Object Authentication in the Context of the Internet of Things: A Survey

Maha Saadeh[1], Azzam Sleit[2], Khair Eddin Sabri[2]
and Wesam Almobaideen[2,3,*]

[1]*Middlesex University, Dubai, UAE*
[2]*Department of Computer Science, The University of Jordan, Amman, Jordan*
[3]*Rochester Institute of Technology, Dubai, UAE*
Email: m.saadeh@mdx.ac.ae; azzam.sleit@ju.edu.jo; k.sabri@ju.edu.jo;
almobaideen@inf.ju.edu.jo; wxacad@rit.edu
[*]*Corresponding Author*

Received 07 December 2019; Accepted 11 April 2020;
Publication 26 June 2020

Abstract

Internet of Things (IoT) is considered as the future of the Internet that connects billions of objects all together. Trusted communication between these objects is a crucial requirement for the wide deployment of IoT services. Consequently, effective authentication procedures should be applied between the communicating objects. This paper provides a comprehensive survey of object authentication in the IoT. The survey aims to direct future researchers in the field of IoT object authentication by delving into the details of authentication schemes and going through different comparisons. Comparisons are based on various criteria which include authentication process characteristics, the underlying architecture, key generation and distribution techniques, supporting IoT challenges, security analysis, and performance evaluation. Additionally, this survey highlights the main issues and challenges of IoT objects authentication and recommends future research directions.

Keywords: Internet of Things, object authentication, authentication challenges, Identity-based Cryptography, Smartcard authentication.

Journal of Cyber Security and Mobility, Vol. 9_3, 385–448.
doi: 10.13052/jcsm2245-1439.932

1 Introduction

Recent development and deployment of smart technologies have introduced new lifestyle in various communities. Gradually, people lifestyle has changed toward smartness and intelligence. Moreover, different daily activities such as route planning, navigation, transportation decisions, traffic and healthcare monitoring, and elderly and children supervision, can be facilitated by the development of smart phones, smart homes, and even smart communities [1–5]. This requires high connectivity between a huge number of smart objects, systems, and devices. In order to evolve toward a new world of connected objects, the Internet of Things (IoT) has been introduced as the future of the Internet [6–8]. Figure 1 shows the main applications of IoT.

For wide and fast deployment of IoT, people should trust these new technologies and should be encouraged to securely access various IoT resources. This can be facilitated by the provision of trusted communication services such as Key distribution and object authentication schemes [9–11].

Authentication schemes manage entity verification based on asymmetric methods, such as Public Key Cryptography (PKC) and Identity Based Cryptography (IBC), or symmetric methods [12]. Identity based cryptography is a special type of public key cryptography where entity identity is used as a public key eliminating the need for certificate management [13].

This paper presents a comprehensive survey for IoT object authentication schemes. Several IBC and non-IBC based authentication schemes are summarized and compared. Moreover, it highlights IoT object authentication

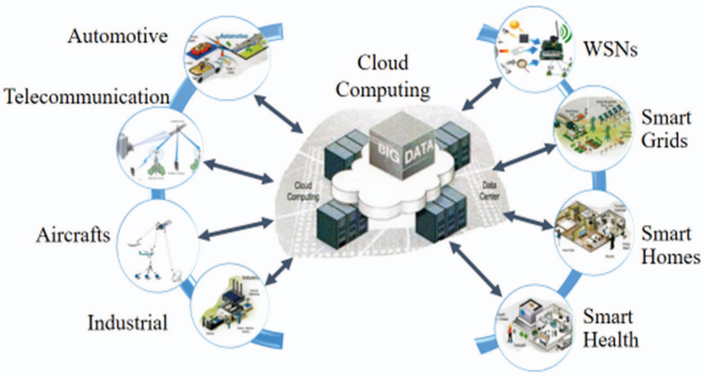

Figure 1 Internet of things main applications.

issues and challenges. The contributions of this survey can be summarized as in the following points:

1. Provides a comprehensive survey which summarizes various IBC and non-IBC authentication schemes in different IoT environments mainly; wireless sensor networks and cloud centric IoT environments.
2. Highlights the advantages and disadvantages of the studied schemes.
3. Provides several comparisons in tabular form for IoT authentication schemes according to multiple criteria, that mainly include; the authentication process, classification of the architecture i.e. hierarchal or centralized, challenges, key generation and distribution, security analysis and performance evaluation provision.
4. Discuss object authentication issues and challenges in the context of internet of things and recommends research directions for objects authentication in the context of IoT.

The rest of this paper is organized as follows. Section 2 discusses the main related works. Section 3 summarizes and compares PKC authentication schemes. IBC and smartcard authentication schemes are summarized and compared in Section 4 and Section 5, respectively. Authors observations are summarized in Section 6. Section 7 discusses the main challenges of IoT object authentication and provides research recommendation based on the discussed observations. Finally, Section 8 concludes this survey.

2 Related Works

In the literature, several surveys have been conducted to study research efforts in the field of object authentication. In [13–20] authentication schemes based on IBC have been studied. The objectives of these surveys were to review the main concepts of IBC, summarize several IBC authentication schemes, highlight their main advantages and disadvantages, discuss the main applications of IBC, and highlight some issues related to the future use of IBC. Dedicated research for IBC authentication schemes in MANETs, cloud computing environments, and VANETs have been conducted in [16, 18], and [19], respectively. Other IBC and non-IBC authentication schemes are considered in [10, 12, 21–23]. The work presented in [21] provides a description of Mobile Cloud Computing (MCC) security challenges and a comprehensive survey of authentication schemes in MCC. The authors in [23] survey authentication schemes for VANET and presents open security issues in VANET authentication. The research conducted in [10, 12], and [22] survey authentication protocols in different IoT environments. A survey on Single Sign-On (SSO) schemes is presented in [24] and a survey of smartcard-based authentication is conducted in [25]. Table 1 summarizes the main objectives of related surveys that exist in the literature and compares between them.

3 Authentication Schemes Based on Public Key Cryptography

Public key cryptosystem is a cryptographic system that uses two keys; enciphering key and deciphering key. Enciphering key could [26] be the public key and is used to encrypt messages to be sent confidentially to the keys' owner. The keys' owner uses the deciphering key to decrypt these messages. Since the owner is the only one who should know the deciphering key, it is called the private key. Public and private keys are related, that is if any text is encrypted by one of them it should be decrypted by the other. To ensure a high security level of PKC, there must be no easily computation method to derive one key from the other [27]. The private key can be used as enciphering key to generate digital signatures. Receiver can verify the correctness of this signature using the corresponding public key which is used as a deciphering key and called verification key. Digital signatures are important to guarantee authentication, non-repudiation, and message integrity security requirements [28].

The correctness of the public key is usually protected by a certificate [13]. X.509 is a certificate standard which is defined by the International Telecommunications Union's Standardization sector (ITU-T). This standard defines the format of digital certificates [29]. Digital certificates are usually issued by a trusted third party called the Certificate Authority (CA). Keys and certificates are managed by the Public Key Infrastructure (PKI) [13].

3.1 Summary of PKC authentication schemes

In [30–38] Elliptic Curve Cryptography (ECC) based PKC schemes are proposed. The scheme in [30] is proposed for WSNs and the authentication is performed in two phases: the first phase is system initialization in which all Elliptic Curve (EC) parameters are selected and the private key is generated. After initialization, all public parameters are distributed to the network. The base station can be used as a CA to generate all nodes private keys and distribute them to sensor nodes. The second phase is node authentication using ECC in which node B authenticates node A when node A wants to

Table 1 A comparison between related surveys in the literature

Ref	Description	Scope	Domain	Discuss Security Issues	Present Comparisons/ Classifications	Date
[14]	1. Review the basic concepts of IBE and IBS. 2. Review some IBC schemes that are based on bilinear pairing and some non-IBC schemes. 3. Highlight some problems of IBC	1. Bilinear pairing-based IBC schemes. 2. Some non-IBC schemes.	Open	No	No	2004
[15]	1. Review basic mathematical concepts related to IBC which are integer factorization, quadratic residues and bilinear pairings. 2. Survey three fundamental IBC primitives; digital signature, encryption and key agreement. 3. Review the main concepts of IBC.	IBC schemes	Open	No	No	2005
[16]	1. Review the concepts of IBC. 2. Survey the security applications of IBC in MANETs. 3. Summarize schemes related to master and private keys, group keys generation, and secure routing. 4. Discuss the applications of IBC in MANETs and highlights IBC issues.	IBC schemes	MANET	Yes	Yes	2011

(*Continued*)

Table 1 Continued

Ref	Description	Scope	Domain	Discuss Security Issues	Present Comparisons/ Classifications	Date
[24]	1. Survey various SSO methods and highlights their advantages. 2. Discuss the different types of SSO.	SSO methods	Open	No	No	2012
[17]	1. Survey various identity based Signcryption methods. 2. Highlight their advantages and disadvantages.	IB multi-receiver based signcryption methods	Open	No	Yes	2014
[13]	1. Review basic concepts of IBC. 2. Survey various IBC schemes based on bilinear pairing. 3. Compare IBC schemes with PKI schemes. 4. Highlight the advantages and disadvantages of IBC. 5. Study the applications of IBC.	IBC schemes	Open	No	No	2014
[18]	1. Survey various IBE schemes in cloud computing. 2. Highlight its advantages and disadvantages. 3. Propose an IBE development.	IBE schemes	Cloud computing	No	Yes	2015

[12]	1. Survey various authentication schemes and highlights the advantages and dis advantages. 2. Classify the studied schemes based on key bootstrapping mechanisms in IoT. 3. Provide an overview on recent trends on IoT security protocols	Secure communication in IOT.	IoT	Yes	Yes	2015
[21]	1. Provide a description of MCC security challenges. 2. Provide a comprehensive survey of authentication methods in MCC and highlights its advantages and disadvantages. 3. Provide a comparison of authentication methods in MCC based on security and performance features. 4. Discuss several open challenges of authentication in MCC.	Authentication methods in MCC.	Mobile cloud computing	Yes	Yes	2016
[10]	1. Survey authentication protocols in different IoT environments mainly Wireless sensor networks and cloud centric IoT environments. 2. Discuss authentication issues in IoT layered architectures. 3. Provide a taxonomy of authentication protocols for the IoT according to how the authentication process is performed and the characteristics of the authentication process. 4. Provide a comparison of authentication protocols for the IoT according to the evaluation model and security attacks.	Authentication schemes in IoT.	IoT	Yes	Yes	2016

(*Continued*)

Table 1 Continued

Ref	Description	Scope	Domain	Discuss Security Issues	Present Comparisons/ Classifications	Date
[19]	1. Present a survey of all the existing identity-based batch verification schemes for VANET and highlights the advantages and disadvantages.	IB batch verification schemes for VANET.	VANET	No	No	2016
[20]	1. Review the basic concepts of IBC and HIBC. 2. Review several IBC schemes and their advantages and disadvantages. 3. Highlight the applications of IBC.	IBC and HIBC schemes.	Open	No	No	2016
[22]	1. Survey authentication protocols in different IoT environments mainly (1) Machine to machine communications (M2M), (2) Internet of Vehicles (IoV), (3) Internet of Energy (IoE), and (4) Internet of Sensors (IoS). 2. Provide a taxonomy and comparison of authenticationprotocols for the IoT.	Authentication schemes for IoT	IoT	Yes	Yes	2016
[23]	1. Survey authentication schemes for VANET. 2. Classify authentication schemes and discuss their mechanisms, advantages, disadvantages, performance and scope. 3. Present open security issues in VANET authentication.	Authentication schemes for VANET	VANET	Yes	Yes	2017

[25]	1. Study of biometric based remote user authentication schemes using smart cards. 2. Summarize and discuss distinct attacks that are likely to occur on a remote user authentication scheme.	Biometric based remote user authentication schemes using smart cards	open	Yes	Yes	2017
This survey	1. Survey authentication protocols in different IoT environments mainly wireless sensor networks and cloud IoT environments. 2. Summarize various identity and non-identity based authentication schemes related to encryption, signature and smartcard generation. 3. Highlight the advantages and disadvantages of the studied schemes. 4. Review the basic concepts of identity-based cryptography and public key infrastructure. 5. Provide a comparison in tabular form for authentication protocols in IoT according to several factors. 6. Discuss authentication issues and challenges in the internet of things. 7. Suggest and discuss research directions for objects authentication in the internet of things.	Authentication schemes in IoT.	IoT	Yes	Yes	2019

communicate with node B according to the following steps: Step 1: Node A calculates Ta = a × r1 × Pb where r1 is a randomly selected integer, Pb is B's public key, and "a" is A's private key. Then, A sends the calculated Ta to B. Step 2: Node B calculates Tb = b × r2 × Pa where r2 is a randomly selected integer, Pa is A's public key, and "b" is B's private key. Then, B sends the calculated Tb to A. Step 3: Node A calculates SA = r1 × Tb and sends SA to B. Step 4: B calculates SB = r2 × Ta and then validates whether the equation SB = SA holds. If yes, then the authentication of node A is completed.

