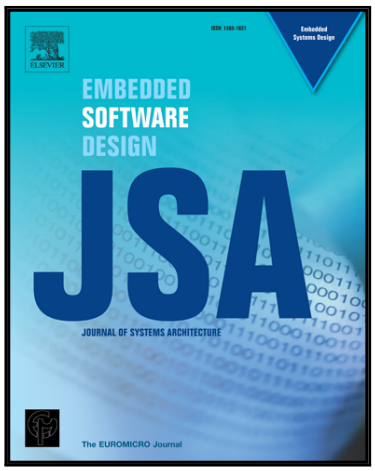

Authentication in cloud-driven IoT-based big data environment: survey and outlook

Mohammad Wazid, Ashok Kumar Das, Rasheed Hussain, Giancarlo Succi, Joel J.P.C. Rodrigues

PII: S1383-7621(18)30361-8
DOI: https://doi.org/10.1016/j.sysarc.2018.12.005
Reference: SYSARC 1547

To appear in: *Journal of Systems Architecture*

Received date: 1 September 2018
Revised date: 11 November 2018
Accepted date: 24 December 2018

Please cite this article as: Mohammad Wazid, Ashok Kumar Das, Rasheed Hussain, Giancarlo Succi, Joel J.P.C. Rodrigues, Authentication in cloud-driven IoT-based big data environment: survey and outlook, *Journal of Systems Architecture* (2018), doi: https://doi.org/10.1016/j.sysarc.2018.12.005

Authentication in cloud-driven IoT-based big data environment: survey and outlook

Mohammad Wazid [a], Ashok Kumar Das [b], Rasheed Hussain [c], Giancarlo Succi [d], Joel J. P. C. Rodrigues [e,*]

[a] *Cyber Security and Networks Lab, Innopolis University, Innopolis 420500, Russian Federation*
E-mail: wazidkec2005@gmail.com
[b] *Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India*
E-mail: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in
[c] *Department of Computer Science, Innopolis University, Innopolis 420500, Russian Federation*
E-mail: r.hussain@innopolis.ru
[d] *Department of Computer Science, Innopolis University, Innopolis 420500, Russian Federation*
E-mail: g.succi@innopolis.ru
[e] *National Institute of Telecommunications (Inatel), Brazil; Instituto de Telecomunicações, Portugal; University of Fortaleza (UNIFOR), Brazil*
E-mail: joeljr@ieee.org
[*] *Corresponding author*

Abstract

The Internet of Things (IoT) is composed of different networked objects (i.e., smart devices) which are interconnected to gather, process, refine, and exchange meaningful data over the Internet. These objects are assigned to their respective IP addresses, and they are able to send and receive data over a network without any human assistance. IoT offers different types of applications, such as, but not limited to, smart traffic monitoring, smart home, smart health care and smart cities, to name a few. In a Cyber-Physical System (CPS), computing elements coordinate and communicate with sensor devices, which monitor cyber and physical indicators, and actuators, and also modify the cyber and physical environment where they run. The synergy of computational as well as physical components, specifically the use of CPSs, led to the advancement of IoT implementations. In a cloud-driven IoT-based big data environment, a cloud-based platform is used to store the data generated by IoT devices (normally by sensor devices) which further can be considered as a big data warehouse. This environment is highly scalable and provides important real-time event processing (for example, in critical scenarios like surveillance and monitoring of an industrial plant). In IoT-based critical applications, the real-time data access is obligatory as and when it is required. Such access is possible if we permit only authorized external users to access the real-time data directly from the IoT sensors. Sometimes authorized user may also request for big data query processing and big data analytics over the data stored in cloud servers to figure out hidden patterns of some phenomena (i.e., chances of fire in an industrial plant in future). Therefore, we need secure authentication schemes for cloud-driven IoT-based big data environment in which a legitimate user and an IoT sensor can mutually authenticate each other and establish a common session key for secure communication. In this context, this paper first discusses the network and threat models of the authentication schemes for cloud-driven IoT-based big data environment. Some security requirements, issues and challenges of this environment are then discussed. A taxonomy of various existing authentication schemes applicable for cloud-driven IoT-based big data environment is also discussed, which covers a comparative study of these schemes. We identify and briefly discuss some future research challenges in designing the authentication schemes and other security protocols for cloud-driven IoT-based big data environment that need to be addressed in the future.

Keywords: Internet of Things (IoT), Cyber-Physical System (CPS), cloud computing, big data, authentication, key agreement, security.

1. Introduction

Information and Communications Technology (ICT) evolves a new kind of communication environment, Internet of Things (IoT). IoT objects have ability to collect and transfer data over a network without any human assistance. A typical scenario of a generic IoT environment is given in Figure 1. In this environment, there are different scenarios, such as home, transport and community. These scenarios consist of several smart devices, such as sensors, actuators, smart toys, and electronic products [1], [2], [3]. All these smart devices are connected to the Internet through the gateway node. Various users, such as smart home users and doctors, and users of industrial data, can access the real-time data from the designated specified IoT devices through the gateway node(s) [2], [4].

In a Cyber-Physical System (CPS), computing elements coordinate and communicate with sensor devices, which monitor cyber and physical indicators, and actuators, and also modify the cyber and physical environment where they run. The synergy of computational as well as physical components, specifically the use of CPSs, led to the advancement of IoT implementations [5]. IoT is poised to provide consumers with dependable, responsive, and ingenious network connectivity which then can provide real-time control over the remote IoT

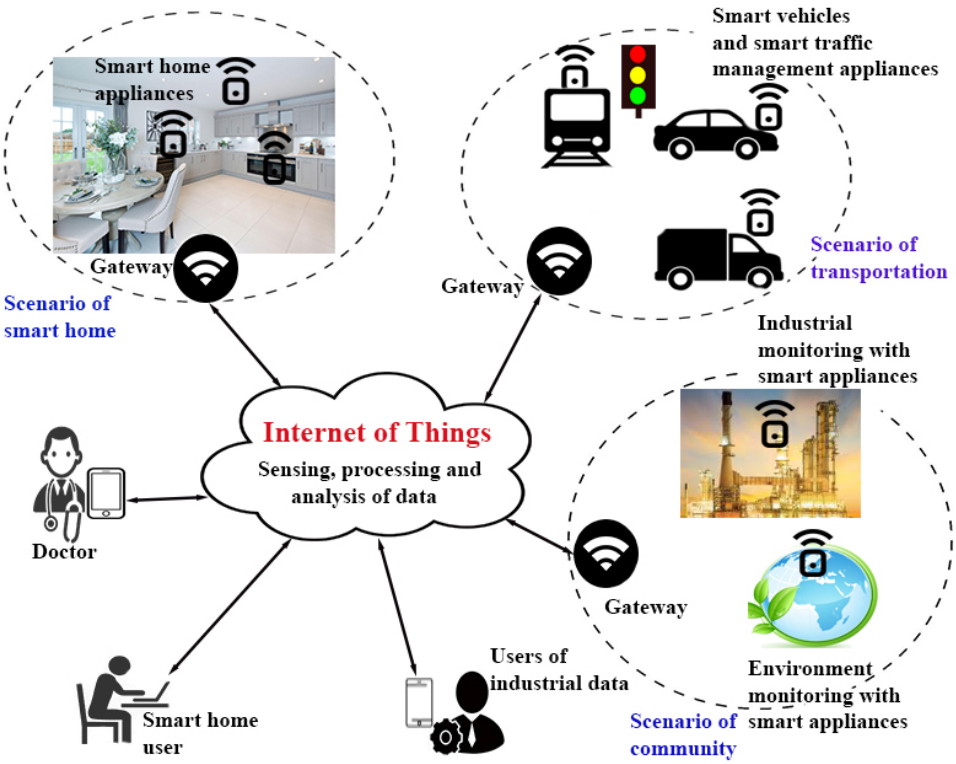

Figure 1: A generic IoT environment (Adapted from [2])

sensors. IoT networks offer plethora of different types of applications in different domains, such as smart infrastructure, health-care, critical infrastructure and intelligent transportation system, to name a few [2], [6], [7]. Depending on the underlying application, IoT devices produce massive data that needs to be stored, processed, analyzed, and visualized. Traditional storage and computing platforms may not handle the volume, velocity, and variety of data produced by IoT devices. Therefore, it is imperative to leverage other available mechanisms. To this end, cloud computing is the most viable option to store and process the massive scale data produced by IoT environment. In other words, cloud computing provides a pathway (i.e., platform, infrastructure and software tools) for this data to produce meaningful output depending on the underlying application. Cloud computing and IoT have a complementary relationship and both serve to increase efficiency in our day-to-day tasks. Other advantage of cloud computing for IoT is that it enables better collaboration which is essential for developers today. By allowing developers to store and access data remotely, developers can access data immediately and work on projects without delay.

