Chapter 12
Access Control and Authentication in the Internet of Things Environment

Aditya Kaushal Ranjan and Gaurav Somani

12.1 Introduction

The scientific and business communities have realized the importance of IoT (Internet of Things) and its emergence in enhancing our day-to-day lifestyle. According to Gartner's forecast, there will be 20 billion devices connected to the IoT by 2020 [1]. Vast numbers of diverse devices from different vendors have already been connected towards achieving this target. The capabilities of these devices range from tiny measuring sensors to RFID mechanisms to traditional processing devices such as PCs and notebooks. The IoT application areas also vary from homes to hospitals, supply chain systems to industry automation, farming to electric grids, etc. It is important to address the concern of heterogeneity, scalability, energy efficiency (due to power and cost constraints of devices), integration and mining of enormous generated data (widely termed as Big Data), device configuration management, and most importantly the security (both at the logical level and physical level) and privacy.

Security of data and devices is one of the most significant concerns in the IoT. For example, security breaches and unwanted alterations in smart healthcare systems and faulty/irregular readings of health parameters of the patient could lead to unwanted or even fatal treatment. The whole credibility and deployability of the IoT solely depend on security aspects only. Authentication and access control are the first steps towards any security measures. With whom and up to what extent, one can access/communicate the devices in IoT scenario, are important aspects of security, especially when diverse devices with different capability have to perform collaborative tasks. The aim of this chapter is to introduce the reader with access

A.K. Ranjan (✉) • G. Somani
Department of Computer Science and Engineering, Central University of Rajasthan, Ajmer, India
e-mail: aditya.k.ranjan@ieee.org; gaurav@curaj.ac.in

Z. Mahmood (ed.), *Connectivity Frameworks for Smart Devices*,
Computer Communications and Networks, DOI 10.1007/978-3-319-33124-9_12

control granularities to abstract the various aspects, which are applicable to distributed environments. It is indeed important to differentiate the classical mobile computing literature from the modern IoT scenario. We will detail its present state of the art and future research direction in this chapter.

This chapter discusses the different architecture of IoT in Sect. 12.2, followed by Sect. 12.3 which describes the role of access control in connectivity of devices in both inter- and intra-domain. It is important to know how IoT paradigm is different from traditional ubiquitous computing. Therefore, Sect. 12.4 is devoted to it. Then we explore different issues and the current state of the art in Sect. 12.5. Section 12.6 outlines the various IoT aspects from distributed computing perspective. Access control and authentication in IoT have enormous scope for future research directions that are given in Sect. 12.7. We describe the guidelines for effective solutions in Sect. 12.8. The conclusions are presented in Sect. 12.9.

12.2 IoT Architecture from Security Perspective

For the sake of completeness, we would look at an abstract generic architecture for IoT. It would provide the reader a comprehensive as well as an abstract understanding between various components. In early days of IoT, numerous architectures have been proposed by the researchers and industry practitioners according to their specific needs. However, different federal agencies have also taken interest in this venture and presented numerous architecture such as IoT-A [2, 3, 6], SENSEI [5], and ETSI M2M [2, 4]. Additionally, a few allied architectures are also available, e.g., JCA-IoT [6], OGC [7], and IETF architectures. In this chapter, we attempt to provide an overview of some of these architectures for understanding the conceptual and actual elements. Readers are advised to refer to [2] for more details.

12.2.1 "IoT-A" Reference Architecture

IoT-A [2, 3, 6], the European Lighthouse Integrated Project, has addressed the Internet-of-Things Architecture for 3 years (2010–2013) and created an architectural reference model together with the definition of an initial set of essential building blocks. Collectively, these blocks are envisioned as foundations for developing the emerging IoT products.

For better understanding, this architecture can be divided into two parts: the first being a reference model and the second being the reference architecture, as briefly discussed below:

- The reference model consists of IoT domain model, functional model, and communication model. For the IoT domain model, three types of devices are necessary: sensors, actuator, and tags. UML is used to describe the domain

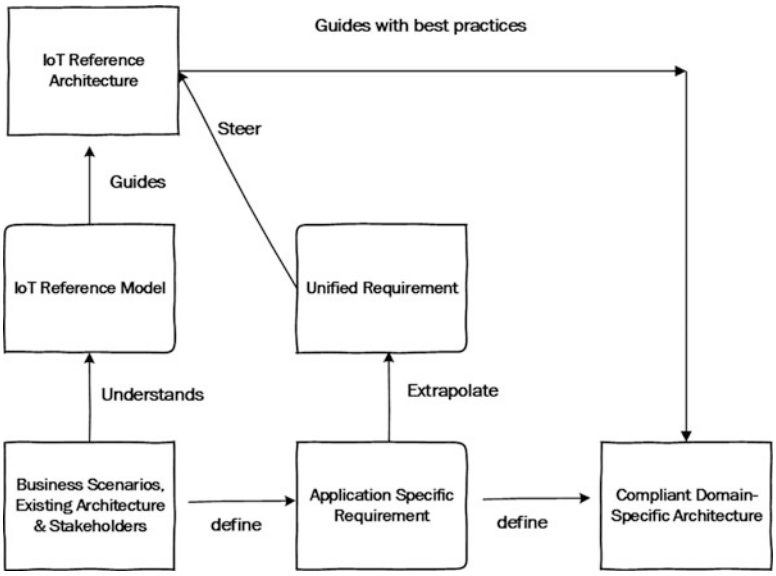

Fig. 12.1 IoT-reference model and IoT-reference architecture dependency and model influences

model. Services are classified into three types: resource-level services, virtual entity services, and integrated services. In functional model mainly functional groups are divided, which consist of all functionalities of the respective entities. Communication model includes identification of endpoint interactions, traffic patterns, etc.

- Reference architecture is the beginning of established concrete architecture and actual systems. For addressing the concerns of concrete architecture, it could be divided into three parts: functional view, information view, and deployment/operational view. Figure 12.1 shows the influence factors and dependency of the IoT-A. IoT-reference model guides IoT-reference architecture. All business scenarios, stakeholder's interests, and previous architecture have been addressed in IoT-reference model only. These factors also govern application-specific requirement; that is also useful to derive domain-specific architectures and unified requirement that is finally useful to guide IoT-reference architecture.