The scheme proposed in [31] uses two trusted authority models; the Registration Authority (RA) and the Home Registration Authority (HRA). The authentication between users and objects should be performed through the RA as follows: 1 – when any user wants to access an object, the object issues an authentication request to the RA. 2 – the RA asks for the user ID and contacts the HRA for user verification. 3 – knowing the user ID, the HRA verifies the user and sends the verification to the RA. 4 – the RA issues a session key based on ECC to communicate with the user securely.

The scheme that is proposed in [32] solves the problem of IoT heterogeneity by managing different IoT domains using controllers and central database. Moreover, it uses gateways between different networks. The authentication is performed in three phases which are the gateway certificate phase in which each gateway generates its own public key using ECC and requests for a certificate from its domain controller. The next phase is the things registration phase in which each thing requests a public key from the controller through its network gateway. Finally, in the authentication phase the thing requests to be authenticated by the gateway.

The method in [33] is based on blind signature. There are three entities; devices, gateway and storage server. All credentials are stored on the storage server and key pair for each entity is assumed to be generated using ECC. The method is performed in four phases; registration, storage, retrieval, and authentication. The device should be authenticated to the gateway to be allowed for network accessing as follows: 1 – the device sends a message to the gateway containing its ID, registration ID (obtained during the registration phase) and its signature (retrieved from the storage), all encrypted with the gateway public key. 2 – the gateway decrypts it and finds the stored hash and the device public key using the registration ID, then it decrypts the signature using the device public key and compares the resulted hash with the stored hash. If they are the same, then the device is authenticated.

The authors in [34] and [35] have proposed an authentication method based on ECC for cloud environment. The method is performed in three phases in which the device ID and ECC points are used for authentication. Firstly, in the registration phase the embedded device registers itself with the cloud server which stores a cookie on the embedded device. Secondly, in pre-computation and login phase the device sends a login request to the server containing two elliptic curve point. Finally, in authentication phase the embedded device and the cloud server authenticate each other using elliptic curve parameters and the two points sent in the login phase.

The scheme in [36] is an ECC based authentication scheme for smart grid. The proposed scheme is performed in two phases: the initialization phase in which the control center finds all public parameters, loads smart appliances with their IDs, and it loads the substation with the IDs list. Then, the substation finds its secret key and the key pairs for the appliances. Next, in the authentication phase, mutual authentication is performed between the specified smart appliance and the substation using substation's secret key and the appliance's key pair.

A One Time Signature (OTS) scheme is proposed in [37]. In this scheme, the signer generates his signature based on a selected random string, time, and a shared password. The authentication is performed according to the following order: The Smart Meter (SM) sends a signed message to the control server which uses the shared password and the time to check the SM. Then, the server generates his signature and sends it to the SM which verifies it. By this stage mutual authentication is achieved between the SM and the control server.

The authentication scheme that is proposed in [38] uses OTP implemented based on ECC. The proposed scheme is suitable to be used in many IOT applications such as, Smart city, Smart parking, and Waste management. For each communication session between the object and the server, elliptic curve Diffie–Hellman (ECDH) is used to agree on a secret session key K. Then, based on K, a one-time password is generated to authenticate the object. Once it is authenticated a one-time key is generated using K to be used in the communication between the object and the server. In [39] an energy-efficient and secure mutual authentication protocol is proposed. It is based on combination of RC5 (Rivest Cipher) and ECC. ECDH is used to exchange the session key to be used in RC5 for data confidentiality. Elliptic Curve digital signature algorithm (ECDSA) is used to sign the message and ensure authentication and data integrity. Since this scheme is based on ECC, it is suitable for IoT constrained devices.

Non-ECC based schemes are proposed in [40–42]. In [40] the authentication process is handled by a separated agent to reduce the authentication overhead at the cloud server. To authenticate cloud users, users' devices should be registered to an authentication server. Then, each user is assigned a unique code by the authentication server which encrypts it using a pre-chosen password and sends it to the user. At the user side, this code is decrypted using the same chosen password. On the other hand, unregistered devices are authenticated by Software-as-a-Service (SaaS) agent using Modified Diffie-Hellman (MDH) algorithm.

In [41] inter-cloud authentication based on inter-cloud Single Sign-On (SSO) scheme is proposed. The scheme allows users to access an inter-cloud community resources using SSO account. Each cloud should register its resources to an inter-cloud manager server to join the inter-cloud community. Users also need to get their inter-cloud accounts by registering their information to the manager server. The authentication process is performed using Shibboleth and is done through an Identity Provider (IdP). In order to associate the inter cloud account with clouds local accounts, a proxy certificate is used to do the mapping.

A layered authentication scheme is proposed in [42]. Each layer consists of one or more cells. Each cell has a cell manager which manages the inter-communication with other cells. Authentication can be performed between peer nodes in the same cell or between nodes in different cells. In the first case, a node should know the certificate of its peer in advance. In the second case, a node must contact its cell manager to get its peer certificate. Then, the cell manager contacts other cell managers to get the required certificate. The communication between cell managers is done using their certificates that have been issued by their layer manager.

In [43], the authors have proposed Radio-Frequency Identification (RFID)-based authentication using ECC. The authentication process is initiated by the tag reader and ends with the tag and the tag reader authenticating each other and the server authenticating both tag and tag reader. Before each session, the server assigns a temporary key to the tags which is stored in the tag database and updated after every session. This scheme ensures privacy by preventing any adversary from retrieving tag's significant information during the communication.

3.2 Comparison and discussion

Table 3 shows the comparison between PKC based authentication schemes in regard with the characteristics of the authentication process. The authentication process between network's entities is performed directly in all studied

Table 2 Pros and cons of the studied PKC authentication methods

Ref	Pros	Cons
[30]	1. Based on ECC which is suitable for constrained devices. 2. Supports networks and nodes heterogeneity.	The need for trusted certification authority to generate and distribute public and private keys.
[31]	1. Based on ECC which is suitable for constrained devices. 2. Supports network and nodes heterogeneity. 3. Supports mobility. 4. Can be applied over multiple domains. 5. Scalable due to the use of HRA for each domain to register domain's users only.	HRA and RA communicate with the user during the authentication which could increase the overhead on these entities.
[32]	1. Based on ECC which is suitable for constrained devices. 2. Scalable. 3. Solves heterogeneous problem. 4. Considers moving things.	1. Needs a trusted authority (the controller) to issue public key certificates to gateways. 2. The authentication process is done through the gateway which could increase the overhead on this entity.
[33]	1. Credentials could be stored on a separated storage which keeps credentials safe against compromised node attack. 2. Uses blind signature for credential retrieval from a separated storage. 3. No need for trusted authority. 4. Scalable since gateways are not required to store users' credentials. 5. Support heterogeneity.	Centralized architecture could increase the overhead on gateways.
[34]	Efficient for embedded devices that are HTTP enabled since it is based on ECC and HTTP cookies.	1. Does not support IoT challenges such as scalability, heterogeneity, constrained devices and mobility. 2. Failed to achieve mutual authentication which is proved by [35].

(*Continued*)

Table 2 Continued

Ref	Pros	Cons
[35]	Efficient for embedded devices that are HTTP enabled since it is based on ECC and HTTP cookies.	Does not support IoT challenges such as scalability, heterogeneity, constrained devices and mobility.
[36]	Based on ECC which is suitable for constrained devices.	1. Low scalability due to the centralized architecture. 2. Does not support IoT challenges such as heterogeneity and mobility.
[37]	1. Based on OTS which is efficient due to the use of a one-way function. 2. Based on ECC which is suitable for constrained devices. 3. Solve key escrow problem.	1. OTS suffers from man in the middle attack and large signature size. 2. Does not support IoT challenges such as scalability, heterogeneity, and mobility.
[38]	1. Based on ECC which is suitable for constrained devices. 2. Support scalability since it is distributed. 3. Support mobility and suitable for different domains.	1. No mutual authentication. 2. Three credentials should be generated for each session.
[39]	1. Based on ECC which is suitable for constrained devices. 2. Support scalability since it is distributed. 3. Support mobility and suitable for different domains. 4. Support mutual authentication.	Multiple credential scheme.
[40]	Scalable due to the use of a client-based user authentication which decreases the dependency on cloud-based operations. Moreover, using cloud-based and a separated authentication server will increase the ability of managing authentication in large number of requests simultaneously.	1. Does not support IoT challenges such as heterogeneity, constrained devices and mobility. 2. The authentication process is done through the authentication server which could increase the overhead on this entity. 3. Suffers from single point of failure problem due to the centralized authentication server. 4. The performance of this scheme is not evaluated.

(*Continued*)

Table 2 Continued

Ref	Pros	Cons
[41]	1. Based on SSO which allows the user to access different clouds using single sign on. 2. Supports multiple domains. 3. Supports heterogeneity.	1. Does not support scalability due to the centralized architecture. 2. The performance of this scheme is not evaluated. 3. Both users and cloud systems should be registered to the same inter-cloud manager. 4. In SSO there is a need for trusted IdP in each authentication process which could become the inter-cloud system bottleneck when too many requests have to be performed. 5. During the authentication process, the IdP should be associated with a secure channel to transmit the keys such as Secure Socket Layer (SSL). 6. Public key cryptography such as RSA is usually used by SSL, therefore, this technique is not suitable for simple IoT devices.
[42]	1. Supports IoT challenges such as scalability, heterogeneity, and constrained devices. 2. Can be applied over multiple domains.	1. To group the nodes into layers/cells, there is a need to have a global information about the network which requires the initial layer manager to contact all available nodes to know their status. 2. The criteria that are used to group network nodes into layers/cells should be defined prior the grouping process. 3. To localize the needed resources, nodes metadata should be collected at the run time. 4. The search strategy to localize nodes should be chosen with regard to the grouping criteria and should be efficient by avoiding traffic overhead. 5. If different policies are used by different layers/cells, all cell managers should be aware of these policies. 6. The performance of this scheme is not evaluated.

(*Continued*)

Table 2 Continued

Ref	Pros	Cons
[43]	1. Supports IoT challenges such as scalability, heterogeneity, and constrained devices. 2. Based on ECC which is suitable for low-resource devices.	1. For each session new keys should be calculated. 2. Tags' keys and readers' public keys should be preloaded to the tags by the server.

Table 3 A comparison between PKC authentication methods according to authentication process characteristics

Ref	Mutual Authentication	Registration Phase	Offline Phase	Additional Hardware	Multiple Credentials	Direct or Indirect Authentication
[30]						Direct
[31]	√	√	√			Direct
[32]		√				Direct
[33]		√				Direct
[34]		√	√			Direct
[35]	√	√	√			Direct
[36]	√					Direct
[37]	√				√	Direct
[38]		√			√	Direct
[39]	√	√			√	Direct
[40]	√	√				Direct
[41]		√				Direct
[42]	√		√			Direct/Indirect
[43]	√					Direct

schemes. Most of the studied schemes achieved mutual authentication and none of them uses any additional hardware to perform the authentication process. Moreover, except for [30, 36, 37], registration/offline phases are essential phases in the authentication process. Table 4 shows the comparison between PKC based schemes according to the architecture. As in symmetric based schemes, studies have concentrated on centralized architectures whereas hierarchal architectures are not extensively considered. In Table 5 the comparison between PKC based schemes according to IoT challenges is illustrated. As can be seen, supporting IoT constrained devices is the most considered challenge followed by heterogeneity and scalability. Three schemes are applied over multiple domains. As in symmetric based schemes,

Table 4 A comparison between PKC authentication methods according to method architecture

Ref	Centralized Architecture	Hierarchal Architecture	Decentralized flat Architecture
[30]			√
[31]	√	√	
[32]	√	√	
[33]	√		
[34]			√
[35]			√
[36]	√		
[37]	√		
[38]			√
[39]			√
[40]	√		
[41]	√		
[42]	√	√	
[43]	√		

Table 5 A comparison between PKC authentication methods according to iot challenges support

Ref	Support Scalability	Support Networks Heterogeneity	Support Nodes Heterogeneity	Support Mobility	Support Constrained Devices	Support Multiple Domains
[30]	×	√	√	×	√	×
[31]	√	√	√	√	√	√
[32]	√	√	√	√	√	√
[33]	√	√	√	×	√	×
[34]	×	×	×	×	×	×
[35]	×	×	×	×	×	×
[36]	×	×	×	×	√	×
[37]	×	×	×	×	√	×
[38]	√	√	√	√	√	√
[39]	√	√	√	√	√	√
[40]	√	×	×	×	×	×
[41]	×	√	√	×	×	√
[42]	√	√	√	×	√	√
[43]	√	×	√	×	√	×

mobility has been considered by only one scheme. Table 6 shows the comparison according to keys generation and distribution methods. As can be noticed, various methods are used to distribute keys pair among entities. ECC is the most used method in the studied PKC schemes. On the other hand, some schemes assume the use of secret channel to distribute key pair. Finally,

Table 6 A comparison between PKC authentication methods according to keys generation and distribution methods

Ref	Identity is used in keys/credentials generation	Keys Generation method	Keys distribution method
[30]	No	PKC-ECC	Secure channel
[31]	Yes	PKC-ECC	Secure channel
[32]	Yes	PKC-ECC	ECC
[33]	No	PKC-ECC	ECC
[34]	Yes	PKC-ECC	ECC
[35]	Yes	PKC-ECC	ECC
[36]	Yes	PKC-ECC	Secure channel
[37]	No	PKC-ECC	Pre-distributed
[38]	No	PKG-ECC	ECDH
[39]	No	PKG-ECC	ECDH
[40]	No	PKC	Public
[41]	No	PKC	Not mentioned
[42]	No	PKC	DH
[43]	No	PKG-ECC	Stored in the tag

security analysis and performance evaluation for the studied PKC schemes are listed in Tables 7 and 8, respectively.