1.1. Advantages of cloud-driven IoT

Cloud-driven IoT has several advantages over a generic IoT architecture. Using this architecture, we can process the queries in real-time with reduced communication cost that can further reduce the processing overhead [8]. In the following, we outline several other advantages of cloud-driven IoT over the traditional IoT.

1.1.1. Role of big data

As aforementioned, cloud is the suitable platform for offloading the data produced by IoT devices for storing and further processing. The fact that IoT data can be rendered as big data, advocates for using cloud computing environment to handle IoT-generated big data. The role of cloud-driven IoT-based big data environment is given below [9], [10], [11]:

- In an IoT environment, the data generated by smart IoT devices may experience an exponential growth with time.
- Eventually, we may collect exabytes of data which needs to be processed efficiently and logically in order to make the right decisions.
- Conventional methods for data processing, storage systems, data warehouses and relational databases provide limited support to the analysis of the data generated by smart IoT devices.
- Traditional methods are costly when dealing with massive amount of data.
- Most importantly, traditional methods are not able to provide efficient processing speed which is pivotal for the real-time processing where smart IoT devices are deployed in a deployement field (e.g., in fire detection in an industrial plant).
- New tools and techniques capable of storing and processing huge amount of data, are essential for IoT.
- Such tools and techniques facilitate streamlining the capturing as well as providing support for processing, stor-

age, transfer, searching, analysis and visualization of huge amount of data generated by smart IoT devices.

In a cloud-driven IoT-based environment, cloud based platform is leveraged to store the data produced by IoT sensors which further can be considered as a big data warehouse. This environment is highly scalable and provides real time event processing which is very important in some of the critical scenarios (i.e., surveillance and monitoring of an industrial plant). In IoT-based critical applications, the communicating parties may need access to the real-time data. For such data access, it is required for the external parties (users) to be authorized to access the real-time data directly from the IoT sensors deployed in the network. Once both the user and an accessed IoT sensor mutually authenticate each other, they need to establish a session key. With the help of the established session key, they can securely communicate with each other. Sometimes authorized users may also request for big data processing and big data analytic over the stored data to obtain some results or predictions on the massive data such as chances of fire in an industrial plant in future, and so on.

1.2. Motivation

The requirements of authentication schemes for cloud-driven IoT-based big data environment are as follows. The IoT based applications facilitate day-to-day life of the people. However, the IoT environment is vulnerable to different security and privacy threats as different kinds of attacks, such as leakage of confidential information, replay, man-in-the-middle, impersonation and denial-of-service attacks can be mounted by an adversary. In the presence of such malicious attacks, any unauthorized tasks, such as disclosing of confidential information and denial-of-service to IoT sensors can be performed by the remote malicious users. Such circumstances may cause direct consequences and can also even endanger human lives who use IoT-based applications in their day-to-day lives. Therefore, we need secure authentication schemes for cloud-driven IoT-based big data environment in which a legitimate user and an IoT sensor can mutually authenticate each other, and then can establish a common session key for their secure communication. In addition, the authorized users can access the data from the cloud servers securely after their successful mutual authentication and session key establishment procedure [2], [12], [13]. Therefore, we provide a generalized model for authentication mechanism for cloud-driven IoT-based big data environment. The proposed model will help the researchers in the designing new authentication schemes for cloud-driven IoT-based big data environment.

1.3. Research contributions

The main contributions of this review work presented in this article are summarized below.

- A generalized authentication model for cloud-driven IoT-based big data environment has been proposed.
- We explain the detailed working of authentication procedure that happens among different communicating parties, such as users and IoT sensors with the help of the trusted gateway node(s).
- We then provide a systematic overview of possible security challenges in this domain with respect to limited computation power, memory storage and energy requirement, scalability, mobility, support for heterogeneous devices and dynamic security updates, protection against physical capturing of IoT devices, and also the security and privacy of IoT sensors' data.
- Next, we analyze some state-of-art existing authentication schemes which can be applicable for cloud-driven IoT-based big data environment too.
- Finally, possible future research directions on authentication in cloud-driven IoT-based big data environment are discussed. Some of the future research directions are on the security of authentication schemes, efficiency of authentication schemes, scalability of authentication schemes, privacy of data maintained at big data warehouse, heterogeneity of IoT networks environment as well as privacy-aware authentication.

1.4. Paper outline

The network as well as threat models associated with authentication schemes in cloud-driven IoT-based big data environment are explained in Section 2. Security challenges and issues of authentication schemes in cloud-driven IoT-based big data environment are discussed in Section 3. Taxonomy of the existing authentication schemes for IoT environment is given in Section 4. The future research directions of this area are discussed in Section Section 5. Finally, the paper is concluded in Section 6.

2. System models

The following two models can be used to explain the working as well as the threats associated with authentication schemes for cloud-driven IoT-based big data environment.

2.1. Network model

The network model of an authentication procedure in cloud-driven IoT-based big data environment is given in Figure 2. According to this model, the IoT sensors are deployed in some target fields of the IoT environment, such as fire detection in an industrial plant and health monitoring of a patient with smart implantable medical devices. Suppose a user (i.e., the head of plant rescue team or a doctor) wants to access real-time data from some designated IoT sensors. In such scenarios, user and IoT sensor need to mutually authenticate each other. After mutual authentication, both user and IoT sensor agree on a secret session key. Later, they use this established session key for securing their future communication. Note that user and IoT sensor communicate through a gateway node which is connected to the Internet. In such environment, entire data which is sensed and processed by IoT sensors need to be stored

securely to the cloud servers. Cloud servers create a data warehouse for the incoming data from IoT. To draw conclusions from this big data, we need big data query processing and analytic mechanism. After analyzing the reports of big data analytic procedure, the application and/or user can take decision accordingly (i.e., chances of getting fire in the industrial plant). There is also a trusted authority which generates the required credentials for IoT sensors, cloud servers and gateway node and then stores the credentials in its memory prior to their deployment in the network. Users are required to register with the trusted authority before accessing the real-time data from the IoT sensors and cloud server. This registration is carried out through a secure channel (or in person) [2], [14], [15].

2.2. Threat model

For an authentication scheme in cloud-driven IoT-based big data environment, we can follow the widely-accepted Dolev-Yao (DY) threat model [16]. In the DY model, the communicating parties communicate over an insure channel. Since the communication channel is public, therefore communicating end-point parties like user, IoT sensors, cloud servers are not, in general, trustworthy. An adversary $\mathcal{A}$ can have the chance to eavesdrop the exchanged messages. $\mathcal{A}$ is also able to delete or modify the transmitted messages. We utilize the widely-accepted Canetti and Krawczyk's adversary model, known as the CK-adversary model [17], [18] which is treated as the current *de facto* standard model in modeling an authenticated key-agreement security protocol. Under the CK-adversary model, $\mathcal{A}$ has the capabilities as in the DY model, and in addition, he/she may compromise of the secret credentials as well as the session states & session keys in the sessions. Furthermore, $\mathcal{A}$ can physical capture some IoT sensors or smart sensing devices to obtain the stored credentials in those devices with the help of sophisticated power analysis attacks [19]. In addition, the mobile device or smart phone or smart card of a legal registered user can be lost or stolen. As a result, the secret credentials stored in the mobile device or smart phone can be also extracted by an adversary. The extracted data can be then used in other related unauthorized tasks, such as session key computation, smart sensing device impersonation attack, replay attack, man-in-the-middle attack and privileged-insider attack. Finally, the gateway node needs to be a semi-trusted entity in the network, which can be deployed in a physical locking system as suggested in [20]. If $\mathcal{A}$ gets authorized access to the cloud servers, he/she can also use the stored data at the cloud servers for malicious objectives.

3. Security issues and challenges of authentication schemes for cloud-driven IoT-based big data environment

Society is adopting IoT-based applications and technologies which further facilitate and add value to their day-to-day life. The cloud-driven IoT-based big data technology can be used in various applications such as to store vital private information of patient's health care data. Moreover, the Internet connected smart devices can be utilized in various applications, such as industrial plant monitoring and control, controlling home appliances remotely, elderly people health monitoring and support because these devices can be accessed anytime from anywhere. Just like other technology domain, this domain also has several issues and challenges as the Internet connected smart devices (i.e., IoT sensors) are vulnerable to various attacks which are the soft target for the existing network attackers. The security issues and challenges of authentication schemes for cloud-driven IoT-based big data environment are discussed below [8], [12], [21].

3.1. Security requirements

Following are the security requirements of cloud-driven IoT-based big data environment [21], [22].

