the AllJoyn framework and uses elliptic curve cryptography to authenticate users. Lee et al. 2014 proposed the lightweight authentication technique by upgrading the original RFID system security basis for IoT. Current RFID systems do not use encryption for authentication, which is a security flaw. A lightweight cryptographic system based on the XOR technique that employs encrypted passwords for authentication is proposed to solve this problem. Existing certifications rely on signatures, which are difficult to apply on resource-constrained IoT devices. A confirmation code, on the other hand, is straightforward to maintain in an IoT setting. Zhao et al. 2011 introduced an asymmetric mutual authentication system for the Internet of things that performs authentication between the terminal node and the platform. Both SHA1 and feature extraction are used in the proposed method. As a result, IoT security, as well as computation and transmission costs, have decreased.

3.4 Access Control Models with Examples

As the backbone technology for ensuring information security, access control opens up possibilities for addressing the IoT's difficulties mentioned above. Access control can efficiently monitor resource access and prevent illegal data flow. However, because IoT search is a relatively new study topic, standard access control methods and approaches cannot adequately tackle IoT search's access control issues. The following are the aspects of data access in the IoT search environment. Figure 3.6 illustrates the IoT ecosystem access control taxonomy in very abstract form.

- **Massive**: According to a 2011 analysis, M2M traffic in the USA grew by 250 percent and estimated that it would cross the total Internet users count by 2020. As per the latest reports in 2021, nearly 25 billion devices are connected with a speed of 9. 127 new devices every second. These devices generate massive amounts of data which introduces new issues in data management and utilization.
- **Dynamic**: Nodes and users often change in the IoT search environment, and access objects are frequently added and removed. Because of its dynamic nature, it is impossible to forecast all user information ahead of time and correctly comprehend the user and permission structure.
- **Strong Privacy**: Data privacy and security have become increasingly crucial as data sharing has progressed. Many privacy proposals, such as ISO/IEC 29100:2011, privacy by design, global data protection law, and fair information practice principles, have been suggested by governments and researchers to safeguard an individual's privacy. On the other hand, many academics wonder whether these principles have aided privacy because some of them emphasize individual control over data rather than data security.
- **Multiparty Commonality**: Data is no longer restricted to a single or closed environment in IoT search; instead, it is created and shared by a number of cooperating entities. Multiple dynamically connected information systems make up the IoT search service. Information is transferred and shared across partnering firms to meet the complex application needs.