4 Authentication Schemes Based on Identity-Based Cryptography

Identity-based cryptography is a PKC approach in which entity identity is used as a public key. In encryption-based IBC, called Identity Based Encryption (IBE), the sender uses receiver's identity-based public key to encrypt a message *M* into cipher text *C*. The receiver uses his private key, which is generated based on his identity, to decrypt *C* and obtain *M*. If the sender wants to send a signed message, he uses his private key to generate the signature and sends the signed message to the receiver who uses the sender's identity based public key to verify the signature. The main idea behind IBC is to generate private keys based on identities. The generation process is done usually by a separated entity called Private Key Generator (PKG).

IBC was first proposed by Shamir [44]. In his proposal, identities were used as a signature verification key. The scheme was called Identity based Signature (IBS) and could not be used for encryption-decryption process [13]. Latterly, an efficient IBE scheme was proposed by Boneh and Franklin [45]. Following are the main phases in IBS and IBE.

IBS: An Identity based signature scheme has the following four phases:

Table 7 A comparison between PKC authentication methods according to security analysis

Ref/ Attacks	[30]	[31]	[32]	[33]	[34]	[35]	[36]	[37]	[38]	[39]	[40]	[41]	[42]	[43]
MITM Attack	×	√	√	×	√	√	×	√	√	√	√	√	√	×
Insider Attack	×	×	×	√	×	×	×	√	×	×	×	×	×	×
Timing Attack	×	×	×	×	×	×	×	×	×	×	√	×	×	×
Impersonation Attack	×	×	×	√	×	×	×	×	×	√	×	×	×	×
Replay Attack	×	√	√	×	√	√	×	√	√	√	×	×	√	√
Eavesdropping Attack	√	√	×	√	√	√	×	×	×	√	√	×	√	√
Dos Attack	×	×	×	×	×	×	×	√	×	×	×	×	×	√
Forgery attack	√	×	×	×	×	×	×	×	√	√	×	×	×	×
Masquerade Attack	×	×	√	×	×	×	×	×	×	×	×	×	×	×
Physical Attack	×	×	×	√	×	×	×	×	√	×	×	×	×	×
Brute Force Attack	×	×	×	√	√	√	×	×	×	×	√	×	×	×
Anonymity	×	×	×	×	√	√	×	×	×	×	×	×	×	×
Identity Protection	×	×	×	×	×	×	√	×	×	×	×	×	×	×
Correctness Proof	×	×	×	×	×	×	√	√	√	√	×	×	×	×
Password change/guessing Attack	×	×	×	×	×	×	×	√	×	×	×	×	×	×
Privacy	×	×	×	×	×	×	×	×	×	×	×	×	×	√

Table 8 A comparison between PKC authentication methods according to performance evaluation.

Ref/ Performance Metrics	[30]	[31]	[32]	[33]	[34]	[35]	[36]	[37]	[38]	[39]	[40]	[41]	[42]	[43]
Time Cost	√	×	×	√	×	×	×	√	√	√	×	×	×	×
Energy Cost	×	×	×	×	×	×	×	×	√	√	×	×	×	×
Computation Cost	×	×	√	×	√	×	√	√	√	×	×	×	×	√
Communication Cost	×	×	×	×	√	×	×	×	√	×	×	×	×	√
Storage	×	×	√	×	√	×	×	×	×	√	×	×	×	√

1. Setup phase: in which the PKG selects system's public parameters, hash functions, and generates the master key.
2. Extract phase: in which the sender contacts with the PKG to get its private key which is generated based on its identity, system's parameters, and the master key.
3. Sign phase: in which the sender uses its private key and system's parameters to issue a signature *S* on the message *M*, and sends <*M, S*> to the receiver.
4. Verify phase: in which the receiver checks the correctness of the signature using sender's identity, *S, M*, and system's parameters. If this phase passes, then the sender is authenticated.

IBE: An identity-based encryption scheme has the following four phases:

1. Setup phase: in which the PKG selects system's public parameters, hash functions, and generates the master key.
2. Extract phase: in which the user contacts the PKG to get its private key which is generated based on its identity, system's parameters and the master key.
3. Encrypt phase: the sender uses receiver's identity, i.e. public key, and system's parameters to encrypt a message *M* into cipher text *C* and sends *C* to the receiver.
4. Decrypt phase: the receiver uses its private key and system's parameters to decrypt the cipher *C*.

4.1 Summary of IBS authentication schemes

In this subsection the studied IBS authentication schemes are discussed and compared where we start firstly with a summary of these IBS based schemes.

Several bilinear pairing IBS schemes have been proposed. The authors in [46] have proposed a three-layer identity-based authentication method for Automatic Dependent Surveillance-Broadcast (ADS-B) systems. The first layer is the root private key generator which generates system public parameters and publishes it. The second layer consists of airlines that should be registered to the root to get its private key. Finally, the third layer consists of aircrafts which should be registered to airlines to get the private key. The authentication process is done by issuing a digital signature based on the concept of bilinear pairing for each message using sender's ID and private key. The signing-verification process is done through the following phases:

1 – the setup phase in which the root generates its secret key and system's public parameters. 2 – The ExtractAL phase in which the airline registers with the root using its ID and gets its private key. 3 – The ExtractAC in which the aircraft registers to an airline using its ID and gets its private key. 4 – The Sign phase in which the aircraft issues a digital signature for the message. 5 – The Verify and Bverify phases in which the verifier verifies the correctness of single or batch signature(s), respectively.

In [47] an identity-based authentication method for vehicular networks has been proposed. The method is based on identity-based signature by issuing signature keys using hash chains and bilinear pairing. It combines identity signature with pseudonymous authentication scheme, providing strong privacy preservation for vehicles. In addition to that, it allows vehicles to update their credentials on road reducing the overload on trusted authority. The main phases are system initialization, Road Side Units (RSUs) initialization, vehicle initialization, vehicle pseudonymous credential updating, identity revocation, and message signatures and verification. In [48] an ID-based proxy signature method that is based on bilinear mapping and q-strong Diffie-Hellman (DH) problem is proposed. It has three roles, the PKG, the proxy signer, and the original signer. This scheme has five phases: in the setup phase the PKG selects the public parameters based on bilinear mapping and a secret key. In the extract phase the PKG generates the private keys for the proxy signer and the original signer based on their identities and the public parameters. Next is the delegation phase in which the proxy signing key for proxy signature is generated. Afterward, in the proxy signing phase the proxy signing key is used to generate the proxy signature. Finally, in the verification phase the verifier checks the signature using the public parameters, the proxy signature and the message.

In [49], two IBS schemes are proposed. The proposed methods are based on bilinear pairing and have four phases: setup, extract, sign and verify. The difference between the two methods is that the second scheme needs only one-point scalar multiplication computation in first cyclic additive group of bilinear mapping, known as G1, to generate the signature whereas the first scheme needs one-point scalar multiplication computation in G1 and one inverse computation. As a result, the second scheme is more efficient. In [50], an online-offline IBS for WSN is proposed. The proposed scheme uses bilinear pairing for signature computation. All heavy computation is done in the offline phase which reduces the cost of online signing phase. Another bilinear pairing-based IBS is proposed in [51]. The scheme has four phases; setup, key extract, signature generation, and signature verification.

This scheme is efficient and secure against existential forgery under adaptively chosen message and ID attack in the random oracle model. The scheme proposed in [52] is secure without the random oracle model. The scheme is performed in three phases; setup phase in which all public parameters are generated based on bilinear maps. Sign phase in which the participant generates its private key and uses it with its ID to generate the signature. Finally, the verification phase in which the verifier uses the ID to get the verify key, then, it encrypts a random message to create a cipher text C. Then, it decrypts C with the given signature and checks if the same key that was sent by the participant is produced. Another IBS based on bilinear pairing is proposed in [53]. It has four phases: setup, key extract signing, and verification phases. This scheme has low computation cost and small storage requirements.

In [54–56] a hierarchal IBS schemes for cloud computing have been proposed. The top level is the root PKG. The next level consists of all sub-PKGs and the bottom level are the cloud users. In hierarchal IBS private keys are generated to lower level nodes based on their IDs in the hierarchy. The scheme in [54] is proposed for single clouds whereas the scheme in [55] is proposed for federal cloud computing systems in which the user can access several clouds from different domains. The root PKG manages the whole clouds, each private or public cloud is located in the second level. The third level consists of cloud users and servers. The root allocates and manages identities for public and private clouds. On the other hand, public and private clouds allocate and manages identities for users and servers. Another hierarchal IBS scheme for cloud computing is proposed in [56]. This hierarchy consists of a root PKG called the broker. Sub-PKGs are located in Cloud Security Administrators (CSA). To be authenticated, users and organizations from different clouds should register their information to the broker. When a user wants to access the resources for a particular cloud, he should enter his identity according to his position in the hierarchy. Then, the parent CSA contacts the broker to request user authority proof. Afterward, the broker generates a private key and sends it back to the user through the CSA along with its authority proof. These solutions are scalable because of the hierarchal architecture. In addition to IBS schemes both [54] and [56] uses the generated private keys to propose IBE schemes.

All the discussed IBS schemes are based on bilinear pairing. Bilinear pairing is considered to be an expensive cryptographic operation. Its relative computation cost is approximately twenty times higher than the computation cost of the scalar multiplication over elliptic curve group [57].

Non-bilinear pairing schemes are proposed in [57–62]. The IBS scheme that is proposed in [57] is based on discrete logarithm which is simple and efficient. Users' biometric identities are used to extract users' private keys. The private key of each user is divided into multiple shares corresponding to multiple attributes of user biometric. The scheme proposed in [58] uses online-offline signature for aircrafts applications. The aim is to reduce the cost of signature computation by doing all heavy calculation in the offline phase. In online phase the aircraft uses all public parameters, which is assumed to be preloaded, its private key, and the signature parameters generated in the offline phase in order to sign the message. The signature generation is based on ECC. The authors in [59] have proposed an authentication framework based on identity for WSN. The proposed framework is divided into two parts. Firstly, sensor authentication part in which the base station generates private keys for all sensors to be used for online message signing. In addition to that, it generates part of the signature offline and leaves simple operation to be performed online. The second part is user authentication part in which the user registers his identity with the base station and gets his private key. ECC is used for key generation. Another ECC based IBS scheme is proposes in [60]. This proposed scheme has three entities; the PKG, initiator, and responder. The PKG is responsible for EC parameter generation in the setup phase and generates private keys for users based on their identity in the extract phase. The two entities, i.e. initiator and responder, agree on a sheared key that is used for secure communication in the key agreement phase. Another authentication scheme based on IBS is proposed in [61]. This technique is based on cryptographically generated subnet-IDs by sitting the subnet-ID to a truncated hash of the Trusted Authority (TA) public key. Each packet contains IPv6 header along with the needed message and the sender signature. When a packet, which is sent to a particular receiver, arrives at the border gateway then it checks if the sender is in the same subnet as itself. If so, the border gateway and the receiver can authenticate the message using the same TA public key. Otherwise, the receiver needs to obtain the public key of the TA corresponding to the sender's subnet in order to authenticate the message. The TA public key lookup process can be performed by independent TA lookup methods on the IoT gateways.

A non-interactive pairing-free ID-based proxy re-signature scheme for healthcare (ID-PRS) is introduced in [62]. The scheme is based on edge computing architecture to achieve slow-latency message response and computation of?oading of the terminal user. The scheme has four entities:

Table 9 Pros and cons of the studied IBS authentication methods

Ref	Pros	Cons
[46]	1. Provides full batch verification. 2. Scalable due to the hierarchal architecture. 3. Supports moving objects. 4. Can be applied over multiple domains. 5. No Certification Management.	1. Does not support heterogeneity. 2. Does not support constrained devices. 3. Based on bilinear pairing which considered to be expensive operation compared with ECC. 4. Does not solve the key escrow problem.
[47]	1. RSU act as a sub certificates issuer which decrease the overhead of TA. 2. Privacy reservation: although RSUs issue the authentication credentials, they do not know the mapping between the pseudo identities and real identities. 3. Supports mobility. 4. Supports scalability due to the Hierarchal architecture.	1. Does not support heterogeneity. 2. Does not support constrained devices. 3. Based on bilinear pairing which considered to be expensive operation compared with ECC. 4. Does not solve the key escrow problem.
[48]	1. Short signature length. 2. Supports scalability due to the Hierarchal architecture. 3. Suitable for application in some low resource situations. 4. No Certification Management.	1. Does not support heterogeneity and mobility. 2. Based on bilinear pairing. 3. Key escrow problem.
[49]	1. Efficient with low computations. 2. Supports constrained devices. 3. No Certification Management.	1. Based on bilinear pairing. 2. Does not support heterogeneity, scalability and mobility. 3. Does not solve the key escrow problem. 4. Single point of failure.
[50]	1. Uses offline signature which reduces the cost of signature computation by doing all heavy computation in the offline phase. 2. Scalable and efficient for constrained devices. 3. No Certification Management.	1. Based on bilinear pairing. 2. Does not support heterogeneity and mobility. 3. Does not solve the key escrow problem.