- **Confidentiality:** This property ensures the protection of data which is generated by IoT sensor and stored in the cloud-servers at the big data warehouse from any kind of unauthorized access and disclosure.
- **Integrity:** This property ensures that the data which is generated and sent by IoT sensors should not be altered in transit by the existing adversary. Moreover, the integrity of the data maintained at big data warehouse and content should not be compromised.
- **Authentication:** This property enables the IoT devices, such as IoT sensors, users, and cloud servers, to verify the validity of the identity of the peer with which they are communicating.
- **Availability:** This property ensures the availability of various IoT devices, such as IoT sensors and cloud server, to authorized parties when it is required. There should be assurance against any kind of denial-of-service attack.
- **Data freshness:** This property ensures the freshness of the data which is sent by the IoT devices, such as IoT sensors. The cloud-driven IoT-based big data environment also has time varying features. Therefore, there is a great need that ensures each received message should be fresh. Data freshness basically entails that each data set is recent and ensures that no adversary replays with the old messages.
- **Non-repudiation:** This property indicates that a communicating party, such as an IoT sensor cannot deny sending of a message which was sent earlier.
- **Authorization:** This property ensures that only authorized communicating parties are authorized to access and avail the services of the various resources.
- **Resilience against sensing device capture attack:** If some of the interconnected IoT devices are compromised, there should be some security mechanism to protect other non-compromised devices and network resources. For example, if an IoT sensor is physically captured by an adversary, he/she can obtain the secret credentials stored in the memory of this IoT sensor [19]. In this case, the adversary gets information about the session key which was

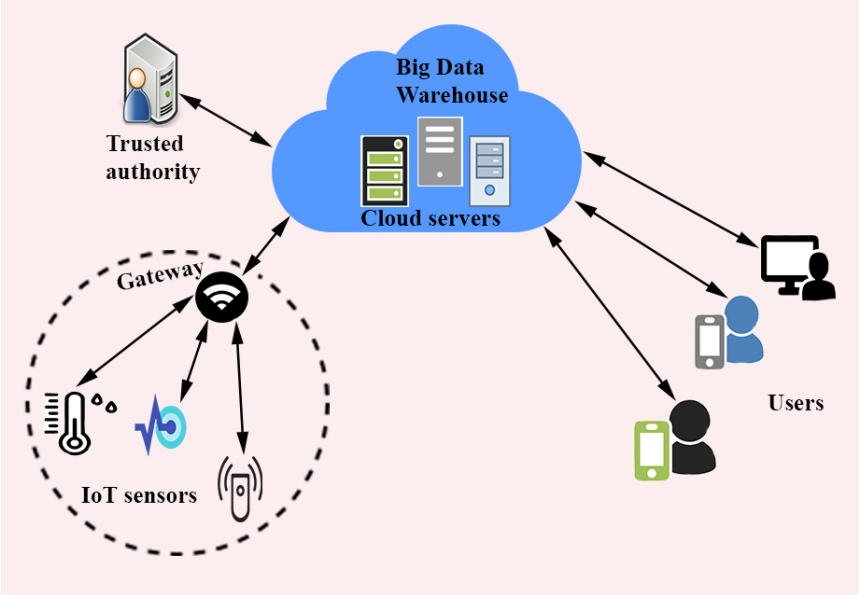

Figure 2: An authentication model for cloud-driven IoT-based big data environment (Adapted from [2], [14])

established between this IoT sensor and a user.The compromising of this IoT sensor should not affect the security of the other part of the network, that is, we should design a key management scheme or (user) authentication scheme is such a way that the physical compromise of some IoT sensors should not affect the secure communication among the non-compromised sensors and also among a user and non-compromised sensors.

- **Unbreakable service:** The smart devices, such as IoT sensors, in the cloud-driven IoT-based big data environment may be failed due to energy issue or can be physically stolen by the adversary. In these circumstances we should have strong deployed mechanism which can provide the service without any discontinuation.

3.2. Security issues and challenges

In the above part of this section we have discussed about the security requirements of cloud-driven IoT-based big data environment. These security requirements need to be considered while design of an authentication scheme for such an environment. Some identified issues and challenges include limited computation power and memory storage, energy requirement, scalability, mobility, support for heterogeneous devices, dynamic security updates, protection against physical capturing, and security and privacy of IoT sensors data at the big data warehouse. In the following part of this section, we discuss about the security issues and challenges in the cloud-driven IoT-based big data environment [13], [20], [21], [22], [23].

- **Limited computation power and memory storage:** In a cloud-driven IoT-based big data environment, IoT devices, such as IoT sensors are equipped with low-speed processors and limited memory storage. The processing capability of these devices is not that powerful in terms of speed. Moreover, these devices are not capable to perform computationally expensive operations which require high computational power with high memory storage. Hence, designing of a security solution which minimizes resource consumption (computation as well as memory storage) with maximum security performance becomes challenging. Therefore, while design user authentication schemes for such an environment we prefer to use light weight cryptographic operations (for example, Advanced Encryption Standard (AES) algorithm [24] and cryptographic one-way hash function [25] can be utilized) [20].

- **Energy requirement:** In the given environment there are resource contained smart devices, such as IoT sensors with limited battery backup. These devices automatically try to save the energy by switching on the power saving mode when no activity needs to be reported. Therefore, due to the battery backup limitations it becomes very challenging to design a security solution which provide the high level of security. Therefore, while design user authentication schemes for such an environment, the light weight cryptographic operations, such as AES algorithm and cryptography one-way hash function are preferable [20], [24], [25], [26].

- **Scalability:** In a cloud-driven IoT-based big data environment, the number of IoT devices increases gradually. More number of devices are getting connected to the network everyday. Therefore, while design an authentication scheme for such an environment we always provide this functionality, such as smart sensing device addition phase [20], [26] without compromising the security requirements.

- **Mobility:** In a cloud-driven IoT-based big data environment some of the devices are mobile in nature for example there is a human being using some wearable sensing device which monitors his/her temperature and sends that to the health big data warehouse which maintained using the cloud servers. Such IoT device are connected to the home

network when that user is at home, whereas they are connected different network when he/she at some other location (i.e., office network). Different networks use different security configuration and settings. Therefore, developing a mobility-compliant security technique becomes challenging [21].

- **Support for heterogeneous devices:** In a cloud-driven IoT-based big data environment, we use different types of devices, such as IoT sensor, personal digital assistant, smartphone, and RFID tags. These devices have different capability in terms of their computation, power, memory, and embedded software. Therefore, the challenge lies in designing an authentication scheme which can support all types of devices [21], [27].

- **Dynamic security updates:** To overcome the security vulnerabilities in the existing schemes, there is a requirement to keep security schemes up-to-date, for example, in case of new smart device addition or device revocation, other network entities will also be informed by the trusted authority so that they can update this in their memory [20], [26]. Therefore, designing of such a scheme which supports dynamic installation or update without compromising the security is also a challenging task [21].

- **Protection against physical capturing:** In a cloud-driven IoT-based big data environment there are the chances that some of the smart devices, such as IoT sensors, may be physically stolen by the adversary. Further adversary can use power analysis attack [19] to extract the information from the memory of IoT sensor then this extracted information can be utilized in other malicious task such as user's password computation, session key computation. Adversary can also clone and replace this device with its malicious device. Tamper-resistant packaging is a way to defend against such attacks [21]. We should also design the authentication scheme in such a way that if some of the smart IoT devices are stolen then that should not affect the security of the communication happens in the remaining part of network [20], [26], [28].

- **Security and privacy of IoT sensors data at the big data warehouse:** The organization can use the data of IoT sensors which is stored at big data warehouse for different kinds of analysis (for example, the chances of fire in an industrial plant in future with possible causes). Such kinds of exposure of data also involve big risks when it comes to security and privacy of the data. Thus, it becomes very important for analysts to consider these issues and deal with the data in such a manner that it will not lead to disruption of privacy [8].

4. Analysis of existing authentication schemes for IoT environment

In the following part of this section, we provide the summary of the different existing authentication schemes related to the IoT environment. After that we perform a comparative study among the state-of-art authentication schemes.

4.1. Review of authentication schemes

A user authentication scheme in the IoT environment has typically the following phases [29]:

- *System setup:* In this phase, the system parameters are picked by the gateway node.

- *Sensing node/IoT sensor registration:* Before the sensing nodes are deployed or installed, they need to be registered with the gateway node. The gateway node then stores the essential secret credentials before deployment of the IoT sensors.

- *User registration:* In order to access information (service) from particular sensing nodes, a user requires to register with the gateway node. The user first inputs his/her credentials (e.g., identity, password and biometrics) secretly to the gateway node and the gateway node issues a smart card or mobile device securely to the user.

- *Login:* In this phase, the user inputs his/her credentials, and these are then verified by the smart card (mobile device). After successful validation of credentials, a login request message is formed and sent to the gateway node via public channel.

- *Authentication and key agreement:* After receiving the login request, the gateway node first validates it and if the verification passes, the gateway node completes this with an authentication request message to the sensing node being accessed. Sensing node then validates the received message and sends the authentication reply to user. User also verifies the received message from the sensing node. Only after mutual authentication between user and sensing node, a session key is established between them. Later, both entities use the session key for secure communication.