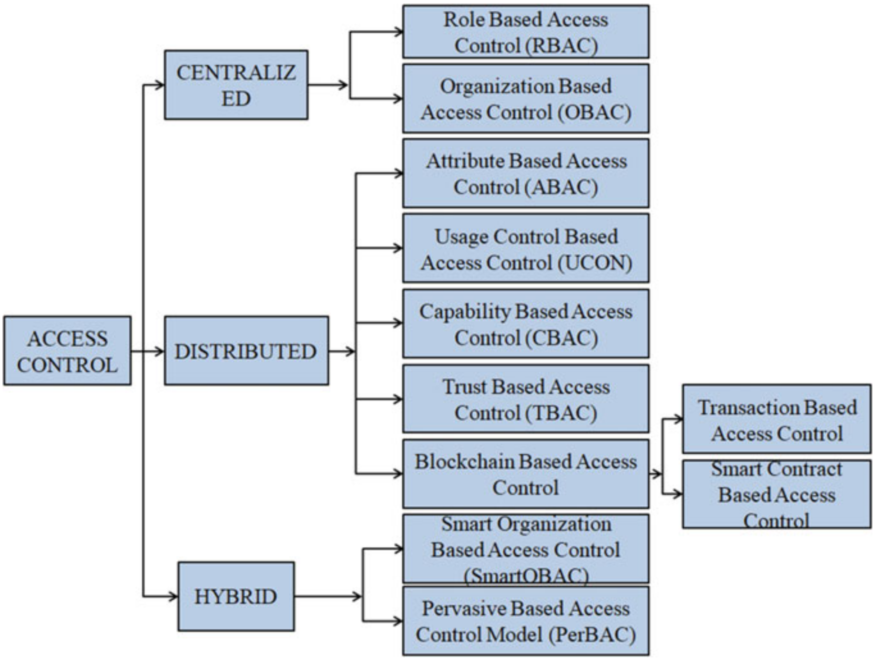

ACCESS CONTROL
CENTRALIZED
DISTRIBUTED
HYBRID
Role Based Access Control (RBAC)
Organization Based Access Control (OBAC)
Attribute Based Access Control (ABAC)
Usage Control Based Access Control (UCON)
Capability Based Access Control (CBAC)
Trust Based Access Control (TBAC)
Blockchain Based Access Control
Transaction Based Access Control
Smart Contract Based Access Control
Smart Organization Based Access Control (SmartOBAC)
Pervasive Based Access Control Model (PerBAC)

Fig. 3.6 Access control taxonomy

Access control mechanism monitors and controls the resources access and utilization based on the defined rules. It acts as the primary security mechanism when maintaining data confidentiality and privacy. Standard access control methods and approaches, on the other hand, are unable to fully address the access control difficulties that IoT search meets because it is a relatively new study area. To achieve specific goals, data is constantly exchanged and shared among devices and people in the IoT ecosystem. In this shared environment, authentication, secrecy, and access control are all required for safe communication. In this shared environment, authentication and secrecy are required to build a secure communication system. How can the edge device verify that the query or command coming from the authorized device is genuine? To ensure authenticity and secrecy, public-key cryptography, signatures, and authentication are commonly utilized. Access control is applied to the data stream in the IoT environment rather than the traditional database management system. Ensure access authorization, managing the scalable IoT architecture, handle a large amount of data stream are some of the access control issues in this case.

By the 1970s, access control schemes like the BLP model and the Biba model Jin and Shen (2012) were primarily used in mainframe systems. The BLP idea is based on a military security approach that addresses hidden hierarchical information access management challenges. It is the first rigorous theoretical proof of a mathematical access control paradigm. In 1975, Kenneth J. Biba created the Biba model. The formal state transition system of a computer security policy establishes access control rules for maintaining data integrity. The Clark–Wilson model Vimercati and Samarati (2011) was published by Clark and Wilson in 1987 to track and audit the subject's state transition as well as the low-watermark policy parameters' runtime alterations. In contrast to Biba, the Clark–Wilson approach uses controlled state transfers to offer comprehensive integrity protection. The Biba model, on the other hand, provides a main multilevel integrity access control mechanism, but it cannot be used without the existence of a trusted subject. As the criteria for computer trustworthiness expanded in the 1980s, research recommended for more flexible access control techniques.

One of the most typical works is the US Department of Defense's trustworthy computer system assessment criteria (TCSEC) (DoD). TCSEC is a standard that specifies the core criteria for assessing the efficacy of security systems. TTCSEC divides access control into two categories depending on the tasks of access authority users as discretionary access control (DAC) and mandatory access control (MAC). Legal users can access objects as individuals or organizations under the DAC paradigm, but illegitimate users cannot. Due to the high level of administrative complexity, DAC must manually manage users, authority, and resources, making it inappropriate for IoT search. A central authority can use the MAC model to assign access rights based on regulations. This category includes policies from both the business and public sectors. In MAC applications, a multilayer security architecture is widely utilized. Despite the fact that the MAC approach overcomes the problem of decentralized resource management by centralizing permission management, it is inefficient for IoT search users.