(*Continued*)

Table 9 Continued

Ref	Pros	Cons
[51]	1. No Certification Management.	1. Based on bilinear pairing. 2. Does not support heterogeneity, scalability constrained devices and mobility. 3. Does not solve the key escrow problem. 4. Single point of failure problem.
[52]	1. It is secure without random oracle model which has several advantages, including shorter public parameters and recipient-anonymity. 2. Short signature. 3. The number of pairing computations needed for signing and verifying is only one time. 4. Scalable and efficient for constrained devices. 5. No Certification Management.	1. Does not support heterogeneity and mobility. 2. Based on bilinear pairing.
[53]	1. Efficient for constrained devices. 2. No Certification Management.	1. Does not support scalability, heterogeneity and mobility. 2. Based on bilinear pairing. 3. Does not solve the key escrow problem. 4. Single point of failure.
[54]	1. Scalable due to the hierarchal architecture. 2. No Certification Management.	1. Does not support heterogeneity, constrained devices and mobility. 2. Based on bilinear pairing. 3. Key escrow problem.
[55]	1. Scalable due to the hierarchal architecture. 2. Supports heterogeneity and constrained devices. 3. No Certification Management.	1. Does not support constrained devices and mobility. 2. Based on bilinear pairing. 3. Does not solve the key escrow problem

(*Continued*)

Table 9 Continued

Ref	Pros	Cons
[56]	1. It enables users to access several cloud systems using single account. 2. The use of hierarchical model makes this technique scalable. 3. Solves the key escrow problem using virtual child. 4. Can be applied over multiple domains. 5. No Certification Management.	1. Users and cloud systems have to be registered to the same root broker. 2. All users and clouds information are kept in a single repository at the broker which could become a system bottleneck. 3. Does not support heterogeneity, constrained devices and mobility. 4. Based on bilinear pairing.
[57]	1. Uses discrete logarithm based signature which is simple and efficient. 2. Private key is constructed as a set of shares and Shamir secret sharing method is used to distribute these shares which gives the proposed scheme the property of being error tolerant since only a subset of the private key shares are needed to verify the signature. 3. No Certification Management.	1. The registration of user bio-metric needs a special hardware. 2. Does not support scalability, heterogeneity, constrained devices and mobility. 3. Does not solve the key escrow problem. 4. Single point of failure.
[58]	1. Scalable. 2. Efficient since it does not based on bilinear pairing. 3. Uses offline signature so all heavy computation is performed in offline phase which reduces the computational cost for signature generation. 4. Supports moving objects. 5. No Certification Management.	1. Does not support heterogeneity and constrained devices. 2. Does not solve the key escrow problem.
[59]	1. Scalable. 2. Efficient since it does not based on bilinear pairing. 3. Supports constrained devices. 4. Uses offline signature so all heavy computation is performed in offline phase which reduces the computational cost for signature generation. 5. No Certification Management	1. Does not support heterogeneity and mobility. 2. Does not solve the key escrow problem

(*Continued*)

Table 9 Continued

Ref	Pros	Cons
[60]	1. Efficient since it does not use bilinear pairing. 2. Supports constrained devices. 3. Supports moving objects. 4. No Certification Management	1. Does not support scalability and heterogeneity. 2. Key escrow problem. 3. Single point of failure.
[61]	1. Efficient since it does not use bilinear pairing. 2. Supports constrained devices. 3. Supports network heterogeneity. 4. Can be applied over multiple domains. 5. No Certification Management	1. The gateways are assumed to be under the same administrative control as the IoT subnet. 2. The TA lookup method may introduce traffic overhead on the network and cause long delay if not carefully chosen. 3. Key escrow problem. 4. Does not support scalability due to centralized architecture. 5. Single point of failure problem.
[62]	1. Suitable to be applied to the resource-constrained devices. 2. Supports mobility. 3. Efficient since it does not use bilinear pairing. 4. No Certification Management 5. Uses edge computing architecture to achieve slow-latency message response and computation offloading of the terminal user. 6. Supports Heterogeneity. 7. Supports scalability using mobile edge computing architecture.	1. Key escrow problem. 2. Centralized cloud server.
[63]	1. Based on ECC so it is efficient to be applied to the resource-constrained devices. 2. Supports mobility and heterogeneity. 3. Does not use bilinear pairing. 4. No Certification Management 5. Uses gateway to reduce the overhead on the object.	1. Key escrow problem. 2. Gateway single point of failure problem

PKG, the hospital, the end-user and the cloud. The PKG is responsible for calculating end-user and hospital administrator private keys. The hospital administrator utilizes its private key and the end-user's identity to generate proxy re-signing key which is used to covert the end-user's signature into the hospital administrator's signature in order to convince the cloud that the outsourced data is from the hospital. This scheme avoids paring expensive operation which makes it suitable for IoT resource-constrained devices.

In [63] the authors proposed an efficient multi-message and multi-receiver signcryption scheme based on IBC. The proposed scheme is efficient since it is based on ECC with employing scalar point multiplication operations rather than bilinear pairing. In order to reduce the overhead on the IoT object, a gateway is used for performing the verification. The sender will generate a full signcryption ciphertext and send it to the gateway. The gateway computes the signcryption veri?cation parameter and transmits to receivers. The receiver veri?es the parameter considering the public key of sender and its own private key as inputs, and then recover the plaintext message

In what follows the above discussed IBS based authentication schemes are compared.

Table 10 shows the comparison between IBS based authentication schemes based on the characteristics of the authentication process. Except for two schemes, the authentication process between network's entities is performed directly. Few schemes achieved mutual authentication and only one of them uses additional hardware to perform the authentication process. In addition to that, none of the IBS schemes uses multiple credentials in the authentication process.

Table 11 shows the comparison between IBS based schemes according to the second criterion. As illustrated, studies have concentrated on centralized architecture, however, more schemes consider hierarchal architectures compared with symmetric and PKC schemes. This increases the scalability of these schemes. In Table 12 the comparison between IBS based schemes according to IoT challenges is illustrated. Supporting scalability is the most considered challenge due to the use of hierarchal IBS schemes followed by supporting IoT constrained devices and mobility. Supporting multiple domains and heterogeneity are the least challenges that have been considered. Table 13 shows the comparison according to keys generation and distribution methods. As can be noticed, most of the studied schemes are based on bilinear pairing to generate private keys. According to the key distribution methods most of the studied IBS schemes assume the use of secure channels. Only one scheme uses the Shamir secret sharing method [57]. Security analysis

Table 10 A comparison between IBS authentication methods according to authentication process characteristics

						Direct or
	Mutual	Registration	Offline	Additional	Multiple	Indirect
Ref	Authentication	Phase	Phase	Hardware	Credentials	Authentication
[46]		√				Direct
[47]	√	√				Direct
[48]		√				Direct
[49]						Direct
[50]			√			Direct
[51]						Direct
[52]						Direct
[53]						Direct
[54]	√					Direct
[55]	√	√				Direct
[56]		√				Indirect
[57]				√		Direct
[58]		√	√			Direct
[59]		√	√			Direct
[60]	√					Direct
[61]						Indirect
[62]		√				Indirect
[63]		√				Indirect

Table 11 A comparison between IBS authentication methods according to method architecture

Ref	Centralized Architecture	Hierarchal Architecture	Decentralized flat Architecture
[46]		√	
[47]		√	
[48]		√	
[49]	√		
[50]	√		
[51]	√		
[52]			√
[53]	√		
[54]		√	
[55]		√	
[56]		√	
[57]	√		
[58]	√		
[59]	√		
[60]	√		
[61]	√		
[62]		√	
[63]			√

Table 12 A comparison between IBS authentication methods according to iot challenges support.

Ref	Support Scalability	Support Networks Heterogeneity	Support Nodes Heterogeneity	Support Mobility	Support Constrained Devices	Support Multiple Domains
[46]	√	×	×	√	×	√
[47]	√	×	×	√	×	×
[48]	√	×	×	×	√	×
[49]	×	×	×	×	√	×
[50]	√	×	×	×	√	×
[51]	×	×	×	×	×	×
[52]	√	×	×	×	√	×
[53]	×	×	×	×	√	×
[54]	√	×	×	×	×	×
[55]	√	√	√	×	×	√
[56]	√	×	×	×	×	√
[57]	×	×	×	×	×	×
[58]	√	×	×	√	×	×
[59]	√	×	×	×	√	×
[60]	×	×	×	√	√	×
[61]	×	√	×	×	√	√
[62]	√	√	√	√	√	√
[63]	√	√	√	√	√	√

is listed in Tables 14 and 15 lists the comparison according to performance evaluation.

4.2 Summary of IBE authentication schemes

Different ways can be used to achieve authentication using IBE. The following are the two approaches used by the studied IBE schemes:

A – Both sender and receiver generate a secret shared key based on the public parameters and their private keys. This approach is based on a shared value, so the correct decryption of this value achieves mutual authentication

1. The sender uses receiver's *ID* based public key to encrypt the shared key and sends the encrypted value to the receiver with the message.
2. The receiver decrypts it using his *ID* based private key.
3. Then the receiver checks the correctness of the sent key by deciding whether it is equal to the value generated on his side.

Table 13 A comparison between IBS authentication methods according to keys generation and distribution methods

Ref	Identity is used in keys/credentials generation	Keys Generation method	Keys distribution method
[46]	Yes	Bilinear Pairing	Secure Channel
[47]	Yes	Bilinear Pairing	Secure Channel
[48]	Yes	Bilinear Pairing	Not Mentioned
[49]	Yes	Bilinear Pairing	Not Mentioned
[50]	Yes	Bilinear Pairing	Secure Channel
[51]	Yes	Bilinear Pairing	Secure Channel
[52]	Yes	Bilinear Pairing	Not Mentioned
[53]	Yes	Bilinear Pairing	Secure Channel
[54]	Yes	Bilinear Pairing	Secure Channel
[55]	Yes	Bilinear Pairing	Secure Channel
[56]	Yes	Bilinear Pairing	Secure Channel
[57]	Yes –Biometric Id	Non-Bilinear Pairing	Shamir Secret Sharing
[58]	Yes	Non-Bilinear Pairing	Secure Channel
[59]	Yes	Non-Bilinear Pairing	Secure Channel
[60]	Yes	Non-Bilinear Pairing	Secure Channel
[61]	Yes	Non-Bilinear Pairing	Not Mentioned
[62]	Yes	None-Bilinear Pairing	Note Mentioned
[63]	Yes	None-Bilinear Pairing	Secure Channel

B – The sender uses a challenge value, and encrypts this value using the receiver's public key. The correct decryption of this value will authenticate the *ID* that is used to encrypt it.

1. The sender sends an encrypted value to the receiver using the receiver's *ID* based public key.
2. The receiver decrypts the message using his private key and sends it back to the sender.
3. Then the sender can check the correctness of the value by checking if it is equal to the value that is sent by him. If so, the receiver is authenticated successfully.