- *Password & biometric update:* This phase is needed only when an authorized registered user wants to update his/her password and biometrics. It is desirable that the user should not involve the gateway node for this activity and hence, this phase can be fully completed locally without the involvement of the gateway node by that user.

- *Smart card (mobile device) revocation:* If the smart card (mobile device) is lost or stolen by an adversary, a user authentication scheme should permit the revocation phase in order to issue a new smart card (mobile device) with a new set of credentials stored into it.

- *Dynamic sensing node addition:* This phase is required when some sensing nodes are physically captured by an adversary or some sensing nodes are exhausted because of a power failure (if the sensing devices are battery powered).

Depending on the number of factors applied in a user authentication scheme, it is called a single-factor or a multi-factor scheme. If only the user password is used, a user authentication scheme is known as single-factor scheme. If a smart card (mobile device) along with a user password are applied, it is

known as a two-factor scheme, and if smart card (mobile device), user password and biometrics are all used, it is called a three-factor scheme [29].

Yeh et al. [30] proposed an elliptic curve cryptography (ECC) based user authentication scheme in wireless sensor networks (WSNs). However, their scheme does not provide mutual authentication.

The network model of the scheme of Yeh et al. [30] is given in Figure 3. In this model, a user starts the communication by successfully login into the system. User sends authentication request message to gateway node. After receiving message from user, gateway node verifies the authenticity of the user. If it verifies successfully then user is authenticated with gateway node. Gateway node further computes other variables and sends authentication request to the sensor node. After receiving message from the gateway node, sensor node verifies the authenticity of the gateway node and if the verification is successful, it sends an authentication reply message to the gateway node. After the successful completion of login and authentication phases of this scheme both user and sensor node establish a secret session key for their future secure communication.

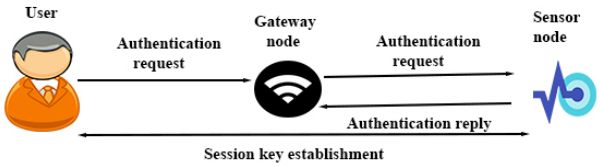

Figure 3: Network model used in [30]

Turkanovic et al. [31] designed a user authentication and key agreement scheme for heterogeneous wireless sensor networks. This enables a remote user to securely negotiate a session key with a general sensor node using a lightweight key agreement protocol. However, this scheme is insecure against offline password guessing, offline identity guessing, smart card theft, user impersonation and sensor node impersonation attacks. Moreover, it does not provide mutual authentication [32].

Farash et al. [33] presented a scheme for user authentication and key establishment for heterogeneous architecture of wireless sensor network which is also applicable for IoT environment. However, later on it is proved in [34] that this scheme suffered from various attacks including password guessing in offline mode by using the lost/stolen smartcard, user impersonation attack and session-specific temporary information leakage attack.

The network model used in the schemes of Turkanovic et al. [31] and Farash et al. [33] is given in Figure 4. In these schemes, a user starts the communication by login into the system and then sends the authentication request to the sensor node. Sensor verifies the request of the user which proves the authenticity of user to the sensor node. Sensor node again sends an authentication request to the gateway node. Gateway node verifies the request of the sensor node. The verification of gateway node proves the authenticity of the sensor node to the gateway node. After this gateway node sends the authentication reply to the sensor node. After receiving authentication reply from gateway node, sensor node verifies the authenticity of the gateway node. If this verification happens successfully then sensor node compute session key and sends authentication reply message to the user. After receiving authentication reply message from sensor node, user also verifies the authenticity of the sensor node. If this verification happens successfully then both user and sensor node establish a secret session key for their future secure communication.

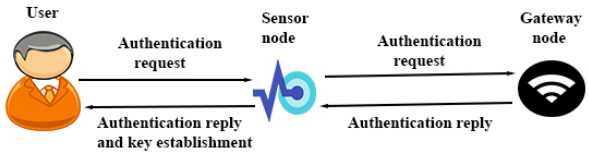

Figure 4: Network model used in [31], [33], [34]

Hsieh and Leu [35] proposed an authentication scheme for wireless sensor networks which can be also applicable for IoT environment. This scheme overcome security drawbacks in [36], [37], [38]. Their scheme is also vulnerable to various attacks, such as insider attack, offline guessing attack, user forgery attack and sensor node physical capture attack [39]. Moreover, this scheme does not provide session key security and also it lacks mutual authentication.

The network model of the scheme of Hsieh and Leu [35] is given in Figure 5. In this model user starts the communication by successfully login into the system. User sends authentication request message to gateway node. After receiving message form user, gateway node verifies the authenticity of the user. If it verifies successfully then user is authenticated with gateway node. Gateway node further computes other variables and sends authentication request to the sensor node. After receiving message from the gateway node, sensor node verifies the authenticity of the gateway node and if it verifies successfully it sends and authentication reply message to the gateway node. Then gateway node checks the authenticity of the sensor node. If it verifies successfully then sensor node is authenticated with gateway node. Further gateway node sends the accept login message to sensor node. Upon receiving this message, the sensor node accepts the request from the user. After the successful completion of login and authentication phases of this scheme, both user and sensor node establish a secret session key for their future secure communication.

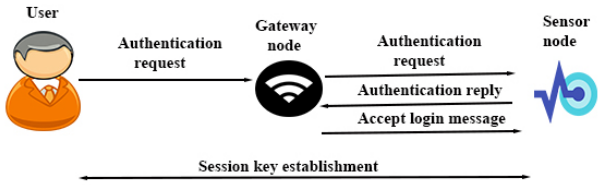

Figure 5: Network model used in [35]

Li et al. [40] proposed an elliptic-curve cryptography (ECC) based authentication scheme for industrial IoT environment. Their scheme does not provide some of the required functionality features, such as stolen/lost mobile device revo-

cation and biometric update. Moreover, their scheme incurs high computational overhead for the resource constrained sensor nodes. The network model of the scheme of Li et al. [40] is provided in Figure 6. In this model, a mobile user starts the communication with the gateway node once successfully login into the system occurs. The mobile user first sends authentication request message to the gateway node. After receiving message form the mobile user, the gateway node verifies the authenticity of the mobile user. If it is verified successfully, the mobile user is authenticated by the gateway node. The gateway node further sends an authentication request to the designated sensor node specified by the mobile user. After receiving message from the gateway node, the sensor node verifies the authenticity of the gateway node. If verification happens successfully, it then sends the authentication reply message to the gateway node. The gateway node then checks the authenticity of the sensor node. Once successful verification is done, the sensor node is authenticated by the gateway node. Furthermore, the gateway node sends authentication reply message to the mobile user. After receiving authentication reply message, the mobile user checks the authenticity of the gateway node. If verification takes place successfully, both the mobile user and sensor node establish a secret session key for their future secure communication.

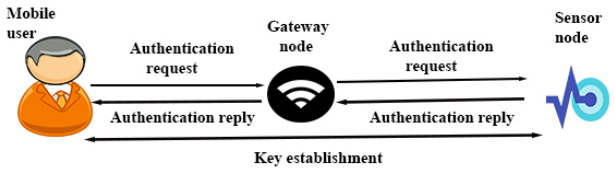

Figure 6: Network model used in [40]

Challa et al. [2] proposed a user authentication scheme for future IoT applications. Their scheme is also based on ECC and it relies on ECC-based digital signature. This scheme requires more computation and communication overheads for the entities involved in IoT environment. The network model of the scheme of Challa et al. [2] is given in Figure 7. In this model user starts the communication by successfully login into the system. User sends authentication request message to gateway node. After receiving message form user, gateway node verifies the authenticity of the user. If it verifies successfully then user is authenticated with gateway node. Gateway node further computes other variables and sends authentication request to the sensing device. After receiving message from the gateway node, sensor device verifies the authenticity of the gateway node and if it verifies successfully it sends and authentication reply message to user. User checks the authenticity of the sensing device. If it verifies successfully then sensing device is authenticated with user. After the successful completion of login and authentication phases of this scheme both user and sensing device mutual authenticates with each other, and establish a secret session key for their future secure communication.

Several other user authentication schemes [44], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], have been proposed in the literature for resource-constrained wireless sensor networks. These schemes can also be applied in the cloud-driven IoT-based big data environment as some IoT devices are also resource-constrained in nature. There are other user authentication schemes [57], [58], [59], [60], [61], [62], [63], which can be also applied in the IoT environment. It is worth noting that most of the available schemes for user authentication and key agreement are not protected against different possible known attacks. Also, some of the schemes are not lightweight as they require more computation and communication overheads. As a result, the existing schemes proposed for this environment may not suite user authentication in cloud-driven IoT environment. Therefore, there is a great need to design a more secure user authentication scheme for cloud-driven IoT-based big data environment which needs to be also lightweight in nature. A legitimate user can then access the real time data from the IoT sensors securely. The legitimate users can also access the data from the cloud servers securely and can also perform big data analytic on the processed data of big data warehouse as mentioned at the cloud servers.