12.2.2 ETSI M2M Architecture

The European Telecommunications Standards Institute (ETSI) established a Technical Committee (TC) on machine-to-machine (M2M) topics for producing a set of standards for communication among machines in 2009 [4]. In Fig. 12.2, it can be seen that it is divided into two domains: gateway and device domain and network domain, as follows:

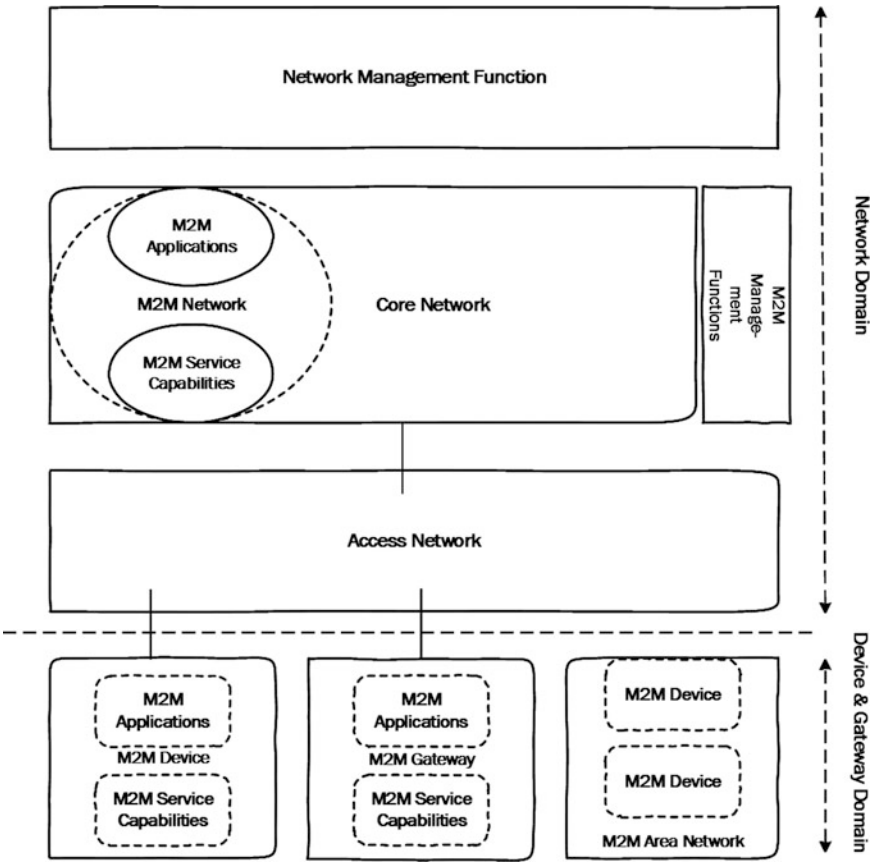

Fig. 12.2 ETSI M2M high-level architecture

- Generally, gateway and device domain is connected through Bluetooth, IPv6 low-energy LAN, etc., and network domain connectivity is done through a higher-level network that is enabled to provide internet connectivity like GSM, 3G, 4G, 5G, etc. So this high-level architecture consists of both functional and topological view. It is more connection oriented in approach. However, we can also clearly see its topological aspects. Gateway is the main "connecting" entity between network and device domains. The topological view is associated with the physical elements like M2M devices and gateways.
- The network domain consists of access network, Core network, M2M service capabilities, M2M application, network management functions, and M2M management functions. A separate classification of service capabilities and resource management also exists with respect to this architecture [2].

12.2.3 SENSEI

The approach of SENSEI was to develop architectural and technological building block to enable integration of real world to the future Internet. The architecture includes real-world service interface plus wireless sensor and actuator network on the Internet at a global level. It is based on the separation of sensing actuating from real-world devices. The assumption for addressing mechanism is IP based [2, 5]. In Fig. 12.3, we note that it is divided into many domains connected through several interfaces, e.g., service interface, network support interface, and PnP interface. It is much more function oriented in its approach.

12.2.4 Open Geospatial Consortium Architecture

The Open Geospatial Consortium (OGC 2013) is an international industry consortium of a few hundred companies, government agencies, and universities that develop publicly available standards [7]. These standards provide geographical information support to the Web, wireless, and location-based services.

OGC developed many standards in the due course of time, which includes sensor Web enablement model (OGC SWE) that develops standards for sensor system models like Sense ML, sensor information model, and sensor services that follow

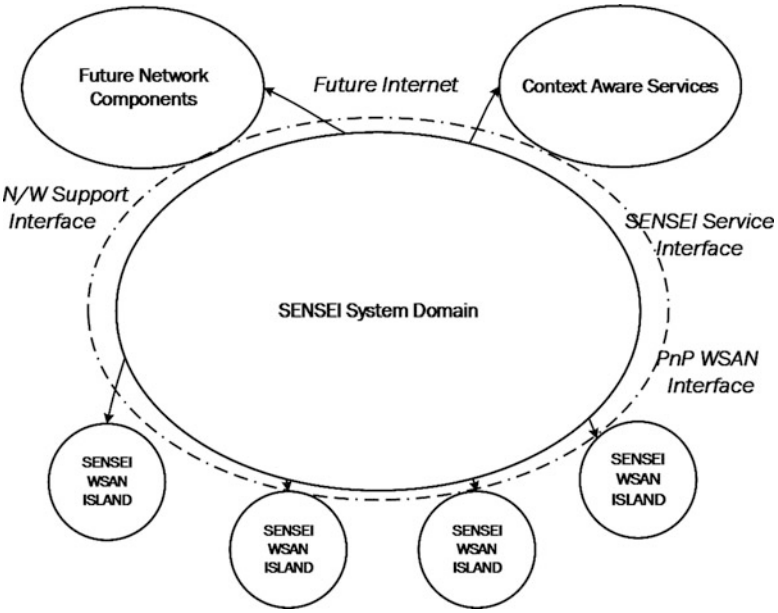

Fig. 12.3 SENSEI architecture

service-oriented architecture. OGC SWE is more information centric than communication centric, similar to ETSI M2M [2].

12.2.5 Comparison Between Different IoT Architectures

IoT-A describes the essential building blocks and identifies design requirements. It also provides guidelines to build architecture for a specific domain and is generic in nature. However, its emphasis is much less on topological part of the architecture. It is first of its kind for integrating all issues of IoT together. However, its generic nature is also a drawback to some extent, when there is a need to focus on a specific problem of certain IoT domain.

ETSI M2M is too specific in nature. It deals with a topological approach of IoT. It has provided a higher-level architecture, which addresses most connectivity needs of M2M paradigms. It lacks generality and cannot address building blocks and design requirements like IoT-A.

SENSEI and OGC are subsidiary architectures that concentrate on sensor issues that are helpful to realize IoT. It helps to understand primary architecture like ETSI M2M, IoT-A, etc. but lacks generality and broadness aspects of IoT architecture.

12.3 Access Control in Connectivity of Devices

To understand the significance of access control in connectivity of the device in the IoT scenario, let us take an example of a smart city. The building elements/domains behind "smart" city are smart home, smart sewerages, smart vehicle networks, smart water supply, smart hospital, smart traffic management, smart grids, electricity supply, etc. For better understanding, the connectivity of devices can be seen in two domains: intra-domain connectivity and inter-domain connectivity.