Several IBE authentication schemes have been proposed in the literature. The scheme in [64] discusses the issues of identity-based cryptography and

Table 14 A comparison between IBS authentication methods according to security analysis

Ref Attacks and																		
security analysis	[46]	[47]	[48]	[49]	[50]	[51]	[52]	[53]	[54]	[55]	[56]	[57]	[58]	[59]	[60]	[61]	[62]	[63]
MITM Attack	×	×	×	×	×	×	×	×	×	×	√	×	×	√	×	√	√	√
Impersonation Attack	×	×	×	×	×	×	×	×	×	×	√	×	×	×	×	×	×	√
Eavesdropping Attack	×	×	×	×	×	×	×	×	×	×	√	×	×	×	×	×	×	√
Dos Attack	×	×	×	×	×	×	×	×	×	×	×	×	×	√	×	×	×	×
Forgery attack	√	×	√	√	√	√	×	√	×	×	×	√	√	×	×	×	√	√
Anonymity	×	√	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Correctness Proof	×	×	√	×	×	×	×	√	×	×	×	√	√	×	√	×	×	√
Chosen Message and ID Attack	√	×	×	√	√	√	√	√	×	×	×	√	√	×	×	×	×	×
Node Compromise Attack	×	×	×	×	×	×	×	×	×	×	×	×	×	√	×	×	×	×
Key Attack	×	×	×	×	×	×	×	×	×	×	×	×	×	×	√	×	×	×
Internal attack	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	√	×

Table 15 A comparison between IBS authentication methods according to performance evaluation

Ref Performance Metrics	[46]	[47]	[48]	[49]	[50]	[51]	[52]	[53]	[54]	[55]	[56]	[57]	[58]	[59]	[60]	[61]	[62]	[63]
Time Cost	√	×	√	×	×	×	√	×	×	×	×	×	×	×	×	×	×	√
Energy Cost	×	×	×	×	×	×	×	×	×	×	×	×	×	√	×	×	×	×
Computation Cost	×	×	√	√	√	√	×	×	√	×	×	√	√	√	√	×	√	√
Communication Cost	×	√	×	×	×	×	×	×	√	×	√	×	×	√	√	×	×	×
Storage	×	×	×	×	×	×	×	√	×	×	×	×	×	√	×	×	×	×
Signature Size	×	×	√	×	√	×	√	×	×	×	×	√	×	√	×	×	×	×
Public Parameters Size	×	×	×	×	×	×	√	×	×	×	×	√	×	×	×	×	×	×
Signing Cost	×	√	×	×	×	×	×	√	×	×	×	×	×	×	×	√	×	×
Verifying Cost	×	√	×	×	×	×	×	√	×	×	×	×	×	√	×	√	×	×
Key Size	×	×	×	×	×	×	×	×	×	×	×	√	×	×	×	×	×	×
Message size	×	×	×	×	×	×	×	×	×	×	√	×	×	×	×	×	×	×

proposes a three levels federated identity management method for clouds environments. The proposed method allows mutual authentication between sender and receiver based on a shared key that is exchanged using IBE. The first level is the domain root PKG which generates system's public parameters and authenticates the next level clouds PKGs. The second level are the private and public clouds PKGs which authenticate the users/servers in the third levels. Each level uses its private key and the identity of the next level in order to generate the next level private key. A sender uses the server's identity and system's parameters to encrypt a session key and sends it to the server which decrypts it using its generated private key. This session key is used for mutual authentication and data confidentiality.

The scheme in [65] is used to authenticate users in cloud environments and has three entities. Firstly, the PKG which is a centralized trusted authority that generates the private keys for the users and the Cloud Revocation Authority (CRA). Secondly, the CRA which is a cloud server that generates the update keys for the un-revocable users. Finally, users who are the senders and receivers, where the receivers can be service providers. The main phases are: 1 – The setup phase in which the PKG generates the public parameters, the master key, and the time update secret key. 2 – The identity key extract phase in which the PKG generates user's identity key based on his ID. 3 – Time key update phase in which the CRA generates the time update key for the user according to certain instance of time using the user's ID and the time update secret key which was generated by the PKG. Afterward, the CRA sends the generated time update key to the user via public channel. 4 – The encryption phase in which the sender uses the receiver ID in order to generate a cipher text which is decrypted by the receiver using his private key, update key, and ID in the decryption phase.

An offline and online ID-based authentication scheme is proposed in [66]. The offline phase is used to store the general parameters and the base station public key in each sensor. Moreover, each sensor generates a node trust value and stores it in the base station. In the online phase, the sender node uses the base station public key to encrypt its generated trust value and a nonce. The base station then decrypts the message and verifies the node's trust value by comparing it to the value stored in the offline phase. If successfully verified, the base station replies with a new nonce generated from the node nonce to be verified by that node.

In [67] a one-way IBE authentication scheme is proposed. In this scheme two offline phases are used in order to preload all sensors with sensors' IDs, their private keys, and the master key. All sensors generate a trust value and store it securely at the base station. Sensor registration and authentication phases are performed in online phase. The authentication is performed when a sensor node securely sends its ID and its generated trust value to the base station. Then, the bases station performs the verification.

A non-bilinear pairing-based scheme is proposed in [68]. The proposed IBE based authentication scheme is based on ECC and Lamport One Time Password (OTP). It is based on generating EC points and using them as keys. It has the following phases: 1 – setup: the PKG selects and generates the ECC parameters and the master key. 2 – extract: In extract phase, the IoT applications and devices register their identities to the PKG and get their public and private keys. 3 – generate: the IoT application requests data from IoT device through a cloud platform. Then, PKG at IoT cloud generates the private key of the device and it also generates the OTP based on EC points and sends it to both the device and the IoT application. 4 – validate: in validate phase, the application communicates with the device by submitting OTP and the device verifies the OTP with that of received one, i.e. from IoT cloud PKG.

In [69], the authors introduced a privacy preserving and mutual authentication scheme using IBE for IoT e-health systems. This scheme solves the key escrow problem since the PKG generates a partial signature for a given entity. IBE is used to encrypt the session key that is used to secure patients' health information. The authentication of the patient is also ensured, due to the integration of his signature.

In what follows the above discussed IBE authentication schemes are compared. Table 17 shows the comparison between IBE authentication schemes according to the characteristics of the authentication process. The authentication process between network's entities is performed directly in all IBE schemes. Few schemes achieved mutual authentication and none of the IBE schemes uses additional hardware or multiple credentials in the authentication process. Most of the studied IBE schemes need offline/registration phases to perform the authentication process.

The comparison between IBE schemes according to the used architecture is listed in Table 18. Like IBS schemes, the studied IBE schemes have concentrated more on centralized architectures. From Table 19 we can notice that supporting scalability is being considered by most of the IBE schemes followed by supporting IoT constrained devices. Other challenges are not commonly considered. Table 20 shows the comparison according to keys generation and distribution methods.

Table 16 Pros and cons of the studied IBE authentication methods.

Ref	Pros	Cons
[64]	1. Scalable due to the hierarchal architecture. 2. Allows users to access multiple clouds in the same domain. 3. No Certification Management.	1. Based on bilinear pairing. 2. Does not solve the key escrow problem. 3. Does not support heterogeneity, constrained devices and mobility
[65]	1. Supports scalability and mobility. 2. Can be used in multiple server environments. 3. No Certification Management.	1. Based on bilinear pairing. 2. Does not solve the key escrow problem. 3. Does not support heterogeneity and constrained devices.
[66]	1. Supports constrained devices. 2. No certificate management.	1. Does not support heterogeneity, scalability, and mobility. 2. Does not solve the keyescrow problem. 3. Based on bilinear pairing.
[67]	1. Supports constrained devices. 2. No certificate management	1. Does not support heterogeneity, scalability, and mobility. 2. Does not solve the key escrow problem. 3. Based on bilinear pairing
[68]	1. Scalable. 2. Efficient since it is not based on bilinear pairing. 3. Supports constrained devices. 4. Supports heterogeneity. 5. No certificate management.	Does not solve the key escrow problem.
[54]	1. Scalable due to the hierarchal architecture. 2. No Certification Management.	1. Does not support heterogeneity, constrained devices and mobility. 2. Based on bilinear pairing. 3. Does not solve the key escrow problem.

(*Continued*)

Table 16 Continued

Ref	Pros	Cons
[56]	1. It enables users to access several cloud systems using single account. 2. The use of hierarchical model makes this technique scalable. 3. Solves the key escrow problem using virtual child. 4. Can be applied over multiple domains. 5. No Certification Management.	1. Users and cloud systems have to be registered to the same root broker. 2. All users and clouds information are kept in a single repository at the broker which could become a system bottleneck. 3. Does not support heterogeneity, constrained devices and mobility. 4. Based on bilinear pairing.
[69]	1. Solves the key escrow problem using partial key generation. 2. No Certification Management. 3. Supports constrained devices.	1. Based on bilinear pairing. 2. Uses central key generation center

Table 17 A comparison between IBE authentication methods according to authentication process characteristics

Ref	Mutual Authentication	Registration Phase	Offline Phase	Additional Hardware	Multiple Credentials	Direct or Indirect Authentication
[64]	√	√				Direct
[65]						Direct
[66]	√		√			Direct
[67]		√	√			Direct
[68]		√				Direct
[54]	√					Direct
[56]		√				Direct
[69]	√	√				Indirect

Table 18 A comparison between IBE authentication methods according to method architecture.

Ref	Centralized Architecture	Hierarchal Architecture	Decentralized flat Architecture
[64]		√	
[65]	√		
[66]	√		
[67]	√		
[68]	√		
[54]		√	
[56]		√	
[69]	√		

Table 19 A comparison between IBE based authentication methods according to iot challenges support

Ref	Support Scalability	Support Networks Heterogeneity	Support Nodes Heterogeneity	Support Mobility	Support Constrained Devices	Support Multiple Domains
[64]	√	×	×	×	×	×
[65]	√	×	×	√	×	×
[66]	×	×	×	×	√	×
[67]	×	×	×	×	√	×
[68]	√	√	√	×	√	×
[54]	√	×	×	×	×	×
[56]	√	×	×	×	×	√
[69]	×	×	√	√	√	×

Table 20 A comparison between IBE authentication methods according to keys generation and distribution methods

Ref	Identity is used in keys/credentials generation	Keys Generation method	Keys distribution method
[64]	Yes	Bilinear Pairing	Not Mentioned
[65]	Yes	Bilinear Pairing	Secure Channel
[66]	Yes	Bilinear Pairing	Offline-preloaded
[67]	Yes	Bilinear Pairing	Secure Channel
[68]	Yes	Non-Bilinear Pairing	Not Mentioned
[54]	Yes	Bilinear Pairing	Secure Channel
[56]	Yes	Bilinear Pairing	Secure Channel
[69]	Yes	Bilinear Pairing	Not Mentioned

As in IBS schemes most of the IBE schemes are based on bilinear pairing and assume the use of secure channels. Security analysis is listed in Tables 21 and 22 lists the comparison according to performance evaluation.

5 Smartcard-based Authentication Schemes

Several smartcards-based authentication schemes have been proposed in the literature. In this section smartcard-based authentication are discussed and compared. Smartcard based authentication method is different from the previously discussed methods in that it is not based on symmetric or asymmetric keys. Instead, it uses smartcards as users' credentials. User smartcard is

Table 21 A comparison between IBE authentication methods according to security analysis

Ref								
Attacks and Security Analysis	[64]	[65]	[66]	[67]	[68]	[54]	[56]	[69]
MITM Attack	×	×	√	√	×	×	√	√
Impersonation Attack	×	×	×	√	×	×	√	×
Replay Attack	×	×	√	√	×	×	×	√
Eavesdropping Attack	×	×	√	√	×	×	√	√
Correctness Proof	×	×	×	√	√	×	×	√
Chosen Message and ID Attack	×	√	×	×	×	×	×	×
Anonymity	×	×	×	×	×	×	×	√
Privacy	×	×	×	×	×	×	×	√

Table 22 A comparison between IBE authentication methods according to performance evaluation

Ref								
Performance Metrics	[64]	[65]	[66]	[67]	[68]	[54]	[56]	[69]
Time Cost	×	×	×	×	√	×	×	×
Energy Cost	×	×	√	√	×	×	×	√
Computation Cost	×	√	×	×	×	√	×	√
Communication Cost	×	×	×	√	×	√	√	√
Key Size	×	×	×	×	√	×	×	×
Message size	×	×	×	×	×	×	√	×
Storage Cost	×	×	×	×	×	×	×	√

generated by the service provider based on user's ID and password [70, 71]. The following are the main phases in smartcard-based authentication:

1. Registration phase: in which the user registers with the service provider using his password and *ID* to ask the service provider to issue a smartcard for him.
2. Login phase: in which the user inserts his smartcard into a card reader and enters his password and *ID*. The smartcard checks the correctness of the password and sends a login message to the service provider.
3. Authentication phase: on receiving the login message, the service provider checks the validity of the smartcard information and authenticates the user.
4. Session key agreement phase: after success authentication, both service provider and the user agree on a session key for data transmission.
5. Password change phase: in which the user can change his password with/without contacting the service provider.

5.1 Summary of smartcard based schemes

The scheme in [70] is for authentication in multi-server environment in which users can access multiple service provider servers using the same smartcard. Users and service providers should register their identities to the controller server. The controller server is responsible for smartcard generation, user authentication and provider authentication. All authentication procedures must go through the controller server. The main phases are: 1 – initialization and registration phase in which the user sends his ID and password to the trusted controller and then the controller finds the user smartcard and sends it back to the user. Also, in this phase the service provider registers his identity to the controller and the controller finds the provider secret key. 2 – The login phase in which the user enters his smartcard into a reader accompanied with his password and ID. Then, the smartcard checks if the user is legal, i.e. the password is correct for the inserted smartcard, to allow the login process to be completed. 3 – The authentication and key agreement phase, in which the service provider authenticates the user through the controller. Time stamps are used to check the validity of message time delay. At the end of this phase the user verifies both the controller and the service provider and agree on a key. 4 – The password updating phase which allows the user to update his password without the controller help.