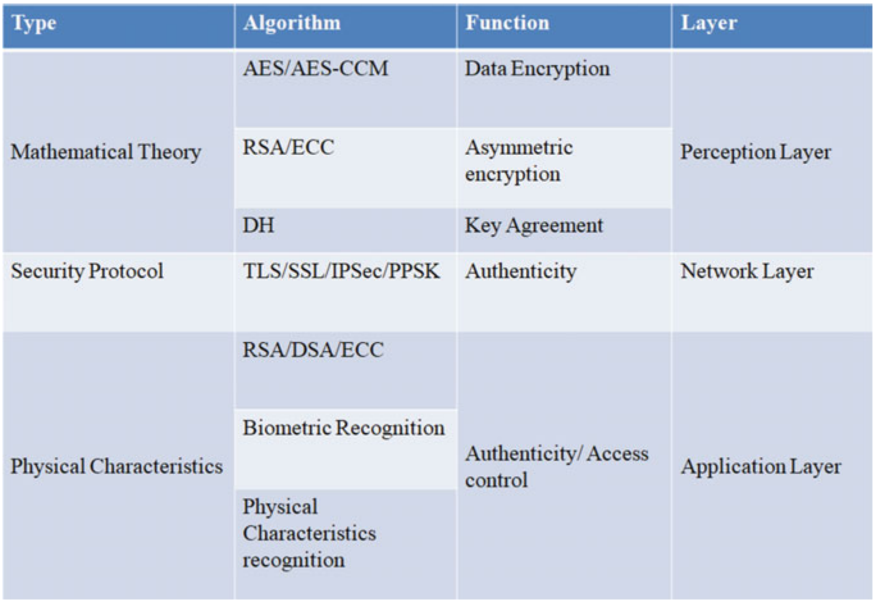
With the introduction of the Internet and the proliferation of large-scale applications of information systems in businesses around the year 2000, traditional access control models like DAC, MAC, and their extension models struggled to handle sophisticated application layer access needs. It was advised to adopt a role-based access control (RBAC) (Sandhu 1998), which limits system access to authorized users. Role permissions, user roles, and role linkages are all components of RBAC that make user assignments simple. RBAC may be used in large corporations to ease security administration and verify that information systems meet information integrity standards. In contrast to MAC and DAC, RBAC can execute these requirements without generating any problems. Access control technology-based applications face substantial challenges when new computer environments emerge, such as Internet of things (IoT) search. DAC, MAC, and RBAC are examples of closed environment approaches incompatible with current computer settings. ABAC Kolter et al. (2007) defines access control rules based on different attributes and environmental attributes, based on the combination of attributes resources or services are allocated or denied.

Ferraiolo et al. (1999) presented RBAC in 1992, a role-based access control system. Unlike traditional access control models, which require a system administrator to assign responsibilities, ownership manually, or security labels to users and objects, ABAC allows users and objects to define access policies based on existing attributes. Because characteristics may represent objects from numerous viewpoints, users can alter access control strategies based on actual circumstances. TRBAC (Bertino et al. 2001) is a temporal RBAC modification that leverages triggers to allow for recurring role enabling, disabling, and temporal dependencies via triggers. Along with time data, location limits must be handled in the IoT environment. When access to resources involves taking into account both time and location information, researchers have proposed spatiotemporal RBAC (STRBAC) (Geepalla et al. 2013) as a high-level concept of access control. Meanwhile, the creators of (Park and Sandhu 2004) developed concept utilization control (UCON), which enables for finer-grained regulation of digital object utilization than standard access control rules and models.

The features of access control entities influence ABAC's access control decisions. Subject attributes, object attributes, permission attributes, and environmental attributes are frequently expressed as four tuples. Although ABAC provides users with a great deal of control over their access to resources, personal data security is not considered. Studies suggest attribute-based encryption (ABE), which encrypts objects based on attribute-based access limits, based on the notion of classical ABAC.

Well-known ABE variants are key policy-based ABE (KP-ABE) (Attrapadung et al. 2011) and cipher-based ABE (CP-ABE) (Porwal and Mittal 2017). In KP-ABE, the policy is linked with the user's private key, whereas in CP-ABE, attributes of the policies are encrypted with the help of the user's private key. The KP-ABE is an inverse form of CP-ABE, where in the first user, freedom is relatively strong. In contrast, data owner freedom is decreased and coming to the second, the data owner determines the access control policy, which gives additional control to the data owner. Figure 3.7 presents a holistic comparison of well-known access control models.