12.3.1 Intra-domain Connectivity

In this section, we discuss connectivity issues in intra-domain communications while considering the buildings of the smart city. Basically, intra-domain connectivity can be done in several ways. For centralized system architecture, individual nodes could establish mutual trust or with the help of a gateway. Authentication and access control are the foremost requirements of trust establishment. Mutual authentication and application-level access control can be easily configured in this scenario. Several states of the art techniques are there for mutual authentication in IoT scenario [53]. For access control at the application level, we have given the present situation as shown in Table 12.1. However, for distributed architecture, the scenario

Table 12.1 Present state of the art in layerwise approach

Attribute and role-based access control, capability-based access control, authentication based on OAuth, admittance control algorithm, Kerberos and RADIUS-based access control, access Control in Contiki OS, user identity-based mechanism, aggregated proof-based hierarchical authentication mechanism, lightweight authentication based on IoT-A, zero-knowledge proof-based solutions, group authentication based on identity-based encryption	Application layer
Device identity-based mechanism, DTLS-based mechanism, OAuth based, delegated authentication, aggregated proof-based hierarchical authentication mechanism, conditional privacy preserving with access linkability with roaming service, authentication based on LISP, EAP-TLS-based authentication based, ECC-based authentication solutions, ECC-based authentication for M2M systems	Transportation layer
EAC framework for authentication, all authentication scheme of RFIDs, two-phase authentication for WSNs	Perception layer

becomes slightly different as every device is capable of handling and processing the data itself through the vision of edge intelligence and collaboration. In that case, P2P-based distributed architecture [53] is helpful in that it brings all P2P-based mechanisms of authentication and access control into the picture. The delegation-based decision-making authority for decentralized-based architecture is also a possibility; as in this case, centralized access control mechanism will also be applied. However, in distributed architecture, heterogeneity will become a major issue. Scalability of such mechanism becomes an issue, as access control and authentication mechanism should be capable of handling millions of devices efficiently.

Figure 12.4 shows the abstract view of N to N communication scenario among building blocks/domains of a typical smart city. Bidirectional long arrows show the inter-domain communication between the different constituent domains, though short arrow depicts the intra-domain connectivity. If we evaluate this figure from distributed IoT point of view, then we find that intra-domain connectivity governs with collaborative paradigms and inter-domain connectivity governs with edge intelligence principle generally. That is why the communication takes place between inter-domain controllers, and intra-domain controller/gateway are achieved through P2P-based or delegation-based architecture as stated above. However, this figure can also be seen from the perspective of centralized architecture, where all connectivity is done through gateway/controller only.

12.3.2 Inter-domain Connectivity

Logically, connectivity issues of inter-domain remain the same as intra-domain issues; however, physically, they will be more diversified in connections. All present mechanisms of access control that is applicable to intra-domain at perception layer require major changes in inter-domain to fit on different kinds of

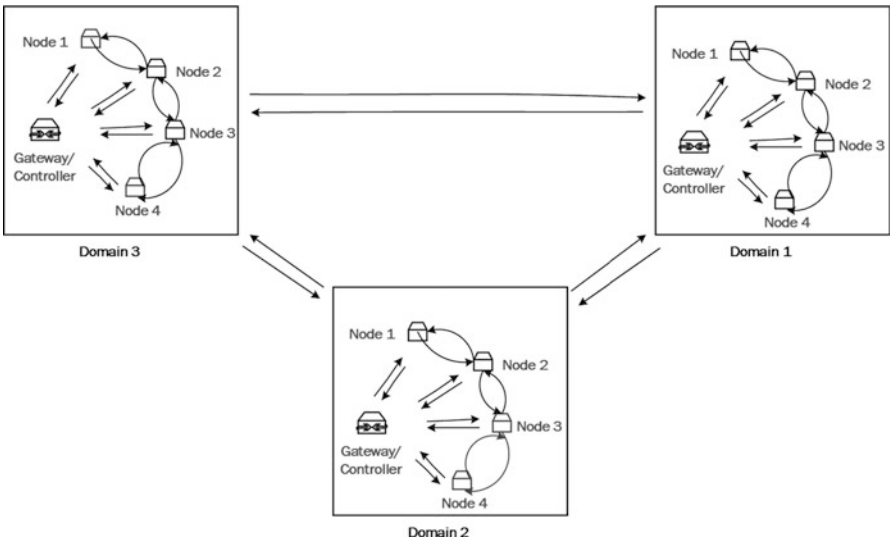

Fig. 12.4 Abstract view of N to N communication scenario in distributed IoT

networks. In distributed IoT scenario, interaction could be dynamic, i.e., entities might not know/trust each other in advance, that is also one of the key challenges for authentication and access control mechanism in inter-domain communications. We frequently find dynamic N to N scenarios (refer to Fig. 12.4), where data providers are active entities and regularly require feedback from receiving entities [53]. Due to edge intelligence and collaboration principle, any node starts communicating to service provider's nodes directly, which requires that access control and authentication mechanisms must be presented to work at both local and global networks (in intra- and inter-domain).

12.4 IoT Security vs Traditional Ubiquitous Security

Ubiquitous computing is also termed as "everywhere, anywhere" computing, referring to embedding the capability of computing to everyday objects [2]. This vision of computing is realized by the sensors to RFID tags to handheld devices to wearable devices. The M2M systems, WSNs, and RFID tag networks are popular paradigms to realize this. However, M2M systems are meant for specific tasks while IoT devices are more generic and diverse in nature. Let us take one instance of body area network (BAN), which observes and computes several health parameters in a ubiquitous way. BANs usually send health readings to nearby hospital servers which process the data to suggest various outcomes to the medical

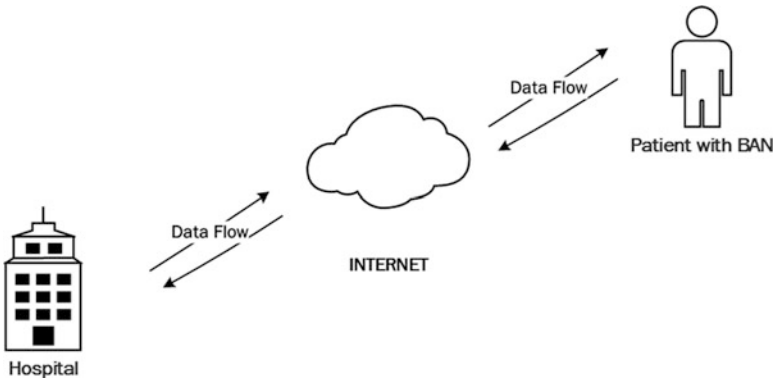

Fig. 12.5 Connectivity scenario of the healthcare IoT

practitioners. This also become part of quick decision-making based on history and machine learning techniques. Consequently, the medical prescription may be suggested by medical practitioners. Taking readings through BAN is a point-specific approach, while communicating with data processing server (hospitals in this case) involves the role of IoT (refer to Fig. 12.5).