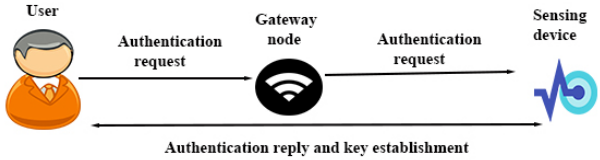

Figure 7: Network model used in [2]

Table 1: Approximate time required for different operations [41]

Notation	Description (time to compute)	Approx. computation time (seconds)
T_h	hash function	0.00032
T_{ecm}	ECC point multiplication	0.0171
T_{eca}	ECC point addition	0.0044

4.2. *Comparative study of authentication schemes*

We provide a comparative study of various authentication schemes which are suggested for the IoT environment or they are closely related to the IoT environment. The considered compared schemes include the schemes of Challa *et al.* [2], Turkanovic *et al.* [31], Farash et al. [33], Li et al. [40], Porambage *et al.* [42] and Porambage *et al.* [43].

In the scheme of Porambage *et al.* [43], two protocols are present: 1) protocol 1 which provides facility to process the key derivation facility to only the legitimate members of the multicast group, and 2) protocol 2 which permits to establish a shared secret key among the entities in a multicast group. Table 1 provides the details of approximate time needed for different cryptographic operations [41].

Table 2 provides the details of computational costs needed for the login and authentication phases. This table depicts the comparison of computational costs among different existing schemes [2], [31], [33], [40], [42], [43]. From the comparative analysis, it is found out that the performance of Challa *et al.*'s scheme [2] is better than Porambage *et al.*'s scheme [43].

Table 2: Comparison of computation overheads of different existing schemes

Protocol	User side	GWN/Base station side	Sensing device/ Sensor side	Total overhead
[2]	$5T_{ecm} + 5T_h$ $\approx 0.0871s$	$5T_{ecm} + 4T_h$ $\approx 0.08678s$	$4T_{ecm} + 3T_h$ $\approx 0.06936s$	$14T_{ecm} + 12T_h$ $\approx 0.24324s$
[31]	$7T_h$ $\approx 0.00224s$	$5T_h$ $\approx 0.0016s$	$7T_h$ $\approx 0.00224s$	$19T_h$ $\approx 0.00608s$
[33]	$11T_h$ $\approx 0.00352s$	$14T_h$ $\approx 0.00448s$	$7T_h$ $\approx 0.00224s$	$32T_h$ $\approx 0.01024s$
[40]	$8T_h + 3T_{ecm}$ $\approx 0.05386s$	$7T_h + T_{ecm}$ $\approx 0.01934s$	$4T_h + 2T_{ecm}$ $\approx 0.03548s$	$19T_h + 6T_{ecm}$ $\approx 0.10868s$
[42]	$3T_h + 2T_{ecm}$ $+T_{eca}$ $\approx 0.0396s$	–	$3T_h + 2T_{ecm}$ $+T_{eca}$ $\approx 0.0396s$	$6T_h + 4T_{ecm}$ $+2T_{eca}$ $\approx 0.0792s$
Protocol-1 [43]	$4T_{ecm} + 8T_h$ $+T_{eca}$ $\approx 0.0754s$	–	$11T_{ecm} + 10T_h$ $+3T_{eca}$ $\approx 0.2045s$	$15T_{ecm} + 18T_h$ $+4T_{eca}$ $\approx 0.2799s$
Protocol-2 [43]	$3T_{ecm} + 7T_h$ $+T_{eca}$ $\approx 0.0579s$	– –	$5T_{ecm} + 7T_h$ $+2T_{eca}$ $\approx 0.0965s$	$8T_{ecm} + 14T_h$ $+3T_{eca}$ $\approx 0.1544s$

Though the scheme [2] requires more computational cost as compared to other schemes [31], [40], [42], but it offers extra security and functionality features which are exhibited in Table 4.

For comparison of communication costs among existing schemes [2], [31], [33], [40], [42], [43], the following assumptions have been made:

- The size of sequence number, random nonce and time stamp is assumed as 32 bits.
- The used hash function is secure hash standard (SHA-1) [64]. Therefore, size of hash digest is 160 bits.
- The identities are 160 bits in size.
- As the security of 160-bit ECC cryptosystem is equivalent to that for 1024-bit RSA cryptosystem [65], an elliptic curve point $P = ((P)_x, (P)_y)$ needs $(160 + 160) = 320$ bits.

Table 3 depicts the communication overheads for the existing schemes during the login and authentication phases. The communication cost required by the scheme [2] is less than that for other schemes [31], [33], [40], [43]. However, the scheme [2] needs more communication overhead as compared to that for Porambage *et al.*'s scheme [42].

The details of the functionality features available in the existing schemes has been also provided in Table 4. The scheme [2] provides the desired security & functionality features, while other schemes [31], [33], [40], [42], [43] lack in supporting key security & functionality features, such as user anonymity preservation, and security against impersonation and offline password guessing attacks.

Table 3: Comparison of communication overheads of the different existing schemes

Protocol	No. of messages	No. of bits
Challa *et al.* [2]	3	2528
Turkanovic *et al.* [31]	4	2720
Farash et al. [33]	4	2752
Li et al. [40]	4	2720
Porambage *et al.* [42]	4	1344
Porambage *et al.* [43]		
-Protocol-1	4	3360
-Protocol-2	2	1136

5. Research challenges and future research directions

Cloud-driven IoT-based big data environment offers plethora of new and emerging applications. Depending on the application, such environment exhibit unique requirements such as real-time data processing and access, for instance, real-time monitoring of an industrial plant, traffic situation in a city, and so on. Modern big data techniques such as big data analytic can also be applied to the huge data generated by the IoT sensors. Such big data analytic procedure helps to find out the hidden patterns in the data, such as to predict health or death risk in an industrial plant. Since cloud-driven IoT-based big data environment is part of the Internet, therefore it inherits the traditional security, privacy, and other challenges from its parental Internet paradigm. To this end, existing schemes in the literature discuss and provide different solutions for the challenges faced by the merger of cloud and IoT. In the following, we point out and discuss the current pressing challenges for research and then through open discussion, we discuss future research directions of authentication in cloud-driven IoT-based big data environment.

Table 4: Comparison of functionality features of the existing schemes

Feature	Porambage *et al.* [42]	Porambage *et al.* [43]	Turkanovic *et al.* [31]	Challa *et al.* [2]	Farash *et al.* [33]	Li *et al.* [40]
FN_1	×	×	✓	✓	×	✓
FN_2	×	✓	×	✓	×	✓
FN_3	−	−	×	✓	×	✓
FN_4	−	−	×	✓	×	✓
FN_5	×	✓	✓	✓	✓	✓
FN_6	✓	×	✓	✓	×	✓
FN_7	×	✓	×	✓	×	✓
FN_8	×	✓	✓	✓	✓	✓
FN_9	×	×	✓	✓	✓	✓
FN_{10}	✓	✓	✓	✓	✓	✓
FN_{11}	✓	✓	✓	✓	✓	✓
FN_{12}	✓	✓	✓	✓	✓	✓
FN_{13}	−	−	×	✓	×	×
FN_{14}	✓	×	×	✓	✓	✓
FN_{15}	×	✓	✓	✓	✓	✓
FN_{16}	−	−	✓	✓	✓	✓
FN_{17}	−	×	×	✓	−	×
FN_{18}	×	×	×	✓	✓	×
FN_{19}	×	×	×	✓	✓	×

Note: FN_1: user anonymity property; FN_2: insider attack; FN_3: off-line password guessing attack; FN_4: stolen smart card attack; FN_5: denial-of-service attack; FN_6: known session key attack; FN_7: user impersonation attack; FN_8: man-in-the middle attack; FN_9: replay attack; FN_{10}: mutual authentication; FN_{11}: session key agreement; FN_{12}: forward secrecy; FN_{13}: stolen/lost device revocation; FN_{14}: untraceability property; FN_{15}: resilience against sensor node/sensing device capture attack; FN_{16}: GWN independent password update phase; FN_{17}: support biometric update phase; FN_{18}: provide security analysis using BAN logic; FN_{19} : provide formal security verification using AVISPA tool.
−: not applicable in a scheme; ×: insecure against a particular attack or does not support a particular feature; ✓: secure against a particular attack or supports a particular feature.