- **Based on ABAC**: All qualities linked with characteristics are used to identify the person and the object. When a user submits an access request in the ABAC model, he is given the appropriate access permission based on his characteristics. Recent research has concentrated on the concept of preserving user privacy since attributes may include users' private information, which, if leaked, would substantially hinder the development of ABAC. Xu et al. introduced the privacy-preserving ABAC (P-ABAC) method. The sensitive characteristics in the P-ABAC are handled using homomorphic encryption on the user's side.
- **Based on RBAC**: The RBAC model defines user responsibilities, privileges, and administrative functionalities as access rules and separates the underlying user tasks. It mainly suffers from role explosion over multiple domains due to improper access rules management. An improved model named service-based RBAC paradigm was proposed by Spiess Patrik (Jindou et al. 2012) to support IoT applications task-based access controls with the help of RBAC. An enhanced RBAC model employed by Zhang and Tian 2010 utilizes the context rules in order to deliver a more scalable, flexible, and lightweight access control mechanism.
- **Based on CapBAC**: In the CapBAC model, however, access control is the user's responsibility. A BlendCAC model, which is a blockchain-enabled decentralized CapBAC, was proposed by Xu et al. 2018. The BlendCAC approach, which leverages a smart contract for access authorization registration, propagation, and revocation, proposes a strong identity-based capability token management technique.



Type	Algorithm	Function	Layer
Mathematical Theory	AES/AES-CCM	Data Encryption	Perception Layer
	RSA/ECC	Asymmetric encryption	
	DH	Key Agreement	
Security Protocol	TLS/SSL/IPSec/PPSK	Authenticity	Network Layer
Physical Characteristics	RSA/DSA/ECC	Authenticity/ Access control	Application Layer
	Biometric Recognition		
	Physical Characteristics recognition		

Fig. 3.7 Security policies literature comparison

A cloud-based authentication framework was proposed by Barreto et al. (2015). Users can use the IoT cloud to manage various intelligent pervasive environments by accessing IoT-based resources and capabilities. In large-scale IoT systems, a federated CapBAC (FedCAC) (Xu et al. 2018) framework presented a strategy for managing identity-based capability tokens, which includes registering, propagating, and revoking access.

- **Based on UCON**: While active user access is active, the UCON model provides a wide range of access qualities by enabling given access to be withdrawn and use to be terminated. UCON is an innovative and promising access control solution for open, distributed, heterogeneous, and networked computer environments. The PEI, a UCON-based security framework that takes a tiered approach to policy, enforcement, and model implementation, was introduced by Zhang et al. (2010). The policy model layer specifies predicates on subject and object properties, system attributes as conditional restrictions, and user actions as obligations.
- **Organizational-Based Access Control (i.e., OrBAC):** In order to form OrBAC, a new dimension called "organization" is added to the existing RBAC paradigm. OrBAC is enhanced by the Trust-OrBAC paradigm, which adds the idea of trust management. With various options, Trust-OrBAC provides two dynamic trust vectors, one for organizations and one for users. The Tr-OrBAC paradigm, which combines Trust, increases cross-organizational collaboration while avoiding malicious activity. The SmartOrBAC concept broke down the challenge into layers. SmartOrBAC divides processing expenses across limited and unconstrained devices.

- **Blockchain or Biometrics Features based**: Because of the diversity of IoT devices, bio-characteristics are increasingly becoming one of the most important factors used to authenticate IoT devices and their users. Ferrag et al. (2019) looked at the biometrics utilized by authentication and authorization techniques for mobile IoT devices, such as voice, fingerprints, and other biometrics. FairAccess for IoT is a blockchain-based access control architecture presented by Ouaddah et al. (2017). New transaction types for giving, gaining, delegating, and canceling access are introduced in FairAccess. In FairAccess, the access token is required to access a protected resource, but it cannot be triggered until the access control conditions have been met. The real-time and bloat blockchain issues are the primary limitations of FairAccess when using the UTXO architecture of blockchain. In recent times, the authors in Egala et al. (2021), Egala et al. (2021) introduced a selective sharing access control mechanism for decentralized IoT medical and time-critical applications. It presents a holistic view of security architecture for time-critical IoT applications.
- **Open Authorization (i.e., OAuth)**: OAuth is a client-side access control mechanism for web server resources. The majority of traditional web and cloud application solutions are incompatible with the context environment. The OAuth-IoT framework was suggested by Sciancalepore et al. (2017) for access control. OAuth-IoT takes advantage of current open standards and harmonizes them correctly. For proper application authentication and authorization, OAuth-IoT natively supports any token format. Fernández et al. (2017) developed an OAuth paradigm for application-scoped authorization that allows controlling roles and permissions. OAuth 2.0 makes authorization incredibly light for all the essential information that is supplied with a token.