Connecting the BAN with hospital and processing the data according to context-based requirements are possible due to Web services. Therefore, security concern applies to multiple layers in the case of IoT. It not only includes the security concern at local level but also the security concern of the Internet, different devices configuration issues, the privacy of generated and computed data, and so on. This makes the concerns more diverse in nature comparable to traditional ubiquitous computing.

In another example, we can take a typical IoT scenario where through a gateway, every device domain and external network domain is connected. Similar security concerns are applicable here also (Fig. 12.6).

Let us now discuss security of IoT in different layers. In all contemporary contributions, security issues can be divided into three layers of IoT, viz., perception/physical, transportation, and application layer [11]. We discuss these issues in the following subsections.

12.4.1 Security Issues at Physical/Perception Layer

Basically, security issues of RFID tags and WSNs come into the picture, such as RFID tag's uniform coding [8], conflict collision, cryptographic algorithms, trust management [9], key management [10], heterogeneous integration and secure routing protocols in WSN, etc. [11]. Privacy protection can be solved by hardware-based schemes [12], password-based schemes, other trade-off-based solutions, etc. For trust management, security protocol, digital signature, etc. are

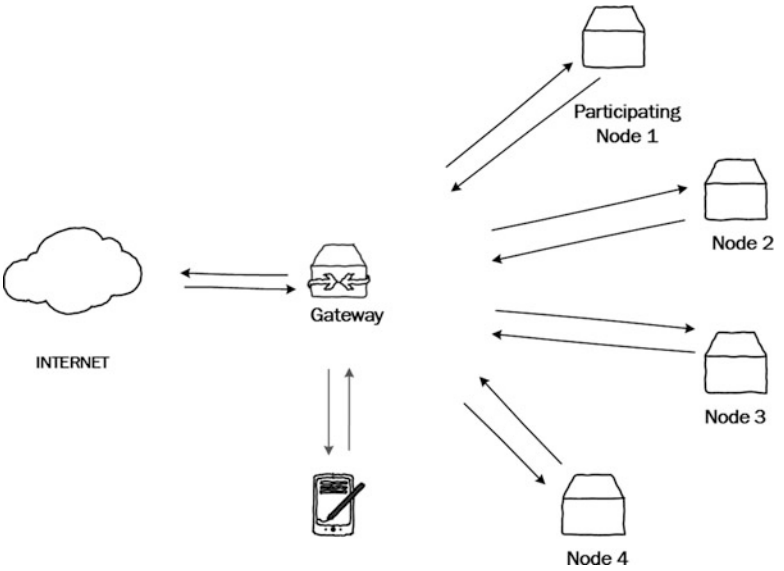

Fig. 12.6 Typical connectivity of the home IoT scenario

beneficial. Symmetric key cryptography is mostly used in RFIDs due to their confidentiality and low computation cost. Different access control and access information format data processing methods are also integrated through heterogeneous technologies which are the core part of IoT.

12.4.2 Security Issues at Transportation Layer

At the transportation layer, phishing attacks, DDoS (distributed Denial of Services) attacks, secure routing issues, data security, information disclosure through creating fake login page or through injecting malicious script on target machine (known as phishing and scripting attack), and network paralysis could happen in various IoT scenarios. For mitigation of all these security issues, attack detection and prevention technologies are used. Access control and network encryption are also helpful for these scenarios [11].

12.4.3 Security Issues at Application Layer

At this layer, DDoS attacks, access control problem, service interruption, illegal intervention, etc. are the main issues that can be solved through middleware, attack detection, and prevention technologies. The information development platform can also prove helpful [11]. In the case of security issues of ubiquitous computing, we

take M2M paradigms as an example. We present here the layerwise security issues and their solutions [13].

12.4.3.1 Security Issues at Physical Layer

These attacks may be classified into active and passive attacks. Passive attacks involve traffic analysis and eavesdropping of wireless communications, while active attacks are more disruptive and may involve jamming and scrambling [14]. Increasing the power levels and employing techniques like spread spectrum, which have direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS), are the techniques useful to defend jamming, eavesdropping, and traffic analysis attacks [15].

12.4.3.2 Security Issues at Medium Access Control Layer

Modification of MAC layer management, identity theft of appliances, data message modification, and Denial of Services attack could happen in this layer. Classic countermeasures of these attacks involve cryptographic mechanisms for encryption and authentication of participating entities. Cryptographic mechanisms are based on the public key and a symmetric key mechanism like ECC, X-509 mechanisms.

12.4.3.3 Security Issues at Network and Adaption Layer

Interoperability between two communication domains is a major issue. Designing of compressed security headers is an important issue. Some issues are key management and management of security association.

12.4.3.4 Security Issues at Transport Layer

Energy-efficient transport layer mechanisms include congestion control and reliability with minimal overhead and retransmissions. Several mechanisms currently exist like reliable message delivery, congestion control, and energy efficiency. The existing mechanisms are Distributed TCP Caching (DTCP) [16], Sensor Transmission Control Protocol (STCP) [17], Adjustable Parallel TCP [18], and Pump Slowly Fetch Quickly (PSFQ) [19].

12.4.3.5 Security Issues at Application Layer

The main technology currently emerging is Constrained Application Protocol (CoAP) [20], which is an alternative to HTTP and is common in traditional

computing systems. For security concern, CoAP uses DTLS for secure communications. For sensing application, ECC-based public key cryptography is used by CoAP.

12.4.4 Summary

After going through the security issues of IoT and M2M systems (as ubiquitous computing systems) separately, we can conclude that some security issues and its solutions overlap in both the environments. However, some issues are specific to IoT scenarios only like scripting and phishing attacks, etc. (described previously in Sect. 12.4.2). Therefore, IoT security issues are somewhat different from traditional computing environments. It involves some issues of traditional Internet as well ubiquitous computing; therefore, it is an important challenge to address these security issues in constrained device scenario.

12.5 Issues of Access Control and Authentication in IoT

The diversity of the devices and networks leads to the aggregation of several services and data from different sources and contexts. Each service and data providers have their own access control policies and authentication methods. Uniform privacy policy languages to express the different types of context, different types of data owner, and different types of request subjects needs to represent high-level aggregating requests and needs to change to the policies [21]. While designing and planning access policies, device resource (computing and storage) needs should be taken into account [22]. It is difficult to design access policies for resource-constrained devices where storage and processing are the main constraints. Location and enforcement points are the main factors, which needs to be considered while designing the efficient access policies. However, few advances have taken place in the area of managing access policies. Traditional methods like ACLs (access control lists), RBAC (role-based access control lists), etc. are there, but still, there is a need to implement some specific approaches which are feasible and consistent to IoT.

In order to see the present state of the art in access control, we classify various contributions in the following categories.