The proposed scheme in [71] is based on ECC. In the initialization phase, ECC general parameters are chosen by the authentication server. Next, in the registration phase, user’s smartcard information is calculated based on ECC parameters, the user password, and user ID. Smartcard information is then sent to the user. Finally, mutual authentication is performed using the generated smartcard and user password between the authentication server and the user.

In [72] a user authentication scheme over multiple servers is proposed. Users can access multiple cloud services using the same smartcard. It consists of three phases. In the first phase, the trusted smartcard generator generates the public parameters, selects its master key, and computes its public key. Next, users and service providers register their identities with the smartcard generator. Then, the smartcard generator computes and generates corresponding credentials for them. Afterward, users’ authentication is performed directly between users and service providers without the involvement of the smartcard generator.

The authentication schemes that are proposed in [73] and [74], are based on user bio-metric. In these schemes, users should register their bio-metrics with the WSN base station. The authentication process is performed as follows: firstly, for each sensor, the base station assigns a unique ID and generates a unique master key in the pre-deployment phase. Secondly, in the registration phase, the user securely registers his bio-metric along with his identity and password to the base station. Then, the base station generates a smartcard based on a hashing method applied on the biometric and sends it to the user securely. In the login phase, the user enters his smartcard and bio-metric to a terminal device. If bio-metric information is verified successfully, the smartcard verifies his identity and password. Finally, the base station uses a series of hashing values to authenticate the user.

In [75–77] identity based authentication schemes are proposed. These schemes require users to be registered with the WSN base station to get their smartcards. The authentication process is performed based on user's registered identity and his smartcard.

In [78] another smartcard user authentication scheme is proposed. The method has three parties: the control server which is responsible for other parties' authentication and registration. The service provider server and the users. The user should get his smartcard from the controller during the registration phase. Then he can request for service access from the service provider server using his smartcard. The service provider can accept the request if the controller authenticates the user using the smartcard.

The scheme that is proposed in [79] has three entities: the cloud servers, the users and the Control Server (CS). The authentication should go through the cloud CS to allow user to access cloud servers. It has the following phases: 1 – cloud server registration phase in which a cloud server sends his ID and a random number to the CS. Then, the CS uses a hash function to compute the private key for the cloud server. 2 – User registration phase in which the user chooses an ID, password and two numbers. The CS generates a smartcard to the user and the user uses it in the communication. 3 – In the login phase, the user enters his smartcard to a card reader and enters his password and ID. The smartcard verifies the user and then it allows the communication. 4 – Authentication phase in which mutual authentication is done between the CS, the cloud server, and the user. 5 – In the password change phase, the user can update his password without the CS involvement. 6 – Finally, in identity update phase, the user can update his ID, but the CS should be updated with the new ID too.

In [80] an authentication scheme based on smartcard is proposed for WSNs. The scheme has three entities; users, sensors and the gateway. All users should register to the gateway to get their smartcard. Sensors should

Table 23 Pros and cons of the studied smartcard based authentication methods

Ref	Pros	Cons
[70]	1. Users can access multiple service providers with the same smartcard (if registered with the same controller). 2. Not based on bilinear pairing.	1. Multiple credentials are used. 2. Low scalability due to the centralized architecture. 3. Single point of failure. 4. Need additional hardware. 5. Does not support heterogeneity, constrained devices, and mobility.
[71]	1. Based on ECC not bilinear pairing. 2. Scalable.	1. Multiple credentials are used. 2. Does not support heterogeneity, constrained devices, and mobility.
[72]	1. Users can access multiple service providers with the same smartcard (if registered with the same id provider). 2. Supports constrained devices. 3. Applied over multiple domains.	1. Multiple credentials are used. 2. Low scalability due to the centralized architecture. 3. Single point of failure. 4. Need additional hardware. 5. Does not support heterogeneity. 6. Based on bilinear pairing.
[73]	1. Supports constrained devices. 2. Supports nodes heterogeneity. 3. Not based on bilinear pairing.	1. Multiple credentials are used. 2. Low scalability due to the centralized base station. 3. Single point of failure. 4. Need additional hardware. 5. Does not support network heterogeneity and mobility.
[74]	1. Supports constrained devices. 2. Supports nodes heterogeneity. 3. Not based on bilinear pairing	1. Multiple credentials are used. 2. Low scalability due to the centralized base station. 3. Single point of failure. 4. Need additional hardware. 5. Does not support network heterogeneity and mobility.
[75]	1. Supports constrained devices. 2. Supports nodes heterogeneity. 3. Not based on bilinear pairing	1. Multiple credentials are used. 2. Low scalability due to the centralized gateway. 3. Single point of failure. 4. Does not support network heterogeneity and mobility. 5. Users should update the base station when they change their passwords.

(*Continued*)

Table 23 Continued

Ref	Pros	Cons
[76]	1. Supports constrained devices. 2. Not based on bilinear pairing	1. Multiple credentials are used. 2. Low scalability due to the centralized base station. 3. Single point of failure. 4. Does not support heterogeneity and mobility.
[77]	1. Supports constrained devices. 2. Not based on bilinear pairing	1. Multiple credentials are used. 2. Low scalability due to the centralized gateway. 3. Single point of failure. 4. Does not support heterogeneity and mobility.
[78]	1. Users can access multiple service providers with the same smartcard (if registered with the same controller). 2. Not based on bilinear pairing. 3. Support constrained devices.	1. Multiple credentials are used. 2. Low scalability due to the centralized architecture. 3. Single point of failure. 4. Does not support heterogeneity and mobility
[79]	1. Not based on bilinear pairing. 2. Supports constrained devices.	1. Multiple credentials are used. 2. Low scalability due to the centralized architecture. 3. Single point of failure. 4. Need additional hardware. 5. Does not support heterogeneity and mobility
[80]	1. Not based on bilinear pairing. 2. Supports constrained devices. 3. Supports nodes heterogeneity.	1. Multiple credentials are used. 2. Low scalability due to the centralized architecture. 3. Single point of failure. 4. Need additional hardware. 5. Does not support network heterogeneity and mobility.
[81]	1. Sensor can be in foreign network. 2. Not based on bilinear pairing. 3. Supports constrained devices. 4. Supports scalability since the use of multiple gateways.	1. Multiple credentials are used. 2. Need additional hardware. 3. Does not support heterogeneity and mobility. 4. Users should update their home gateway when they change their passwords.

(*Continued*)

Table 23 Continued

Ref	Pros	Cons
[82]	1. Sensor can be in foreign network. 2. Not based on bilinear pairing. 3. Supports constrained devices. 4. Supports scalability since the use of multiple gateways. 5. The use of bio-hashing which has the advantages of clean separation of the genuine, zero error rate and imposter populations.	1. Multiple credentials are used. 2. Need additional hardware. 3. Does not support heterogeneity and mobility
[83]	1. Suitable for constrained devices. 2. Not based on bilinear pairing. 3. Supports heterogeneity and scalability.	1. Multiple credentials are used. 2. Need additional hardware. 3. Needs certificate management.

also be registered to the gateway to be authenticated. If any user wants to access a sensor node, the sensor authenticates the user through the gateway. Two schemes for multi-gateway sensor networks are proposed in [81] and [82]. The user login to the sensor network using his smartcard, and the home gateway tries to locate the requested sensor in its local network. If home gateway could not locate the sensor locally, it will try to locate it in the foreign network. When the home gateway locates the requested sensor, it performs the authentication between the user, the sensor and the gateway. These schemes are based on simple XOR and hash functions to generate the smartcard and the session key. Another smartcard-based authentication scheme is proposed in [83]. This scheme considers the limited capabilities of IoT devices and is based on ECC.

5.2 Comparison and discussion

The comparison according to the first criterion is illustrated in Table 24. Unlike symmetric and asymmetric key schemes, indirect authentication has been commonly considered. All of the studied smartcard schemes achieved mutual authentication and uses multiple credentials in the authentication process. Moreover, most of the studied smartcard schemes need additional hardware to complete the authentication process. Registration phase is essential in all studied schemes to perform the authentication process.

Table 24 A comparison between Smartcard based authentication methods according to authentication process characteristics

Ref	Mutual Authentication	Registration Phase	Offline Phase	Additional Hardware	Multiple Credentials	Direct or Indirect Authentication
[70]	√	√		√	√	Direct
[71]	√	√			√	Direct
[72]	√	√		√	√	Direct
[73]	√	√		√	√	Indirect
[74]	√	√		√	√	Indirect
[75]	√	√			√	Indirect
[76]	√	√	√		√	Direct
[77]	√	√	√		√	Indirect
[78]	√	√		√	√	Direct
[79]	√	√		√	√	Direct
[80]	√	√	√	√	√	Indirect
[81]	√	√		√	√	Indirect
[82]	√	√	√	√	√	Indirect
[83]	√			√	√	Direct

Table 25 A comparison between smartcard based authentication methods according to method architecture.

Ref	Centralized Architecture	Hierarchal Architecture	Decentralized flat Architecture
[70]	√		
[71]			√
[72]	√		
[73]	√	√	
[74]	√	√	
[75]	√	√	
[76]	√	√	
[77]	√		
[78]	√		
[79]	√		
[80]	√		
[81]	√		
[82]	√		
[83]			√

Table 25 shows the comparison between smartcard-based schemes according to the architecture. All studied schemes, except [71], use centralized architecture due to the use of centralized server to generate the smartcard. In Table 26 the comparison between smartcard-based schemes according to IoT challenges is illustrated. As can be noticed, the most

Table 26 A comparison between smartcard based authentication methods according to IoT challenges support

Ref	Support Scalability	Support Networks Heterogeneity	Support Nodes Heterogeneity	Support Mobility	Support Constrained Devices	Support Multiple Domains
[70]	×	×	×	×	×	×
[71]	√	×	×	×	×	×
[72]	×	×	×	Not mentioned	√	√
[73]	×	×	√	×	√	×
[74]	×	×	√	×	√	×
[75]	×	×	√	×	√	×
[76]	×	×	×	×	√	×
[77]	×	×	×	×	√	×
[78]	×	×	×	×	√	×
[79]	×	×	×	×	√	×
[80]	×	×	√	×	√	×
[81]	√	×	×	×	√	×
[82]	√	×	×	×	√	×
[83]	√	√	×	√	√	√

considered challenge is supporting constrained devices. Other challenges are not widely considered. Table 27 shows the comparison according to keys generation and distribution methods. Different methods are used for key generation, but the most used method is hashing. According to the key distribution methods all of the studied schemes assume the use of secure channel to distribute users' credentials. Finally, Tables 28 and 29 list the comparison according to the security analysis and performance evaluation, respectively.

6 Observations

From the discussed PKC, IBC, and smartcard-based authentication schemes, the following observations can be noticed:

1. Most of the studied PKC, IBS, and IBE based authentication schemes perform direct authentication between entities.
2. The use of a single credential is found in almost all the PKC, IBS, and IBE based authentication schemes.
3. Achieving mutual authentication between entities is not mandatory in asymmetric key based schemes since no symmetric data (such as key) is required to be shared here.

Table 27 A comparison between Smartcard based authentication methods according to keys generation and distribution methods

Ref	Identity is used in keys/credentials generation	Keys Generation method	Keys distribution method
[70]	Yes	Hashing	Secure Channel
[71]	Yes	ECC	Secure Channel
[72]	Yes	Bilinear Pairing	Secure Channel
[73]	Yes	Hashing and XOR	Secure Channel
[74]	Yes	Hashing and XOR	Secure Channel
[75]	Yes	Hashing	Secure Channel
[76]	Yes	ECC	Secure Channel
[77]	Yes	Hashing and XOR	Secure Channel
[78]	Yes	ECC	Secure Channel
[79]	Yes	Hashing	Secure Channel
[80]	Yes	Hashing and XOR	Secure Channel
[81]	Yes	Hashing and XOR	Secure Channel
[82]	Yes	Hashing and XOR	Secure Channel
[83]	No	ECC	Elliptic Curve Dif?e–Hellman

4. The need for certificates and certificate management process increases the overhead of PKC based schemes compared with IBC based schemes.
5. The use of hierarchal architectures provides better scalability compared with other architectures.
6. In PKC based schemes, constrained devices are better supported using ECC since it is more efficient that other PKC schemes such as RSA.
7. In most of the studied IBC based schemes, key escrow problem has not been solved.
8. Although bilinear pairing has complex computation, it has been used in most of the studied IBC based schemes.
9. Networks and nodes heterogeneity are not considered in most of the studied asymmetric key based schemes.
10. Most of the studied asymmetric key based authentication schemes consider a single domain of application.
11. Most of the studied asymmetric key based authentication schemes does not support moving objects.
12. All the studied smartcard-based authentication schemes use multiple credentials for user authentication.
13. All the studied smartcard-based authentication schemes achieve mutual authentication between network entities.