3.4.1 Open Challenges

1. **Policy Conflict Due to Fragmented Authorizations**: Several IoT access control solutions are available, the majority of which highlight the importance of integrating inter-domain access controls to form network-level controls. Nevertheless, they believe that a single entity governs resources by ignoring the multiparty sharing feature. Always considering multiple local rules may increase conflict in generating system-level access rules because of deviations in fragmented rules. Several techniques use an essential strategy to address this issue, such as approving access only when all users agree. This strategy, however, is too restrictive to be used in real-world applications since it would limit resource availability. More work is needed to focus on policy conflict resolution caused by varied authorizations, enhancing policy composition, and automating conflict resolution.
2. **Policy Conflict Due to fragmented Relationships between parties**: This sort of policy conflict arises due to the particular characteristics of the IoT search environment. In the process of integrating multiparty access control policies, the rules of multiple agents include several constraints. Access to the same resource

may be restricted differently by multiple owners. Based on these limits, several access control decisions that correspond to each resource may be derived. Each ace control option may be tailored to the needs of different users. However, the options may be mutually exclusive. Inconsistencies and disagreements are common when these constraints are combined. As a result, figuring out how to choose and update access control options for different users quickly and dynamically is a serious issue that must be solved.

3. **Attribute-Permission Assignment Within Noisy Data**: The Internet of things (IoT) search engine is a collaborative ecosystem that spans several domains. Distinct domains have different access control policies. Because attributes are essential, and the access control decision is made based on the set of attributes of the requester. Every non-ABAC access control model must be converted to the ABAC model to achieve unified administration of an access control policy. ABAC is well-suited to the IoT search context because it separates the policy administration from the access control decision. Moreover, ABAC requires a pure and quality correlation between attributes and permissions to migrate from role-permission and user-permission relationships. Noise data, in particular, is frequently included in the initial user-permission relationships, affecting policy generation accuracy and posing significant security threats to access control systems. A significant research problem in controlling access for IoT search is how to manage attribute-permission assignment inside noisy data.
4. **Modeling and Evaluation of IoT Security Search**: As the Internet of things (IoT) has grown in popularity, so has its security. In recent decades, many similar complex security challenges have been effectively solved using modeling and simulation (MS). MS approaches and tools are also helpful in tackling IoT challenges since IoT has a unique address and communicates using conventional communication protocols. However, modeling and evaluating IoT security searches have received little attention.
5. **Things authentication and anonymity in IoT**: In the subject of industrial control security IoT, many authentication mechanisms aiming at real-time communication between the cloud platform and sensing devices are being developed. However, these approaches' efficacy and security cannot always be ensured at the same time. More emphasis should be placed on device authentication and anonymity protection technologies to ensure the data source's reliability, privacy, and data availability.

3.4.1.1 Addressing Risks

There is no distrusting that IoT security is too complex, but experts in the area are well-clued in the stylish ways for practical threat assessment and compensating reduction. Expert cooperation makes IoT installations a breath. One of the crucial ideas is that security must be inaptly regarded right at the launch of the design process, inside the professional moxie stationed as soon as possible—indeed from outside the business if needed. There is no question that this procedure leads to increased security.

The longer the process of critically analyzing, testing, and hardening IoT results is held up, the more delicate and precious it becomes to do it right the first time. Worse yet, chancing significant excrescences or inadequate contingency medications after a suspected breach has formerly passed can be far more expensive.