12.5.1 Modification/Improvisation of Existing Access Control Methods

Many efforts have been taking place to apply traditional methods of access control to IoT scenarios. Sun et al. [22] have evaluated ABAC (attribute-based access control) and RBAC (role-based access control) and found that RBAC cannot satisfy

large-scale dynamic users but ABAC can satisfy dynamic problem; however, working mechanism is difficult. In order to cope with this problem, authors [22] have proposed ARBAC (attribute- and role-based access control) that has an advantage of both schemes. They presented the architecture and have shown the correspondence between attribute expressions and role with definitions of three relationships. They have also done a conflict detection and policy optimization. The advantages of proposed work on managing permissions, viz., modifying, adding, and deleting, are also mentioned. Real-time implementation and empirical data are missing to support the claims.

Another work that comes under this classification is by Mahalle et al. [23]. They have proposed the capability-based access control methods. They have suggested separate data structures with device id and access rights. Therefore, if any subject possesses the capability match with capability stored in the device, then access is granted.

One classical example of access control in IoT is presented in [24]. They used RBAC as a base access control techniques. They used thing's role and application in a particular network as a basis for access control, where extended RBAC has been used and named as context-based access control. Here access has been granted, based on a set of contextual information collected from environments of the system and user.

Fremantle [26] explored the use of OAuth for IoT systems that use MQTT 1.1 protocol. After implementations, they have concluded that both IoT and non-IoT clients can use OAuth tokens. It is also concluded that in IoT client secret security is much harder unlikely all Web application are deployed in a single phase.

Another work presented in [27] has used modified DTLS authentication to control access at the device level (physical/perception layer) where all resources hosted on the resource server are available to any client that has a right to connect.

The abovementioned works are a few recent reports and works on access control methods that use modifications or extensions of existing systems/mechanisms. They succeeded to show that existing mechanisms are also compatible with an IoT scenario with some modifications.

12.5.2 New Approaches to Access Control Mechanisms in IoT

Liu [28] has defined a new admittance control algorithm, where new connection is adapted and a service call is launched in the current community when a user switches their current community. However, this algorithm follows the RBAC approach.

Pereira et al. [29] have combined the concept of Kerberos and RADIUS and implemented the mechanism on CoAP. They have successfully achieved their goals of access control in constrained devices. One more work on access control [30] that

implements the access control mechanism in "Contiki OS" ensures that apps only use specified APIs and do not have arbitrary memory access. They proposed a mechanism from which apps can work only on specified memory location. Therefore, they cannot access the details of OS. They have used a third data structure called "permissions" for storing information, regarding access control. They have also introduced new APIs, which has many "get" functions especially for nonuser interactive functions which do not use inter-process communications.

Thuan [31] has proposed a user-centric identity management framework that consists of users, devices, service provider, and identity providers. They have also discussed udevID (universal device identity). Banerjee et al. [32] have proposed channel access control through novel zero-exposure slot allocation in which packet transmission timing is used to detect a collision, also for collision resolution and for scheduling.

12.5.3 Present State of the Art and Issues in Authentication

Identity management is an important requirement for heterogeneity, without which successful realization of IoT is not possible. With this scenario, authentication is the most important aspect of identity management. There is a need to realize authentication in several layers. For privacy protection, password-based schemes are popular through the implementation of hash locks, random hash lock, hash chain, etc. for RFIDs and WSNs at physical layer [13]. Users, devices, and network authentication at application and transportation layers all come under access control. We can see the relevant solutions in Table 12.2.

In the case of authentication, we can see two types of schemes: certificate based and non-certificate based. Certificate-based solutions try to implement existing Internet standards like DTLS, DEX, minimal IKEv2, etc. [33, 34]. Let us see the present state of the art in authentication for IoT scenarios.

Mahalle et al. [23] proposed an authentication scheme based on the Diffie-Hellman algorithm for the secret key generation. The mechanism requires one or more KDC (key distribution center) to generate domain parameters. After this, they proposed a protocol for identity establishment for one-way and two-way authentication.

Liu et al. [24] have proposed authentication mechanism by using simple and secure key establishment method based on ECC. They have used federated identity management through home registration authority. They also proposed a framework for entity authentication, action authentication, and claim authentication and have done a formal analysis of these through CSP approach. They have shown that those mechanisms satisfied many requirements of IoT.

Hummen [33] proposed a delegation-based architecture for the expensive handshake of DTLS for constrained devices. They have presented empirical data for the entire process. The delegation server they presented establishes a connection on

Table 12.2 Summary of the present state of the art

Works	Base techniques	Real-time implementation	Security analysis
Sun et al. [22]	ARBAC+RBAC	No	No
Mahalle et al. [23]	Capability-based access control	Yes	No
Liu et al. [24] and Zhang et al. [25]	RBAC based, context based	No, No	No, No
Fremantle et al. [26]	OAuth	Yes	Yes
Sitenkov et al. [27]	DTLS based	Yes	Yes
Liu et al. [28]	EAC based	No	Yes
Pereira et al. [29]	SoA (service-oriented architecture) based	No	Yes
Mituca et al. [30]	MDSE (model-driven software engg.)	No	No
Thuan et al. [31]	Token based	No	No
Banerjee et al. [32]	Zero-exposure slot allocation	Yes	Yes
Hummen et al. [33]	DTLS	Yes	No
Gerdes et al. [34]	CoAP + DTLS	No	No
Ning et al. [35]	Aggregated proof based	No	Yes
Hernandez-Ramos et al. [36]	SEAPOL + EAP + RADIUS	Yes	No
Lai et al. [37]	Bilinear map + hybrid linear combination encryption	Yes	Yes
Jan et al. [38]	Challenge response based	Yes	No
Raheem et al. [39]	LISP based	No	Yes
Pawlowski et al. [40]	EAP-TEPANOM based	Yes	No
Druml et al. [41]	ECC based	Yes	No
Schukat et al. [42]	Zero-knowledge proofs	Yes	No
Flood et al. [43]	Zero-knowledge proofs	Yes	No
Porambage et al. [44]	Implicit certificate based	Yes	No
Yao et al. [45]	Nyberg's fast one-way accumulator	No	Yes
Kothmayr et al. [46]	DTLS	Yes	No
Lee et al. [47]	XOR based	Yes	No
Mahalle et al. [48]	TGCA	Yes	Yes
Adiga et al. [49]	Identity-based encryption	Yes	No

behalf of constrained devices. The authors presented empirical data to show DTLS overheads on constrained devices.

Similar work has also been proposed by Gerdes et al. [34] by suggesting the protocols for delegating the client authentication and authorization in constrained devices that are based on symmetric key cryptography. These protocols rely on DTLS for data transfer. They have systematically pointed out the clear cut objectives and defined authorization- and authentication-related tasks.