Table 28 A comparison between smartcard based authentication methods according to security analysis

Ref														
Attacks and Security Analysis	[70]	[71]	[72]	[73]	[74]	[75]	[76]	[77]	[78]	[79]	[80]	[81]	[82]	[83]
MITM Attack	×	√	√	√	√	√	√	√	×	×	×	×	×	√
Insider Attack	√	√	×	×	√	√	√	×	×	√	√	√	√	×
Impersonation Attack	×	√	×	√	√	√	√	√	√	√	√	×	√	×
Replay Attack	√	√	√	√	√	√	√	√	√	√	√	×	√	√
Eavesdropping Attack	√	√	√	√	√	√	√	√	×	×	×	×	×	√
Dos Attack	√	×	×	√	×	×	√	√	×	×	√	×	√	×
Forgery attack	√	√	√	×	×	√	√	×	×	×	×	√	×	×
Masquerade Attack	√	×	×	√	√	×	×	×	×	×	×	×	×	×
Untraceable	√	×	√	×	×	×	×	×	×	×	×	×	×	×
Anonymity	√	√	√	×	×	×	×	×	√	√	√	×	√	×
Identity Protection	√	×	×	×	×	×	×	×	×	×	×	×	×	×
Correctness Proof	×	×	√	×	×	×	×	×	×	×	×	×	√	×
Password change/guessing Attack	√	√	√	√	×	√	×	√	×	√	√	√	√	√
Stolen Smartcard Attack	√	×	×	×	√	√	×	√	√	×	√	×	√	√
Key Attack	×	×	×	×	×	×	×	×	×	×	×	√	√	×

Table 29 A comparison between smartcard based authentication methods according to performance evaluation

Ref														
Performance Metrics	[70]	[71]	[72]	[73]	[74]	[75]	[76]	[77]	[78]	[79]	[80]	[81]	[82]	[83]
Time Cost	√	×	√	×	×	×	×	×	×	×	×	√	×	√
Energy Cost	×	×	×	×	×	×	×	√	×	×	×	×	×	×
Computation Cost	×	√	×	√	√	√	√	√	√	√	√	×	√	×
Communication Cost	×	×	×	√	√	×	×	√	×	√	√	×	√	×
Storage	√	×	×	×	×	×	×	×	×	×	×	×	×	×

14. Registration is an essential phase in the authentication process in order to register user information and get credentials.
15. Most of the studied smartcard-based authentication schemes need additional hardware to insert the smartcard.

7 Challenges and Research Recommendations

This section discusses the main object authentication issues and challenges in the context of IoT. Moreover, it provides and discusses some directions to be recommended for future research based on the comparisons that are discussed through this survey. These recommendations could help future researchers in solving IoT challenges in their proposals.

Heterogeneity: IoT consists of billions of connected components, which are called objects or things. These objects could be sensors, actuators, embedded devises, traditional computers, smart phones, and even embedded chips on animals and people. An autonomous system, such as smart home or smart campus, is a system that connects different objects and allows them to communicate according to certain procedures and policies that are specified by the system administration unit. Consequently, autonomous systems are heterogeneous in terms of their components, policies, and procedures [84, 85]. This heterogeneity affects the authentication process since different authentication procedures could be followed to allow for an authenticated communication between these heterogeneous systems.

To support heterogeneity, it is recommended to consider various types of IoT objects and networks in future authentication solutions since diverse nature of IoT components is the main characteristics of IoT. Moreover, multiple domains solutions are recommended since IoT connects large number of varying systems and domains which support application with various needs and services.

Mobility: Mobile objects are objects that moves from one autonomous system to another and exchange their data with these autonomous systems in order to legally access the required resources or services. A mobile object that moves between such heterogeneous autonomous systems would face the problem of having different credentials for each system. This could cause management and performance issues since the mobile object must follow various authentication procedures that could include redundant components and credential data exchange. Consequently, this would affect the performance in terms of increasing the time needed for object authentication as well as increasing the exposure of the object credentials to attackers [86].

According to the comparisons in this survey. little work has been done in the literature that consider indirect and mobile solutions. Consequently, more research efforts are needed to be directed towards end to end solutions. This is recommended in order to support moving objects across multiple networks/systems.

Scalability: Scalability is an issue here since mobile objects can access resources in several autonomous systems and a single system may communicate with many mobile objects. This could cause management overhead that affects the performance of the authentication solution. To support scalability, additional research contributions are needed in proposing authentication solutions that are based on hierarchal architectures. This is recommended since centralized architectures have the disadvantages of single node failure problem and single node bottleneck problem.

Constraints of devices: Resources limitation is one of the major issues to be considered in IoT object authentication. Mobile objects can access several autonomous systems which could increase the overhead of authentication procedures on mobile objects which could be, sensors, embedded devices, and other tiny objects. These objects have limited processing capabilities, memory storage, and power resources [85, 87]. As a result, complex authentication schemes that require high computational power, bandwidth, or storage are not suitable for them.

To support constrained devices and reduce computation overhead, asymmetric key approaches are recommended since these approaches do not require pre-distribution process for key pair and large memory to store all shared keys. In addition to that, the overhead could be reduced by using IBC methods since the overhead of certificates management and revocation is eliminated. For PKC methods it is recommended to use ECC since it is computationally more efficient than other PKC algorithms such as RSA. Moreover, the trend of using non-bilinear solutions, such as the using of hashing and XOR operations, is recommended for better computational overhead reduction.

In summary, to control and facilitate authenticated communication between various IoT heterogeneous components, tackle their resource limitation, and manage the huge amount of transferred data, authentication schemes should consider heterogeneity, mobility, scalability, and the capability of constrained devices in their solutions.

8 Conclusion

Supporting trusted and authenticated communication between IoT objects is a key of successful and wide deployment of services provided over IoT. In this paper a comprehensive survey of IoT object authentication schemes has been conducted to help and guide future researchers in delving into the details of authentication schemes in the context of IoT.

The survey provides a taxonomy of authentication schemes based on the authentication method and the application domain. Moreover, it provides different comparisons between the studied schemes according to six criteria; authentication process characteristics, the underlying architecture, key generation and distribution, supporting IoT challenges, security analysis, and performance evaluation. Finally, the survey highlights the main issues and challenges in IoT object authentication and recommends some research directions for future researchers with regards to survey comparisons.

References

[1] F. Alaba, M. Othman, I. A. Hashem and F. Alotaibib, "Internet of things Security: A Survey," Journal of Network and Computer Applications, vol. 88, pp. 20–28, 2017.

[2] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," in Ninth International Conference on Computational Intelligence and Security, 2013.

[3] W. Almobaideen, M. Allan and M. Saadeh, "Smart Archaeological Tourism: Contention, Convenience and Accessibility in the Context of Cloud-Centric IoT," Mediterranean Archaeology and Archaeometry, vol. 16, no. 1, 2016.

[4] W. Almobaideen, M. Saadeh, N. Al-Anbaki, R. Zaghloul and A. Aladwan, "Geographical Route Selection Based On User Public Transportation and Service Preferences," in 9th International Conference on Next Generation Mobile Apps, Services and Technologies (NGMAST), Cambridge, 2015.

[5] S. Li, L. Da Xu and S. Zhao, "The internet of things: a survey," Information Systems Frontiers, vol. 17, no. 2, p. 243–259, 2015.

[6] H. Saadeh, W. Almobaideen, K. E. Sabri and M. Saadeh, "Hybrid SDN-ICN Architecture Design for the Internet of Things," in Sixth International Conference on Software Defined Systems (SDS), Rome, 2019.

[7] R. Khan, S. U. Khan, R. Zaheer and S. Khan, "Future Internet: The Internet of Things Architecture,Possible Applications and Key Challenges," in 10th International Conference on Frontiers of Information Technology, 2012.

[8] S. Andreev, O. Galinina, A. Pyattaev, M. Gerasimenko, T. Tirronen, J. Torsner, J. Sachs, M. Dohler and Y. Koucheryavy, "Understanding the IoT Connectivity Landscape –A Contemporary M2M Radio Technology Roadmap," Communications Magazine, vol. 53, no. 9, pp. 32–40, 16 September 2015.

[9] Z. Yan, P. Zhang and A. V. Vasilakos, "A survey on trust management for Internet of Things," Journal of Network and Computer Applications, vol. 42, pp. 120–134, 2014.

[10] M. Saadeh, . A. Sleit, M. Qatawneh and . W. Almobaideen, "Authentication Techniques for the Internet of Things: A Survey," in Cybersecurity and Cyberforensics Conference, Amman, Jordan, 2016.

[11] O. Abualghanam, M. Qatawneh and W. Almobaideen, "A Survey of Key Distribution in the Context of Internet of Things," Journal of Theoretical and Applied Information Technology, vol. 97, no. 22, pp. 3217–3241, 2019.

[12] K.. T. Nguyen, M. Laurent and N. Oualha, "Survey on secure communication protocols for the Internet," Ad Hoc Networks, vol. 32, pp. 17–31, September 2015.

[13] Girish and H. Phaneendra , "Identity-Based Cryptography and Comparison with traditional Public key Encryption: A Survey," International Journal of Computer Science and Information Technologies, vol. 5, no. 4, pp. 5521–5525, 2014.

[14] J. Baek, J. Newmarch, R. Safavi-Naini and W. Susilo, "A Survey of Identity-Based Cryptography," in Identification And Authentication Issues In Computing, Melbourne, 2004.

[15] M. C. Gorantla, R. Gangishetti and . A. Saxena, "A Survey on ID-Based Cryptographic Primitives," 2005.

[16] S. Zhao, A. Aggarwal, R. Frost and X. Bai, "A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks," IEEE Communications Surveys & Tutorials, vol. 14, no. 2, pp. 380–400, 24 March 2011.

[17] A. Tripathi and K. Burse, "Identity based Signcryption and security attacks and prevention- A Survey," International Journal of Engineering and Technical Research, vol. 2, no. 11, pp. 167–169, 14 November 2014.

[18] M. Langute and H. A. Hingoliwala , “Survey: Identity- Based Encryption in Cloud Computing,” International Journal of Science and Research, vol. 4 , no. 12, pp. 862–866, December 2015 .

[19] P. Mahapatra and A. Naveena, “A Survey on Identity Based Batch Verification Scheme for Privacy and Security in VANET,” International Research Journal of Engineering and Technology, vol. 3, no. 4, April 2016.

[20] D. Kalyani and R. Sridevi, “Survey on Identity based and Hierarchical Identity based Encryption Schemes,” International Journal of Computer Applications, vol. 134, no. 14, January 2016.

[21] M. Alizadeh, S. Abolfazli, M. Zamani and S. Baharun, “Authenticationin mobile cloud computing,” Journal of Network and Computer Applications, vol. 61, pp. 59–80, February 2016.

[22] M. A. Ferrag, L. A. Maglaras, H. Janicke and J. Jiang, “Authentication Protocols for Internet of Things: A Comprehensive Survey,” 2016.

[23] S. S. Manvi and S. Tangade, “A survey on authentication schemes in VANETs for secured communication,” Vehicular Communications, vol. 9, pp. 19–30, 2017.

[24] V. Radha and D. H. Reddya, “A Survey on Single Sign-On Techniques,” Procedia Technology, vol. 4, pp. 134—139, 14 June 2012.

[25] T. Limbasiy and N. Doshi, “An analytical study of biometric based remote user authentication schemes using smart cards,” Computers & Electrical Engineering, vol. 59, pp. 305–321, April 2017.

[26] R. Boussada, M. E. Elhdhili and . L. A. Saidane , “Toward Privacy Preserving in IoT E-health Systems: A Key Escrow Identity-based Encryption Scheme,” in 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2018.

[27] M. E. Hellman, “An Overview of Public Key Cryptography,” IEEE Communications Magazine, vol. 40, no. 5, pp. 42–49, 2002.

[28] Digital_signature, “Digital_signature,” wikipedia, 2017. [Online]. Available: https://en.wikipedia.org/wiki/Digital_signature. [Accessed 11 7 2017].

[29] X.509, “X.509,” wikipedia, 2017. [Online]. Available: https://en.wikipedia.org/wiki/X.509. [Accessed 10 7 2017].

[30] F. Chu, R. Zhang, R. Ni and W. Dai, “An Improved Identity Authentication Scheme for Internet of Things in Heterogeneous Networking Environments,” in Network-Based Information Systems, Gwangju, South Korea, 2013.

[31] J. Liu, Y. Xiao and C. L. P. Chen, “Authentication and Access Control in the Internet of Things,” in 32nd International Conference on Distributed Computing Systems Workshops, 2012.

[32] O. Salman , . S. Abdallah , . I. H. Elhajj , . A. Chehab and A. Kayssi , “Identity-Based Authentication Scheme for the Internet of Things,” in Computers and Communication (ISCC), Messina, Italy, 2016.

[33] A. K. Ranjan and . M. Hussain, “Terminal Authentication in M2M Communications in the Context of Internet of Things,” in Twelfth International Multi-Conference on Information Processing, 2016.

[34] S. Kalra and S. K. Sood, “Secure authentication scheme for IoT and cloud servers,” PervasiveandMobileComputing, vol. 24, pp. 210–223, December 2015.

[35] C.-C. Chang, H.-L. Wu and C.-Y. Sun, “Noteson“Secure authentication scheme for IoT and cloud servers”,” Pervasive and Mobile Computing, vol. 38, pp. 275–278, July 2017.