According to Juniper Research's Star Critic Steffen Sorrell, cybersecurity in IoT is crucial. For enterprises, the first political step is to develop safety from the ground up, focusing entirely on the fundamentals. Consider the secure element as an example. It is possible to attach it to the device and use it to carry out cryptographic procedures. In the security chain, the tackle security module is an often duplicated critical tackle item (HSM). Structure protection from exposure is the first political step for businesses. We need to think about security holistically from the ground up (devices, networks, applications, infrastructure) regarding how they can be secured moment and in the future. The three pillars that uphold connected things and services must be defended as an overall cybersecurity strategy.

- Confidentiality,
- Integrity,
- Availability.

It is a matter of designing applicable security within the three security pillars to guarantee that their pretensions are met. Companies may help unauthorized access to data, things, and software by espousing recommended security results, similar as device and authentication operation results grounded on encryption ways, as soon as possible, with expert knowledge applied.

References

Antonakakis M, April T, Bailey M, Bernhard M, Bursztein E, Cochran J, Durumeric Z, Halderman JA,Invernizzi L, Kallitsis M, Kumar D, Lever C, Ma Z, Mason J, Menscher D, Seaman C, Sullivan N, Thomas K, Zhou Y (2017) Understanding the mirai botnet. In: Proceedings of the 26th USENIX Security Symposium

Attrapadung N, Libert B, de Panafieu E (2011) Expressive key-policy attribute-based encryption with constant-size ciphertexts. In: Catalano D, Fazio N, Gennaro R, Nicolosi A (eds) Public key cryptography-PKC 2011, Berlin, Heidelberg. Springer, Berlin, pp 90–108

Barreto L, Celesti A, Villari M, Fazio M, Puliafito A (2015) An authentication model for IoT clouds. In: 2015 IEEE/ACM International conference on advances in social networks analysis and mining (ASONAM), pp 1032–1035

Bertino E, Bonatti P, Ferrari E (2001) Trbac: a temporal role-based access control model. ACM Trans Inf Syst Secur 4:191–233

Capitani De, di Vimercati S, Samarati P (2011) Clark and Wilson model. Springer, US, Boston, pp 208–209

Cruz-Piris L, Rivera D, Marsa-Maestre I, De la Hoz E, Velasco J (2018) Access control mechanism for IoT environments based on modelling communication procedures as resources. Sensors (Basel, Switzerland) 18:03

Dib O, Toumi K (2020) Decentralized identity systems: architecture, challenges, solutions and future directions. Ann Emerg Technol Comput 4(19–40):12

Egala BS, Pradhan AK, Badarla V, Mohanty SP (2021) Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet Things J 8(14):11717–11731

Egala BS, Pradhan AK, Badarla V, Mohanty SP (2021) iblock: an intelligent decentralised blockchain-based pandemic detection and assisting system. J Signal Process Syst 10:1939–8115

Ferdous MS, Poet R (2013) Dynamic identity federation using security assertion markup language (saml). Policies Res Identity Manag 131–146

Fernandez F, Alonso A, Marco L, Salvachua J (2017) A model to enable application-scoped access control as a service for IoT using oauth 2.0. In: 2017 20th conference on innovations in clouds, internet and networks (ICIN), pp 322–324

Ferrag MA, Maglaras L, Derhab A (2019) Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends. Secur Commun Netw 04

Ferraiolo DF, Barkley JF, Kuhn DR (1999) A role-based access control model and reference implementation within a corporate intranet. ACM Trans Inf Syst Secur 2:34–64

Fett D, Küsters R, Schmitz G (2016) A comprehensive formal security analysis of oauth 2.0. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, CCS '16, New York, NY, USA, Association for Computing Machinery, pp 1204–1215

Geepalla E, Bordbar B, Du X (2013) Spatio-temporal role based access control for physical access control systems, pp 39–42

Jia X, Hu N, Su S, Yin S, Zhao Y, Cheng X, Zhang C (2020) Irba:an identity-based cross-domain authentication scheme for the internet of things. Electronics 9(4)

Jindou J, Xiaofeng Q, Cheng C (2012) Access control method for web of things based on role and SNS. In: 2012 IEEE 12th International conference on computer and information technology, pp 316–321