5.1. Security of authentication schemes

Majority of authentication schemes proposed for cloud-driven IoT-based big data environment are not secure and susceptible to various attacks, such as privileged insider attack, online/offline password guessing, session key leakage and computation, and physical capturing of smart IoT devices, to name a few. Moreover some of them do not provide required additional functional features such as dynamic smart IoT device addition, device revocation, password and bio-metric update. Therefore, an authentication scheme must be evaluated for its security through all possible security analysis. Wang et al. [66] identified some important security aspects while analyzing some existing authentication schemes in the literature and pointed out that achieving the soundness of authentication scheme is still an open issue. It was noticed that the formal security analysis under the standard model can not seize some structural mistakes when we prove the security of a scheme. Hence, it becomes mandatory to analyze a scheme using other methods including formal proof (i.e., the Burrows-AbadiNeedham (BAN) logic and random oracle models, such as the Real-Or-Random (RoR) model [67]) and also informal security analysis.

The BAN logic is a set of rules which can be used for analyzing the authentication protocols. It helps the communicating parties to determine whether the exchanged messages are trustworthy. The BAN logic proof provides secure mutual authentication proof among two participating entities in the network. In IoT environment, we need to prove that a user and a sensing device mutually authenticate each other. This is acheived through BAN logic proof by verifying the messages' origin, freshness as well as trustworthiness [2].

Abdalla et al. [67] presented a new as well as stronger model for authenticated key exchange protocols, called the ROR model. The ROR model is provably stronger than the existing models, in the sense that a scheme proven secure in this model is also secure in the existing model. Using the ROR model, we can prove that a user authentication protocol provides the session key security. As mentioned in the threat model (Section 2.2), under the CK adversary model [67], an adversary $\mathcal{A}$ has the capabilities as in the Dolev-Yao (DY) model [16], and in addition, he/she may compromise of the secret credentials as well as the session states & session keys in the sessions. Therefore, it is strongly recommended that the session key construction should be based on short-term (temporal) and long-term secrets so that we can make the session key security of a designed user authentication scheme in the IoT environment much stronger.

We can also verify formally the security of user authentication schemes using some automated formal security verification software tools (for example, Automated Validation of Internet Security Protocols and Applications (AVISPA) [68]). AVISPA is a widely-accepted software tool which proves the resilience of a user authentication scheme against its replay and man-in-the-middle attacks. In recent years, AVISPA has been used in formal security verification in various user authentication protocols [2, 20, 26, 28, 69]. In addition, there is another popular formal security verification tool, called ProVerif [70]. Proverif is based on applied pi calculus [71] and it is used for proving session key secrecy and authentication. The details of its implementation can be found in [72].

5.2. Efficiency of authentication schemes

In a cloud-driven IoT-based big data environment, smart devices such as IoT sensors are resource constrained (i.e., they have less computation power, limited storage capacity and limited battery backup). Therefore, these devices are unable to perform compute- and storage- and communication-intensive operations. Moreover it is not recommended to use large size messages during the authentication and key establishment phases. The reason is that it will consume other resources of the environment (i.e., fast battery drainage of the IoT sensors in sending and receiving large sized messages). Hence, we need to design authentication scheme in such a way that the scheme should have less computation costs, communication costs and storage cost along without compromising the security of the scheme [20], [26], [73], [74]. Furthermore, depending on the application, real-time ultra-fast authentication is another challenge for such resource-constrained devices. It is desired to have an ultra-fast authentication for different real-time services such as in case of emergency situations. More in-depth investigation is needed to leverage new security technique (both traditional cryptographic techniques with necessary tweaks and new emerging techniques) are essential. These kinds of authentication schemes are more applicable to the mobile appli-

cations associated with IoT. For instance, transportation systems applications and body area network applications [75]. In this context, Hussain et al. [76] proposed a fast authentication mechanism for moving electric cars on the road to authenticate with the road segment while charging on the move. But in future more investigation is needed for emerging ultra-fast authentication that fulfill the underlying requirements of both the network and the users.

5.3. Scalability of authentication schemes

IoT is a massively heterogeneous network of different communication paradigms and application domains with their own requirements and capabilities. In this context, the authentication among applications, services, and users therewith, make it a challenging tasks. Consider a scenario where Electronic Health Records (EHRs) of certain users are stored in an IoT-enabled cloud infrastructure for further processing. Different devices pertaining to the Body Area Network (BANs) generate data and send it to the cloud. When these devices send the data to cloud, they must authenticate to the local gateway and upon successful authentication, data is forwarded to the local gateway. Similarly, the gateway must authenticate itself to the cloud infrastructure. On the other hand, the applications that use this data and/or information as a result of the data in the cloud, must authenticate to the cloud. Thus, there are multiple authentications involve which might be different from each other. This is just a simple example for the sake of illustration. Similar patterns can be found in other application breeds of IoT. For an end-to-end authentication mechanism in cloud-driven IoT-based big data environment, it is important that the authentication scheme should be scalable across different domains. More in-depth investigation is needed in this direction.

5.4. Physically secure authentication schemes

A Physically Unclonable Function (PUF) is considered as a one-way function that maps a set of challenges to another set of responses based on the unique physical micro structure of a device. PUF is a promising primitive to achieve authentication, access control, and traceability. It is also very useful for secure and low-cost authentication [77]. An ideal PUF has the following important properties:

- The output of the PUF is always dependent on a physical system.
- It is easy to evaluate and construct the PUF.
- PUF output is unpredictable in nature and it works as a random function.
- PUF is also uncloneable.

It is therefore interesting to devise a lightweight privacy-preserving authentication scheme for the IoT system by considering PUF as it is done for other environment [78].

5.5. Privacy of data maintained at big data warehouse

Data privacy depicts how information should be handled based on its relative importance. The cloud-driven IoT-based big data environment is also applicable to the information sensitive applications such as those in health care domain. In such privacy-demanding environment, smart health sensors around the body of a patient sense his/her health related information and send the sensed data to the cloud servers for storage and processing. In this context, it is crucial to maintain the privacy of data, for both stored data as well as data in transit. Therefore, we require new and efficient techniques that provide privacy to stored data and data in transit at the same time for cloud-driven IoT-based big data environment [8], [11], [79]. Similarly, privacy-aware authentication schemes must be tailored for IoT environment where device and/or user's privacy is preserved.

5.6. Heterogeneity of IoT networks environment

Cloud-driven IoT-based big data environment is diverse, we use different kinds of devices ranging from full-edged desktops, laptops, personal digital assistants to low-end RFID tags. Moreover, devices operate under different kinds of communication protocols. These devices are different in terms of their computation power, communication range, storage capacity, and operating system, such as embedded software. Therefore, we need to design a technique in such a way that it can accommodate all different types of devices and associated technologies [21].

5.7. Cross-platform authentication

The heterogeneity of IoT environment is a double-edged sword. On one hand it allows different application domains to interconnect, but at the same time poses challenges for efficient authentication mechanisms. For instance, when a smart home application needs to access the data from BAN or any other network, then the authentication must be robust in a way that applications should seamlessly retrieve the data from the target network. However, it is important to note that usually data is stored in the cloud for which an additional authentication is needed. Therefore, in the above example, the smart home application must first authenticate to the gateway, then to the cloud, and (upon verification of the access rights) retrieve the data. A robust and efficient authentication mechanism is needed to provide seamless connectivity across different IoT platforms [80].

5.8. Privacy-aware authentication

In privacy-aware authentication scheme multiple communicating parties can authenticate and communicate among each other securely. Moreover, the scheme should provide secure key establishment, along with user anonymity and user untraceability properties. In literature many authors claimed that their schemes are secured and achieved the above discussed properties. But later on it was identified that their schemes had privacy issues as the schemes failed to preserve anonymity and untraceability properties [40], [81], [82], [83]. Therefore, designing of a privacy-aware authentication scheme is also a future research challenge for cloud-driven IoT-based big data environment.

5.9. Use of data mining techniques

Data mining techniques play major role in big data analytic which is used to find out the patterns from the big data, (for example, chances of fire in an industrial plant in future). Therefore, it is important to ensure the data mining technique which we use should be secured against not just external threats, but also from the insiders who abuse network privileges to obtain sensitive information. Therefore, designing of a secure big data analytic technique for IoT sensors data is also a future research challenge [8], [11], [84].

5.10. Granular auditing

Granular auditing helps in determining the attacks that happen on the big data warehouse, for example, when attacks occurred, what were the consequences. By performing auditing, we can identify what should be done to improve the security of the system so that these attacks never happen in future [85]. Hence, it becomes essential to provide some techniques for granular auditing for cloud-driven IoT-based big data environment which will help in detection and prevention of attacks that happen in this environment.

6. Conclusion

We discussed the network and threat model of authentication mechanism for cloud-driven IoT-based big data environment. We then discussed the security requirements and security issues challenges in the cloud-driven IoT-based big data environment particularly needed for authentication techniques. We also provided a taxonomy of existing authentication schemes related to the cloud-driven IoT-based big data environment. We also provided a comparative study of computation costs, communication costs, and security and functionality features of the existing authentication schemes applicable for cloud-driven IoT-based big data environment. Finally, we identified some future research challenges in the designing of authentication and other security protocols for cloud-driven IoT-based big data environment.