Ning et al. [35] proposed aggregated proof-based hierarchical authentication scheme based on U2IoT architecture. The main features of the work include the

establishment of aggregated proofs for multiple targets to achieve backward and forward anonymous data transmission. However, this mechanism lacks generality and works only for layered networks, although exhaustive proofs have been given for the protocol for a unit and ubiquitous IoT.

The work of Hernandez-Ramos [36] was part of IETF Authentication and Authorization for Constrained Environment (ACE). In their studies, they presented a lightweight version of Extensible Authentication Protocol over LAN (EAPOL) by integrating a standard mechanism for bootstrapping processes like EAP and RADIUS.

Lai et al. [37] used group signature schemes for an anonymous user linking function by presenting a mechanism of conditional preserving authentication with access linkability. It hides the real identity of the user and enables the authorized entity to link all access users' information without knowing the real identity of the user. Jan et al. [38] have proposed a mutual authentication mechanism without any device participation in communication. It facilitates less computation and communication overhead. Raheem et al. [39] have proposed a new authentication and key exchange scheme that is based on a locator/ID separation protocol routing architecture. They verified their scheme through AVISPA tool. They have claimed that there are no security flaws in their scheme.

Pawlowski [40] intermixed IEEE 802.15.4 authentication framework and TEPANOM (Trust extension protocol for authentication of newly deployed objects and sensor through the manufacturer). They showed that there is 42 % reduction in a message exchange and 32 % in transferred data. Druml et al. [41] presented ECC-based authentication scheme that shifted the computational intense part to authentication terminal from constraint device.

Schukat et al. [42] presented an authentication protocol for static M2M networks through zero-knowledge proofs. They have also evaluated several previously proposed zero-knowledge proofs. They claimed that their mechanism is suitable for resource-constrained devices. The work of Flood et al. [43] is also similar to Schukat et al.'s work. The work is an extension of previous works only.

Work reported by Porambage et al. [44] is based on traditional certificate-based methods that allow end user and sensor nodes to authenticate through implicit certificates. To prove the compatibility of their work, they have also shown the empirical data for memory utilization. The work of Yao et al. [45] is the modification of Nyberg's fast one-way accumulator as compatible to multicast with simpler computation. They have also evaluated the seven factors of the performance aspects of the proposed work. The work of Kothmayr et al. [46] is first to implement the DTLS in IoT scenario. Therefore, all strengths of DTLS in traditional computing are also valid here.

Lee et al. [48] proposed a lightweight authentication mechanism for RFID tags based on XOR manipulation. The work of Mahalle et al. [48] is meant for authentication of the devices in group communication through TCGA (Threshold Cryptography-based Group Authentication). They have shown the time analysis (by calculating asymptotic time complexity) and formal security analysis of the proposed scheme. Work reported by Adiga et al. [49] has implemented identity-

based cryptography in secure M2M communications for an IoT scenario. They have shown the solution of many issues related to M2M scenario.

Some other lightweight ECC-based schemes have also been proposed, e.g., [50–52], mainly for RFIDs.

12.5.4 Issues in the Present State of the Art

Let us look at the issues inherent in the present state of the art to help us find the research problems and future directions for further development in this field. A summary of the following studies is provided in Table 12.2.

The work of Liu et al. [28], Mahalle [23], and Druml [41] revolves around the ECC-based key exchange. However it is a well-proven and widely accepted mechanism, but it lacks specification for IoT. The work of Pereira et al. [29] is based on service-oriented architecture and uses the concept of Kerberos and RADIUS for access control and authentication. Again they use this popular mechanism and tried to make it compatible in IoT scenario somehow. Sun et al. [22] present a novel contribution in their approach by mixing the concept of ABAC and RBAC and developed as ARBHAC (attribute- and role-based hybrid access control). Its real-time implementation and empirical data are not there to support the claims.

Mituca [30] has presented a novel approach to implementing access control in "Contiki OS," but the real-time implementation is needed. Contributions of Hummen et al. [33] and Gerdes et al. [34] are solely dependent on DTLS mechanism. Conceptually, both works are quite similar in their approach. Both works have proposed delegation servers to perform computation intense tasks. Work reported by Thuan [31] concentrates on user-centric identity management. The way of approach in the paper is innovative, but again real-time implementation is not there to prove it. The work of Fremantle et al. [26] is based on OAuth. They developed a prototype to use in OAuth for access control. They implemented it and drew some fruitful conclusions. The work of Ning [35] is specifically concentrated on U2IoT. They presented authentication scheme for aggregated networks. That is why it lacks generality. The work of Pawlowski et al. [40] is meant for authentication in IoT by mixing the concept of TEPANOM and EAPs. Hummen et al. [33] have conducted a certificate-based authentication feasibility study in IoT scenario. This work is a preliminary of their one of the quoted work. Hernandez-Ramos et al. [36] have proposed a lightweight authentication and authorization protocol based on ARM architecture.

Work reported by Lai [37] is the conditional privacy-preserving authentication with access linkability. They talked about the access control while in roaming. The paper has provided detailed mathematical proofs and security analysis but lacks real-time empirical data.

Jan et al. [38] have proposed a lightweight authentication scheme with the application of AES (Advanced Encryption Standard) with a challenge-response

mechanism. The proposed work also presented experimental data to firm its claim regarding feasibility in IoT scenario. Raheem [39] also proposed an authentication scheme using LISP, which just started emerging. They have also done a security analysis to firm its claims, but real-time implementations are not there. Schukat et al. [42] and its subset work of Flood [43] proposed authentication with zero-knowledge proofs. They have shown key exchange using graph methods.

The work of Porambage et al. [44] seems to be complete regarding theoretical and experimental aspects. They have specifically evaluated their protocol in terms of memory utilization, time, and energy consumption. The only drawback is that it depends on age-old authentication mechanism of certificates.

Work reported by Yao [45] seems promising at first sight. The scheme is novel, but its performance comparison with existing work is missing. The strength of this work is the main drawback of the work of Kothmayr et al. as all the drawback of certificate-based mechanism lies here.

The work of Lee et al. [47] is focused on RFID; therefore, it must experiment for other IoT devices and scenarios. The work of Mahalle [48] is novel, but it would be interesting to see a real-time application of it. Thorough security analysis of the work of Adiga et al. [49] is missing.

We can conclude that many schemes that are proposed in recent times lack real-time implementations. However, a few schemes have very strong fundamental claims like Schukat [42], Raheem [39], Lai et al. [37], Hernandez-Ramos et al. [36], Pawlowski [40], Ning et al. [35], Thuan [31], Mituca et al. [30], and Sun et al. [22], but real-time application of these is still missing. Some other research and developments are very specific to certain networks and for certain architectures that limit their applicability and feasibility. Although they have shown successfully that their work is fully robust to different attacks, there is a need to analyze their claims and verify further their results.