Jin J, Shen M (2012) Analysis of security models based on multilevel security policy. In: 2012 international conference on management of e-commerce and e-government, pp 95–97

Kolter J, Schillinger R, Pernul G (2007) A privacy-enhanced attribute-based access control system. In: Barker S, Ahn G-J (eds) Data and applications security XXI, Berlin, Heidelberg. Springer, Berlin, pp 129–143

Lazouski A, Martinelli F, Mori P (2010) Usage control in computer security: a survey. Comput Sci Rev 4(2):81–99

Lee JY, Lin WC, Huang YH (A lightweight authentication protocol for internet of things. In: 2014 International symposium on next-generation electronics (ISNE), pp 1–2

Mahalle PN, . Prasad NR, Prasad R (2014) Threshold cryptography-based group authentication (TCGA) scheme for the internet of things (IoT). In: 2014 4th International conference on wireless communications, vehicular technology, information theory and aerospace electronic systems (VITAE), pp 1–5

Mahkonen H, Rinta-aho T, Kauppinen T, Sethi M, Kjällman J, Salmela P, Jokikyyny T (2013) Secure m2m cloud testbed. In: Proceedings of the 19th annual international conference on mobile computing &amp; networking, MobiCom '13, New York, NY, USA. Association for Computing Machiner, pp. 135–138

Ouaddah A, Elkalam A, Ouahman A (2017) Fairaccess: a new blockchain-based access control framework for the internet of things. Secur Commun Netw 9:02

Park J, Sandhu R (2004) The ucon<sub>abc</sub> usage control model. ACM Trans Inf Syst Secur 7:128–174

Pasquier IB, Ouahman AA, Kalam AAE, de Montfort MO (2015) Smartorbac security and privacy in the internet of things. In: 2015 IEEE/ACS 12th International conference of computer systems and applications (AICCSA), Los Alamitos, CA, USA, pp 1–8. IEEE Computer Society, Nov 2015

Pereira PP, Eliasson J, Delsing J (2014) An authentication and access control framework for COAP-based internet of things. In: IECON 2014—40th Annual conference of the IEEE Industrial Electronics Society, pp 5293–5299

Porwal S, Mittal S (2017) Implementation of ciphertext policy-attribute based encryption (cp-abe) for fine grained access control of university data. In: 2017 Tenth international conference on contemporary computing (IC3)

Recordon D, Reed D (2006) Openid 2.0: a platform for user-centric identity management. In Proceedings of the Second ACM Workshop on Digital Identity Management. DIM '06 (New York, NY, USA). Association for Computing Machinery, pp 11–16

Sandhu RS (1998) Role-based access control. Adv Comput 46:237–286

Sciancalepore S, Piro G, Caldarola D, Boggia G, Bianchi G (2017) Oauth-iot: an access control framework for the internet of things based on open standards. In: 2017 IEEE symposium on computers and communications (ISCC), pp 676–681

Smeets B (2019) Evolving SIM solutions for IoT. ericsson, 27 May 2019

Teravainen T (2020) What is single sign-on (sso) and how does it work? Apr 2020

Tomanek O, Kencl L (2016) Security and privacy of using ALLJoyn IoT framework at home and beyond. In: 2016 2nd International conference on intelligent green building and smart grid (IGBSG), pp 1–6

Xu R, Chen Y, Blasch E, Chen G (2018) A federated capability-based access control mechanism for internet of things (IoTs) 04:2018

Xu R, Chen Y, Blasch E, Chen G (2018) Blendcac: a blockchain-enabled decentralized capability-based access control for IoTs. In: 2018 IEEE International conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE Smart Data (SmartData), pp 1027–1034

Zhang G, Tian J (2010) An extended role based access control model for the Internet of Things. In: 2010 International conference on information, networking and automation (ICINA), vol 1, pp V1–319–V1–323

Zhao G, Si X, Wang J, Long X, Hu T (2011) A novel mutual authentication scheme for internet of things. In: Proceedings of 2011 International conference on modelling, identification and control, pp 563–566