Acknowledgments

This work was partially supported by Finep/Funttel Grant No. 01.14.0231.00, under the Radiocommunication Reference Center (Centro de Referência em Radicomunicações - CRR) project of the National Institute of Telecommunications (Instituto Nacional de Telecomunicações), Brazil, by National Funding from the FCT – Fundação para a Ciência e a Tecnologia through the UID/EEA/500008/2013 Project; and by Brazilian National Council for Research and Development (CNPq) via Grant No. 309335/2017-5. We also thank the anonymous reviewers for their valuable feedback on the paper which helped us to improve its quality and presentation.

References

[1] A. Sheth. Internet of Things to Smart IoT Through Semantic, Cognitive, and Perceptual Computing. *IEEE Intelligent Systems*, 31(2):108–112, 2016.

[2] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E. J. Yoon, and K. Y. Yoo. Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications. *IEEE Access*, 5:3028–3043, 2017.

[3] J. Yang, Z. Lu, and J. Wu. Smart-toy-edge-computing-oriented data exchange based on blockchain. *Journal of Systems Architecture*, 87:36–48, 2018.

[4] B. Ahlgren, M. Hidell, and E. C. . Ngai. Internet of Things for Smart Cities: Interoperability and Open Data. *IEEE Internet Computing*, 20(6):52–56, 2016.

[5] A. Zanni. Cyber-physical systems and smart cities, 2015. http://www.ibm.com/developerworks/library/ba-cyber-physical-systems-and-smart-cities-iot/index.html Accessed on August 2018.

[6] X. Zeng, S. K. Garg, P. Strazdins, P. P. Jayaraman, D. Georgakopoulos, and R. Ranjan. IOTSim: A simulator for analysing IoT applications. *Journal of Systems Architecture*, 72:93–107, 2017.

[7] C. M. Sosa-Reyna, E. Tello-Leal, and D. Lara-Alabazares. Methodology for the model-driven development of service oriented IoT applications. *Journal of Systems Architecture*, 90:15–22, 2018.

[8] G. S. Aujla, R. Chaudhary, N. Kumar, A. K. Das, and J. J. P. C. Rodrigues. SecSVA: Secure Storage, Verification, and Auditing of Big Data in the Cloud Environment. *IEEE Communications Magazine*, 56(1):78–85, 2018.

[9] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos. Iot-based big data storage systems in cloud computing: Perspectives and challenges. *IEEE Internet of Things Journal*, 4(1):75–87, 2017.

[10] M. Marjani, F. Nasaruddin, A. Gani, A. Karim, I. A. T. Hashem, A. Siddiqa, and I. Yaqoob. Big iot data analytics: Architecture, opportunities, and open research challenges. *IEEE Access*, 5:5247–5261, 2017.

[11] A. Jindal, A. Dua, N. Kumar, A. K. Das, A. V. Vasilakos, and J. J. P. C. Rodrigues. Providing Healthcare-as-a-Service Using Fuzzy Rule Based Big Data Analytics in Cloud Computing. *IEEE Journal of Biomedical and Health Informatics*, 22(5):1605–1618, 2018.

[12] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers. Twenty Security Considerations for Cloud-Supported Internet of Things. *IEEE Internet of Things Journal*, 3(3):269–284, 2016.

[13] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues. Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment. *IEEE Internet of Things Journal*, 2018. doi:10.1109/JIOT.2018.2877690.

[14] Cloud Computing and IoT. http://compass.ie/cloud-Iot-mobile/. accessed on july 2018.

[15] M. Wazid, A. K. Das, and A. V. Vasilakos. Authenticated key management protocol for cloud-assisted body area sensor networks. *Journal of Network and Computer Applications*, 123:112 – 126, 2018.

[16] D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.

[17] R. Canetti and H. Krawczyk. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. In Birgit Pfitzmann, editor, *Advances in Cryptology — EUROCRYPT*, pages 453–474, Innsbruck (Tyrol), Austria, 2001. Springer Berlin Heidelberg.

[18] R. Canetti and H. Krawczyk. Universally composable notions of key exchange and secure channels. In Lars R. Knudsen, editor, *Advances in Cryptology — EUROCRYPT*, pages 337–351, Amsterdam, The Netherlands, 2002. Springer Berlin Heidelberg.

[19] T. S. Messerges, E. A. Dabbish, and R. H. Sloan. Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers*, 51(5):541–552, 2002.

[20] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo. Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment. *IEEE Transactions on Dependable and Secure Computing*, 2017. DOI: 10.1109/TDSC.2017.2764083.

[21] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. Kwak. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*, 3:678–708, 2015.

[22] E. Bertino and N. Islam. Botnets and Internet of Things Security. *Computer*, 50(2):76–79, 2017.

[23] Y. Yang, H. Peng, L. Li, and X. Niu. General Theory of Security and a Study Case in Internet of Things. *IEEE Internet of Things Journal*, 4(2):592–600, 2017.

[24] National Institute of Standards and Technology (NIST), U.S. Department of Commerce. Advanced Encryption Standard (AES) Available at https://nvlpubs.nist.gov/ nistpubs/ fips/nist.fips.197.pdf. Accessed on August 2018., 2001.

[25] Secure Hash Standard. FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995. Available at http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf. Accessed on March 2016., 1995.

[26] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo. Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks. *IEEE Internet of Things Journal*, 5(1):269–282, 2018.

[27] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos. A Novel Authentication and Key Agreement Scheme for Implantable Medical Devices Deployment. *IEEE Journal of Biomedical and Health Informatics*, 22(4):1299–1309, 2018.

[28] F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K. K. R. Choo, M. Wazid, and A. K. Das. An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. *Journal of Network and Computer Applications*, 89:72 – 85, 2017.

[29] A. K. Das, S. Zeadally, and D. He. Taxonomy and analysis of security protocols for Internet of Things. *Future Generation Computer Systems*, 89:110–125, 2018.

[30] H. L. Yeh, T. H. Chen, P. C. Liu, T. H. Kim, and H. W. Wei. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sensors*, 11(5):4767–4779, 2011.

[31] M. Turkanovi, B. Brumen, and M. Hlbl. 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*, 20:96 – 112, 2014.

[32] R. Amin and G. P. Biswas. A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. *Ad Hoc Networks*, 36:58–80, 2016.

[33] M. S. Farash, M. Turkanovic, S. Kumari, and M. Holbl. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. *Ad Hoc Networks*, 36:152 – 176, 2016.

[34] R. Amin, SK. H. Islam, G.P. Biswas, M. K. Khan, L. Leng, and N. Kumar. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Computer Networks*, 101:42 – 62, 2016.

[35] W. B. Hsieh and J. S. Leu. A Robust User Authentication Scheme Using Dynamic Identity in Wireless Sensor Networks. *Wireless Personal Communications*, 77(2):979–989, 2014.

[36] M. L. Das. Two-factor user authentication in wireless sensor networks. *IEEE Transactions on Wireless Communications*, 8(3):1086–1090, 2009.

[37] M. K. Khan and K. Alghathbar. Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks'. *Sensors*, 10(3):2450–2459, 2010.

[38] B. Vaidya, D. Makrakis, and H. T. Mouftah. Improved Two-Factor User Authentication in Wireless Sensor Networks. In *Second International Workshop on Network Assurance and Security Services in Ubiquitous Environments*, pages 600–606, 2010.

[39] F. Wu, L. Xu, S. Kumari, and X. Li. A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security. *Journal of Ambient Intelligence and Humanized Computing*, 8(1):101–116, 2017.

[40] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari. A Robust ECC-Based Provable Secure Authentication Protocol With Privacy Preserving for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 14(8):3599–3609, 2018.

[41] V. Odelu, A. K. Das, and A. Goswami. An efficient biometric-based privacy-preserving three-party authentication with key agreement protocol using smart cards. *Security and Communication Networks*, 8(18):4136–4156.

[42] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila. Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. In *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 2728–2733, 2014.

[43] P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila, and B. Stiller. Group Key Establishment for Enabling Secure Multicast Communication in Wireless Sensor Networks Deployed for IoT Applications. *IEEE Access*, 3:1503–1511, 2015.

[44] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus. TinyPK: Securing Sensor Networks with Public Key Technology. In *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04)*, pages 59–64, Washington DC, USA, 2004.

[45] O. Delgado-Mohatar, A. Fster-Sabater, and J. M. Sierra. A light-weight authentication scheme for wireless sensor networks. *Ad Hoc Networks*, 9(5):727 – 735, 2011.

[46] D. Wang and P. Wang. Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks. *Ad Hoc Networks*, 20(0):1 – 15, 2014.