12.6 Access Control in the Perspective of Distributed Computing

As we have already discussed above, many access control/authentication works are suitable for certain networks or particular architectures only. For distributed and heterogeneous environments like IoT, there is a need for access control mechanism that caters interoperability issues efficiently. Scalability is also an important issue in distributed environment. So, to design and implement effective access control mechanism, we must consider also the scalability and heterogeneity issues very carefully and efficiently.

12.7 Research Direction in Access Control and Authentication for IoT

There is a vast scope for further research in authentication and access control in the IoT. Below, we summarize points regarding various research directions in IoT on access control and authentication:

- There is a lack of well-established access control architecture like AAA (authentication, authorization, and accounting) in IoT scenarios for M2M systems.
- Most of the existing work on access control is based on the traditional mechanism like ACLs, RBACs, etc., but there is a need to develop some access control paradigms specifically for resource-constrained environments.
- As we have pointed out in the previous section, there are very few access control management systems in constrained OSs like Contiki, contradicts with the high-end OSs like Android, etc. Hence, an initiative to develop access control management for constrained environment is needed much like traditional computing environment.
- Interoperability issues of access control mechanism of heterogeneous networks/devices in IoT scenarios are needed to be addressed.
- In existing work of authentication in IoT, a scenario can be classified into two types: certificate based and non-certificate based. Mostly certificate-based solution revolves around modified DTLS [46], etc. for IoT. There is a need to explore other certificate-based authentication mechanism for the IoT scenarios.
- In recent times, many interesting non-certificate-based authentication mechanism has been proposed. But still there are other authentication mechanisms for traditional computing environment that needs to be tested/implemented in IoT like anonymous authentication.
- There is a lack of a proper framework for user authentication in IoT environment. Usability and reliability aspects of user authentication are needed to be addressed.
- It has been observed during the state of the art surveys that a cross-validity of the present work is not there. So thorough security analysis and performance analysis are needed, so one can cross-validate the claims and make further improvements.
- Several security issues in IoT and relating paradigms remain unanswered. So, it will be better to propose some novel mechanisms to defend these.

12.8 Guidelines for Effective Solutions

It is observed in the present state of the art (as mentioned above) that there could be many access control and authentication solutions at different layers (as shown in Table 12.1). In the table, we have included best solutions for each layer from the

present state of the art. It will help us to know what is already available and what needs to be done. All security solutions of RFIDs and WSN lie on the perception layer [7]. Therefore, we have included these solutions in perception layer only. Present solutions are mainly of generic nature; that is why most of the solutions lie in the application and network layers; however, if we see the work of WSN and RFIDs separately, then we can find that most works are at perception layer. All access control solutions must address scalability and complexity. Likewise the contribution of Sun et al. [22], RBAC, is not meant for dynamic users (scalability) and ABAC is complex in operations, so authors proposed ARBAC. The following are the directions and guidelines for designing effective solutions:

- Apart from complexity and scalability, heterogeneity and energy issues are also important. However, computational complexity and energy consumption are somewhat related, but these issues can be evaluated separately.
- Many researchers, e.g., [29, 30, 46] choose to propose access control and authentication solutions by making them compatible with widely accepted and implemented solutions of traditional computing systems in IoT scenario. We have seen many of these in the present state of the art.
- The foremost concern of authentication is scalability; therefore, the mechanisms must satisfy authentication operations of as many nodes as possible.
- However, standalone authentication solutions are suggested to be discouraged because of constrained resource issues. In many cases, devices cannot afford to engage all resources for authentication only. Therefore, it is better to propose complete access management frameworks [24].
- Authentication solutions should be simple and lightweight from the computation point of view, which will address the energy issues and computational resource issues effectively.
- The solution of access control and authentication must be dealt with for intra- and inter-domain connectivity and its interoperability and granularity. It is the most ignored part of the present state of the art.

12.9 Conclusion

In this chapter, we have comprehensively discussed scenarios of access control and authentication concerning the present state of the art and research community's progress. We started with the detailed differentiation of security issues in IoT and traditional ubiquitous computing. We have also evaluated present architectures to get familiar with actual and conceptual building block of IoT. In the present state of the art, we have pointed out certain significant contributions, their merits, and drawbacks and conducted a comparative study. Our goal has been to point certain important future directions for access control and authentication.

In Sect. 12.8, we have mentioned contemporary studies conducted at each layer, to frame the guidelines for future work. The chapter also explains the access control

from the view of distributed computing to show how one should think about access control mechanisms for distributed computing environments.

References

1. Gartner (2015), Gartner Says a thirty-fold increase in internet-connected physical devices by 2020 will significantly alter how the supply chain operates. http://www.gartner.com/newsroom/id/2688717. Accessed 12 June 2015
2. Holler J, Tsiatsis V, Mulligan C, et al (2014) From machine to machine to internet of things. Academic press, Elsevier, Oxford, UK
3. IoT (2015) IoT-ARM white paper. www.iot-a.eu. Accessed 12 June 2015
4. ETSI (2015) ETSI technical specification v 2.1.1. http://www.etsi.org. Accessed 17 June 2015
5. SENSEI (2015) SENSEI white papers. http://www.sensei-project.eu. Accessed 12 June 2015
6. ITU (2015) ITU Joint Coordination Activity on Internet of Things (JCA-IoT) white papers. www.itu.int. Accessed 12 June 2015
7. Open Geospatial Consortium (20115) Open geospatial consortium architecture. www.opengeospatial.org/pub/www/saa/saa_architecture.html. Accessed 17 June 2015
8. RFID (2015) RFIDs uniform coding. http://www.epc-rfid.info/tbd-1. Accessed 15 June 2015
9. Matt B, Joan F, John I, Angelos DK (2015) Trust management. http://www.cs.yale.edu/~jf/BFIK-SIP.pdf. Accessed 15 June 2015
10. Thales, (2015), Key management. https://www.thales-esecurity.com/solutions/by-technology-focus/key-management. Accessed 12 June 2015
11. Jing Q, Athanasios V et al (2014) Security of the internet of things: perspective and challenges. Wirel Netw 20(8):2481–2501, Springer US
12. Thales (2015) Hardware based scheme. https://www.thales-esecurity.com/products-and-services/products-and-services/hardware-security-modules. Accessed 12 June 2015
13. Granjal J, Monteiro E, De Silva J (2013) Security issues and wireless M2M systems, Wireless Networks and Security. Springer, Heidelberg, pp 133–164
14. Trung N (2015) A survey of WiMAX security threats project report. http://www.cse.wustl.edu/~jain/cse571-09/ftp/wimax2/. Accessed 17 June 2015
15. Stephen N (2015) Traffic analysis. http://www.sans.edu/research/security-laboratory/article/traffic-analysis. Accessed 12 June 2015
16. Dunkels A, Alonso J, Voigt T and Ritter H (2004) Distributed TCP caching for wireless sensor networks. Proceedings of 2004 modeling and optimization in mobile, Ad Hoc and wireless Networks, Cambridge, UK
17. Iyer YG, Gandham S, Venkatesan S (2005) STCP: a generic transport layer protocol for wireless sensor networks. Proceedings of 14th International Conference ICCCN 2005, pp 449–454
18. Yusung K, Kilnam C, Lisong XU (2008) Adjusting the aggregate throughput of parallel TCP flows without central coordination. IEICE Trans Commun 5:1615–1618, E91-B
19. Wan CY, Campbell AT, Krishnamurthy L (2005) Pump-slowly, fetch-quickly (PSFQ): a reliable transport protocol for sensor networks. IEEE J Sel Areas Commun 23(4):862–872
20. Shelby Z, Hartke K, Bormann C (2014) The Constrained Application Protocol (CoAP), request for comments: 7252. Internet Engineering Task Force (IETF)
21. Stankovic JA (2014) Research directions for the internet of things. IEEE J Internet Things 1 (1):3–9
22. Sun K, Yin L (2014) Attribute-role-based hybrid access control in the internet of things. In: Proceedings of workshop on APWeb 2014. Changsha, China, Springer LNCS 8710, pp 333–343