[36] L. Zhang, S. Tang and H. Luo, “Elliptic Curve Cryptography-Based Authentication with Identity Protection for Smart Grids,” 23 March 2016.

[37] F. N. Mohades and M. H. Y. Moghadam, “An ECC-Based Mutual Authentication Scheme with One Time Signature (OTS) in Advanced Metering Infrastructure,” Amirkabir International Journal of Science & Research (Modeling, Identification, Simulation & Control) AIJ-MISC)) , vol. 46, no. 1, pp. 31–44, 2014.

[38] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally and Y. Begriche, “A Lightweight ECC-Based Authentication Scheme for Internet of Things (IoT),” IEEE SYSTEMS JOURNAL, pp. 1–11, 2020.

[39] Y. Yilmaz and B. Halak , “A Two-Flights Mutual Authentication forEnergyConstrained IoT Devices,” in 4th InternationalVeri?cationandSecurity Workshop (IVSW), 2019.

[40] F. F. Moghaddam, S. G. Moghaddam and S. Rouzbeh, “A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments,” in Region 10 Symposium, 2014.

[41] C. Powell, T. Aizawa and M. Munetomo, “Design of an SSO Authentication Infrastructure for Heterogeneous Inter-cloud Environments,” in 3ed international conference on cloud networking (CloudNet), 2014.

[42] N. Lincke, N. Kuntze and C. Rudolph, “Distributed Security Management for the IoT,” in IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, 2015.

[43] A. Tewari and B. B. Gupta, “A Robust Anonymity Preserving Authentication Protocol for IoT Devices,” in IEEE International Conference on Consumer Electronics (ICCE), 2018.

[44] A. Shamir, “Identity-based cryptosystems and signature schemes,” In Advances in Cryptology CRYPTO ’84, of LNCS, vol. 196, pp. 47–53, 1984.

[45] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” SIAM J. of Computing,, vol. 32, no. 3, pp. 586–615, 2003.

[46] D. He, N. Kumar, K.-K. R. Choo and W. Wu, “Ef?cient Hierarchical Identity-Based Signature With Batch Verification for Automatic Dependent Surveillance-Broadcast System,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 2, pp. 454–464, 2017.

[47] Y. Zhang, . L. Yang and . S. Wang , “An Efficient Identity-Based Signature Scheme for Vehicular Communications,” in Computational Intelligence and Security (CIS), Shenzhen, China, 2015.

[48] X. Hu, . Y. Yang, Y. Liu, J. Wang and X. Xiong, “A Highly Ef?cient and Identity-Based Proxy Signature Scheme without Random Oracle,” in Information Technology and Electronic Commerce, Dalian, China, 214.

[49] L. Ma, “Two Efficient Identity Based Signature Schemes,” in Emerging Intelligent Data and Web Technologies, Xi’an, China, 2013.

[50] F. Li, D. Zhong and . T. Takagi, “Practical Identity-Based Signature for Wireless Sensor Networks,” Wireless Communications Letters, vol. 1, no. 6, pp. 637–640, December 2012.

[51] P. Gopal, . P. V. Reddy and T. Gowri, “New identity based signature scheme using bilinear pairings over elliptic curves,” in Advance Computing Conference, Ghaziabad, India, 2013.

[52] X. Fei, Y. Zhu and X. Luo, “Efficient Identity-Based Signature Scheme in the Standard Model,” in Advanced Computer Theory and Engineering, Chengdu, China, 2010.

[53] L. Bao-juan and S. Shao-bo , “Identity based Signatures Schemes,” in Communication Software and Networks, Xi’an, China, 2011.

[54] H. Li, Y. Dai, L. Tian and H. Yang, “Identity-Based Authentication for Cloud Computing,” in IEEE International Conference on Cloud Computing, 2009.

[55] L. Yan, C. Rong and G. Zhao, “Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography,” in IEEE International Conference on Cloud Computing, 2009.

[56] A. Qousini, “Role-Based Access Control Model for Privacy Preservation in Cloud Computing Environment,” The University of Jordan, Amman, 2015.

[57] C. Wang , “An Ef?cient Fuzzy Identity-based Signature Scheme with out Bilinear Pairings,” in Computational Intelligence and Security, Kunming, China, 2014.

[58] J. Baek , Y.-j. Byon, E. Hableel and M. Al-Qutayri , “An Authentication Framework for Automatic Dependent Surveillance-Broadcast Based on Online/Offline Identity-Based Signature,” in P2P, Parallel, Grid, Cloud and Internet Computing, COMPIEGNE, France, France, 2013.

[59] R. Yasmin, E. Ritter and G. Wang , “An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures,” in Computer and Information Technology , Bradford, UK, 2010.

[60] S. H. Islam and . G. Biswas, “A pairing-free identity-based two-party authenticated key agreement protocol for secure and efficient communication,” Journal of King Saud University–Computer and Information Sciences, vol. 29, no. 1, pp. 63–73, January 2017.

[61] T. Markmann, T. C. Schmidt and M. Wählisch, “Federated End-to-End Authentication for the Constrained Internet of Things Using IBC and ECC,” in Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication, London, United Kingdom, 2015.

[62] J. Zhang, W. Bai and Y. Wang, “Non-Interactive ID-Based Proxy Re-Signature Scheme for IoT Based on Mobile Edge Computing,” IEEE Access, vol. 7, pp. 37865–37875, 2019.

[63] J. Qiu , K. Fan, K. Zhan, Q. Pan, H. Li and Y. Yan, “An Efficient Multi-Message and Multi-Receiver Signcryption Scheme for Heterogeneous Smart Mobile IoT,” IEEE Access, vol. 7, pp. 180205–180217, 2019.

[64] A. Goel , G. Gupta , M. Bhushan and N. Nirwal, “Identity Management in Hybrid Cloud,” in Green Computing and Internet of Things, Noida, India, 2015.

[65] Y.-M. Tseng, T.-T. Tsai , S.-S. Huang and C.-P. Huang, “Identity-Based Encryption with Cloud Revocation Authority and Its Applications,” IEEE Transactions on Cloud Computing, vol. PP, no. 99, 10 March 2016.

[66] R. Rosli, Y. Yusoff and H. Hashim, “Performance Analysis of ID-Based Authentication On Zigbee Transceiver,” in IEEE symposium on Wireless Technology and Applications (ISWTA), Bandung, Indonesia, 2012.

[67] Y. Yussoff, H. Hashim and M. Baba, "Identity-based Trusted Authentication in Wireless Sensor Network," International Journal of Computer Science Issues (IJCSI), vol. 9, no. 3, p. 230, 2012.

[68] V. L. Shivraj , M. A. Rajan , M. Singh and P. Balamuralidhar, "One Time Password Authentication Scheme based on Elliptic Curves for Internet of Things (IoT)," in The 5th IEEE National Symposium on Information Technology: Towards Smart World, Riyadh, Saudi Arabia, 2015.

[69] R. Boussada, M. E. Elhdhili and L. A. Saidane, "Toward Privacy Preserving in IoT E-health Systems: A Key Escrow Identity-based Encryption Scheme," in 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2018.

[70] K. Xue, P. Hong and C. Ma, "A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture," Journal of Computer and System Sciences, vol. 80, no. 1, pp. 195–206, February 2014.

[71] T.-H. Chen, H.-l. Yeh and W.-K. Shih, "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing," in Fifth FTRA International Conference on Multimedia and Ubiquitous Engineering, 2011.

[72] J.-L. Tsai and N.-W. Lo, "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services," IEEE Systems Journal, vol. 9, no. 3, pp. 805–815, 2015.

[73] A. K. Das and B. Bruhadeshwar, "A Biometric-Based User Authentication Scheme for Heterogeneous Wireless Sensor Networks," in 27th International Conference on Advanced Information Networking and Applications Workshops, 2013.

[74] M. Sarvabhatla and C. S. Vorugunti, "A Secure Biometric-Based User Authentication Scheme for Heterogeneous WSN," in Fourth International Conference of Emerging Applications of Information Technology, 2014.

[75] H.-R. Tseng, R.-H. Jan and W. Yang, "A Robust Password-based Authentication Scheme for Heterogeneous Sensor Networks," Communications of IICM, vol. 11, no. 3, pp. 1–13, 2008.

[76] A. Mnif, O. CheIkhrouhou and M. B. JEMAA, "An ID-based User Authentication Scheme for Wireless Sensor Networks using ECC," in International Conference on Microelectronics (ICM), Hammamet, 2011.

[77] M. Sarvabhatla, L. Kodavali and C. vorugunti, "An Energy Efficient Temporal Credential Based Mutual Authentication Scheme for WSN,"

in 3rd International Conference on Eco-friendly Computing and Communication Systems, 2014.

[78] X. Li, Y. Xiong and W. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smartcards," Journal of Network and Computer Applications, vol. 35, no. 2, pp. 763–769, March 2012.

[79] R. Amin, N. Kumar, G. Biswas, R. Iqbal and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment," Future Generation Computer Systems, pp. 1–27, 29 December 2016.

[80] M. Turkanović, B. Brumen and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," Ad Hoc Networks, vol. 20, pp. 96–112, September 2014.

[81] F. Wu, . L. Xu, S. Kumari, . X. Li, J. Shen, . K.-K. R. Choo, . M. Wazid and . A. K. Das, "An e?cient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment," Journal of Network and Computer Applications, vol. 89, pp. 72–85, July 2017.

[82] J. Srinivas, S. Mukhopadhyay and . D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," Ad Hoc Networks, vol. 54, pp. 147–169, January 2017.

[83] M. A. Gurabi, O. Alfandi, A. Bochem and D. Hogrefe , "Hardware based Two-Factor User Authentication for the Internet of Things," in 14th International Wireless Communications & Mobile Computing Conference (IWCMC), 2018.

[84] S. Park , N. Crespi, H. Park and S.-H. Kim, "IoT Routing Architecture with Autonomous Systems of Things," in IEEE World Forum on Internet of Things (WF-IoT), 2014.

[85] M. I. Hussain, "Internet of Things: challenges and research opportunities," CSI Transactions on ICT, vol. 5, no. 1, pp. 87–95, march 2017.

[86] K. Nahrstedt, H. Li, P. Nguyen, S. Chang and L. Vu, "Internet of Mobile Things: Mobility-Driven Challenges, Designs and Implementations," in IEEE First International Conference on Internet-of-Things Design and Implementation, 2016.

[87] J. Granjal, E. Monteiro and J. Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015. W364W9791

Biographies

Maha Saadeh received her Ph.D. degree in computer science from the University of Jordan in January 2018. She worked as a research and teaching assistant at the computer science department, The University of Jordan from September 2009 to September 2010. She is currently working with Middlesex University in Dubai, UAE. She has a number of publications in a number of local and international journals and conferences. Her research interests are wireless networks, network security, and the Internet of Things (IoT).

Azzam Sleit is the Former Minister of Information and Communications Technology (2013–2015). He is currently working as a Professor of Computer Science, King Abdulla II School for Information Technology, University of Jordan, where he functioned as the Dean (2015–2016) and the Assistant President/Director of the Computer Center (2007–2009). Dr. Sleit holds B.Sc, M.Sc. and Ph.D. in Computer Science. He received his Ph.D. in 1995 from Wayne State University, Michigan. Dr. Sleit was the Chief Information Officer at Hamad Medical/Ministry of Public Health, Qatar. Before joining Hamad Medical, Dr. Sleit was the Vice President of Strategic Group & Director of Professional Services of Triada, USA, where he introduced the NGram Technology and Associative Memory Structures. Dr. Sleit authored more than one hundred refereed research papers related to Cloud

Computing, Imaging Databases, Data Mining, Health and Management Information Systems and Software Engineering, published in reputable journals and conferences.

Khair Eddin Sabri is a professor in the Computer Science Department at The University of Jordan. He obtained his B.Sc. degree in Computer Science from the Applied Science University, Jordan in June 2001. He also received M.Sc. degree in Computer Science from The University of Jordan in January 2004 and a Ph.D. degree in Software Engineering from McMaster University, Ontario Canada in June 2010. He is a member of the Formal Requirements and Information Security Enhancement (FRAISE) Research Group. His main research interest is the formal verification and analysis of security properties.

Wesam Almobaideen is a full professor of computer networks and security at Rochester Institute of Technology (RIT) in Dubai. He holds a B.Sc. in computer science from Muta'h University, Karak, Jordan, M.Sc. degree from The University of Jordan, Amman, Jordan, and a Ph.D. from Bologna University, Bologna, Italy. Before joining RIT-Dubai, he was chairperson of the Department of Computer Science at the University of Jordan for five years. He has also served as Director of the Computer Center for three years, Assistant Dean of the Faculty of Graduate Studies, and Director of the Accreditation and Quality Assurance Office.

His research interests include Wireless Networks, Computer security and Cybersecurity, Internet of Things and cloud Computing. He has published more than 50 research papers in reputable conferences and journals and has supervised over 40 graduate master and doctorate level students.