23. Mahalle PN, Anggorojati B et al (2014) Identity establishment and capability Based access control scheme for internet of things. In: Proceedings of 2009 12th international symposium on Wireless Personal Multimedia Communications (WPMC), Sendai, Japan, pp 187–191
24. Liu J, Xiao Y, Philip CL (2012) Authentication and access control in the internet of things. In: Proceedings of 2012 32nd International conference on distributed computing systems workshops, Macau, China, pp 588–592
25. Zhang G, Tian J (2010) An extended role based access control model for the internet of things. In: Proceedings of 2010 International Conference on Information, Networking and Automation (ICINA), Kunming, China, vol 1, pp 319–323
26. Fremantle P, Aziz B et al. (2014) Federated identity and access management for the internet of things. In: Proceedings of 2014 I.E. international workshop on secure internet of things, Wroclaw, Poland, pp 10–17
27. Sitenkov D (2014) Access control in the internet of things. Master's thesis; SICS
28. Liu L, Yin L et al (2014) EAC: a framework of authentication property for the IoTs. In: Proceedings of 2014 international conference on cyber-enabled distributed computing and knowledge discovery, Shanghai, China, pp 102–105
29. Pereira PP, Eliasson J, Delsing J (2014) An authentication and access control framework for CoAP-based internet of things. Proc 40th 2014 IECON, Dallas, US, pp 5293–5299
30. Mituca A, Moin HA, Prehofer C (2014) Access control for apps running on constrained devices in the internet of things. In: Proceedings of 2014 international workshop on secure internet of things, pp 1–9
31. Thuan DV, Butkus P, Thanh DV (2014) A user centric identity management for internet of things. In: Proceedings of 2014 international conference on IT convergence and security, pp 1–4
32. Banerjee D, Dong B et al (2014) Privacy-preserving channel access for internet of things. IEEE Internet Things J 1(5):430–445
33. Hummen R, Shafagh H et al. (2014) Delegation based authentication and authorization for the IP-based internet of things. In: Proceedings of 2014 I.E. international conference on Sensing, Communication and Networking (SECON), pp 284–292
34. Gerdes S, Bergmann O, Bormann C (2014) Delegated authentication authorization for constrained environments. In: Proceedings of IEEE 22nd international conference on network protocols, pp 654–659
35. Ning H, Liu H, Yang TL (2013) Aggregated-proof based hierarchical authentication scheme for the internet of things. IEEE Trans Parallel Distrib Syst 26(3):657–667
36. Hernandez-Ramos LJ, Pawlowski PM (2015) Toward a lightweight authentication and authorization framework for smart objects. IEEE J Sel Areas Commun 33(4):690–702
37. Lai C, Li H et al (2014) CPAL: a conditional privacy-preserving authentication with access linkability for roaming service. IEEE Internet Things J 1(1):46–57
38. Jan AM, Nanda P et al. (2014) A robust authentication scheme for observing resources in the internet of things environment. In: IEEE 13th International conference on trust, security and privacy in computing and communication, pp 205–211
39. Raheem A, Lasebae A, Loo J (2014) A secure authentication protocol for IP-based wireless sensor communications using the Location/ID Split Protocol (LISP). In: Proceedings of IEEE 13th international conference on trust, security and privacy in computing and communication, pp 840–845
40. Pawlowski PM, Jara JA and Ogorzalek JM et al. (2015) EAP for IoT:more efficient transport of authentication data- TEPANOM case study. In: Proceedings of 2015 29th international conference on advanced information networking and applications workshop, pp 694–699
41. Druml N, Menghin M, et al (2014) A flexible and lightweight ECC-based authentication solution for resource constrained systems. In: Proceeding of 2014 17th Euromicro conference on digital system design, pp 372–378
42. Schukat M, Flood P (2014) Zero-knowledge proofs in M2M communication. In: Proceedings of ISSC 2014/CHCT 2014, pp 269–273

43. Flood P, Schukat M (2014) Peer to peer authentication for small embedded systems. In: Proceedings of 10th international conference on digital technology, pp 68–72
44. Porambage P, Schmitt C et al (2014) Two phase authentication protocol for wireless sensor networks in distributed IoT applications. In: Proc IEEE WCNC 2014, pp 2728–2733
45. Yao X, Han X et al (2013) A lightweight multicast authentication mechanism for small scale IoT applications. IEEE Sensors J 13(10):3693–3701
46. Kothmayr T, Schmitt C et al (2012) A DTLS based end-to-end security architecture for the internet of things with two-way authentication. In: Proceedings of 2012 37th local computer network workshop, pp 956–963
47. Lee JY, Lin W, Huang Y (2014) A lightweight authentication protocol for internet of things. In: Proceedings of 2014 international symposium on next generation electronics, pp 1–2
48. Mahalle NP, Prasad RN, Prased R (2014) Threshold cryptography based group authentication scheme for internet of things. In: Proceedings of 2014 4th international conference on aerospace & electronic systems, pp 1–5
49. Adiga BS, Balamuralidhar P et al. (2012) An identity based encryption using Elliptic curve cryptography for secure M2M communication. In: Proceedings of 2012 SecurIT, pp 68–74
50. Liao Y, Hsiao C (2013) A secure ECC-based RFID authentication scheme using hybrid protocols. Adv Intell Syst Appl 2(21):1–13
51. Liao Y, Hsiao C (2014) A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. Ad Hoc Netw 18:133–146
52. Chou J (2014) An efficient mutual authentication RFID scheme based on elliptic curve cryptography. J Supercomput 70(1):75–94
53. Roman R, Zhou J, Lopez J (2013) On the features and challenges of security and privacy in distributed internet of things. Comput Netw 57:2266–2279