[47] C. C. Lee, C. T. Li, and S. D. Chen. Two attacks on a two-factor user authentication in wireless sensor networks. *Parallel Processing Letters*, 21(1):21 – 26, 2011.

[48] D. Z. Sun, J. X. Li, Z.-Y. Feng, Z.-F. Cao, and G.-Q. Xu. On the security and improvement of a two-factor user authentication scheme in wireless sensor networks. *Personal and Ubiquitous Computing*, 17(5):895–905, 2013.

[49] A. K. Das. A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks. *Peer-to-Peer Networking and Applications*, 9(1):223–244, 2016.

[50] A. K. Das. A Secure and Efficient User Anonymity-Preserving Three-Factor Authentication Protocol for Large-Scale Distributed Wireless Sensor Networks. *Wireless Personal Communications*, 82(3):1377–1404, 2015.

[51] H. L. Yeh, T. H. Chen, P. C. Liu, T. H. Kim, and H. W. Wei. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sensors*, 11(5):4767–4779, 2011.

[52] C. C. Chang and H. D. Le. A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks. *IEEE Transactions on Wireless Communications*, 15(1):357–366, 2016.

[53] P. Gope and T. Hwang. A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks. *IEEE Transactions on Industrial Electronics*, 63(11):7124–7132, 2016.

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

[55] Q. Jiang, S. Zeadally, J. Ma, and D. He. Lightweight Three-Factor Authentication and Key Agreement Protocol for Internet-Integrated Wireless Sensor Networks. *IEEE Access*, 5:3376–3392, 2017.

[56] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. K. H. Islam, and P. Gope. Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks. *Multimedia Tools and Applications*, 77(14):18295–18325, 2018.

[57] P. Gope, R. Amin, S. K. H. Islam, N. Kumar, and V. K. Bhalla. Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. *Future Generation Computer Systems*, 83:629–637, 2018.

[58] P. Gope and B. Sikdar. An Efficient Data Aggregation Scheme for Privacy-Friendly Dynamic Pricing-Based Billing and Demand-Response Management in Smart Grids. *IEEE Internet of Things Journal*, 5(4):3126–3135, 2018.

[59] Q. Feng, D. He, S. Zeadally, and H. Wang. Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment. *Future Generation Computer Systems*, 84:239–251, 2018.

[60] M. Wazid, A. K. Das, N. Kumar, and A. V. Vasilakos. Design of secure key management and user authentication scheme for fog computing services. *Future Generation Computer Systems*, 91:475–492, 2019.

[61] J. Srinivas, A. K. Das, and J. J. P. C. Rodrigues. 2PBDC: privacy-preserving bigdata collection in cloud environment. *The Journal of Supercomputing*, 2018. DOI: 10.1007/s11227-018-2605-1.

[62] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar. Anonymous Lightweight Chaotic Map-Based Authenticated Key Agreement Protocol for Industrial Internet of Things. *IEEE Transactions on Dependable and Secure Computing*, 2018. DOI: 10.1109/TDSC.2018.2857811.

[63] K. Park, Y. Park, Y. Park, and A. K. Das. 2PAKEP: Provably Secure and Efficient Two-Party Authenticated Key Exchange Protocol for Mobile Environment. *IEEE Access*, 6:30225–30241, 2018.

[64] Secure Hash Standard, 1995. FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995.

[65] R. L. Rivest, M. E. Hellman, J. C. Anderson, and J. W. Lyons. Responses to NIST's Proposal. *Commun. ACM*, 35(7):41–54, 1992.

[66] D. Wang, D. He, P. Wang, and C. Chu. Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment. *IEEE Transactions on Dependable and Secure Computing*, 12(4):428–442, 2015.

[67] M. Abdalla, P.A. Fouque, and D. Pointcheval. Password-based authenticated key exchange in the three-party setting. In *8th International Work-*

shop on Theory and Practice in Public Key Cryptography (PKC'05), Lecture Notes in Computer Science (LNCS), volume 3386, pages 65–84, Les Diablerets, Switzerland, 2005.

[68] AVISPA. SPAN, the Security Protocol ANimator for AVISPA, 2017. http://www.avispa-project.org/. Accessed on June 2018.

[69] D. He, M. Ma, S. Zeadally, N. Kumar, and K. Liang. Certificateless Public Key Authenticated Encryption With Keyword Search for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 14(8):3618–3627, 2018.

[70] M. Abadi, B. Blanchet, and H. Comon-Lundh. Models and Proofs of Protocol Security: A Progress Report. In *Proceedings of 21st International Conference on Computer Aided Verification (CAV'09)*, pages 35–49, Grenoble, France, 2009.

[71] M. Abadi and C. Fournet. Mobile Values, New Names, and Secure Communication. *SIGPLAN Notice*, 36(3):104–115, 2001.

[72] ProVerif. http://prosecco.gforge.inria.fr/personal/bblanche/proverif/. Accessed on September 2018.

[73] M. Wazid, A. K. Das, N. Kumar, and A. V. Vasilakos. Design of secure key management and user authentication scheme for fog computing services. *Future Generation Computer Systems*, 91:475 – 492, 2019.

[74] Y. Zhang, D. He, S. Zeadally, D. Wang, and K. R. Choo. Efficient and Provably Secure Distributed Signing Protocol for Mobile Devices in Wireless Networks. *IEEE Internet of Things Journal*, 2018. doi:10.1109/JIOT.2018.2865247.

[75] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. K. R. Choo, and Y. Park. Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment. *IEEE Journal of Biomedical and Health Informatics*, 22(4):1310–1322, 2018.

[76] R. Hussain, J. Son, D. Kim, M. Nogueira Lima, H. Oh, A. O. Tokuta, and J. Seo. PBF: A New Privacy-Aware Billing Framework for Online Electric Vehicles with Bidirectional Auditability. *Wireless Communications and Mobile Computing*, 2017:1–17, 2017. Article ID 5676030, https://doi.org/10.1155/2017/5676030.

[77] C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, and V. Fischer. Implementation and Characterization of a Physical Unclonable Function for IoT: A Case Study With the TERO-PUF. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37(1):97–109, 2018.

[78] P. Gope, J. Lee, and T. Q. S. Quek. Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions. *IEEE Transactions on Information Forensics and Security*, 13(11):2831–2843, 2018.

[79] X. Li, S. Liu, F. Wu, S. Kumari, and J. J. P. C. Rodrigues. Privacy Preserving Data Aggregation Scheme for Mobile Edge Computing Assisted IoT Applications. *IEEE Internet of Things Journal*, 2018. doi:10.1109/JIOT.2018.2874473.

[80] EBU Tech. Cross-Platform Authentication. https:// tech.ebu.ch/ groups/ CPA. Accessed on August 2018.

[81] J. Tsai and N. Lo. A privacy-aware authentication scheme for distributed mobile cloud computing services. *IEEE Systems Journal*, 9(3):805–815, 2015.

[82] D. He, N. Kumar, M. K. Khan, L. Wang, and J. Shen. Efficient privacy-aware authentication scheme for mobile cloud computing services. *IEEE Systems Journal*, 12(2):1621–1631, 2018.

[83] V. Odelu, S. Zeadally, A. K. Das, M. Wazid, and D. He. A secure enhanced privacy-preserving key agreement protocol for wireless mobile networks. *Telecommunication Systems*, 69(4):431–445, 2018.

[84] J. Vaidya, B. Shafiq, W. Fan, D. Mehmood, and D. Lorenzi. A Random Decision Tree Framework for Privacy-Preserving Data Mining. *IEEE Transactions on Dependable and Secure Computing*, 11(5):399–411, 2014.

[85] G. Gross. 9 Key Big Data Security Issue. https://www.alienvault.com/ blogs/ security-essentials/ 9-key-big-data-security-issues. Accessed on August 2018.

Mohammad Wazid has received M.Tech. degree in Computer Network Engineering from Graphic Era University, Dehradun, India and the Ph.D. degree in Computer Science and Engineering from the International Institute of Information Technology, Hyderabad, India. He was Postdoctoral Researcher at Cyber Security and Networks Lab, Innopolis University, Innopolis, Russia. His current research interests include security, remote user authentication, Internet of things (IoT), and cloud computing. He has published more than 55 papers in international journals and conferences in the above areas. Some of his research findings are published in top cited journals, such as the IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Smart Grid, IEEE Internet of Things Journal, IEEE Transactions on Industrial Informatics, IEEE Journal of Biomedical and Health Informatics (formerly IEEE Transactions on Information Technology in Biomedicine), IEEE Consumer Electronics Magazine, IEEE Access, Future Generation Computer Systems, Computers & Electrical Engineering, Computer Methods and Programs in Biomedicine, Security and Communication Networks (Wiley) and Journal of Network and Computer Applications. He was a recipient of the University Gold Medal and the Young Scientist Award by UCOST, Department of Science and Technology, Government of Uttarakhand, India. He has also received Dr. A.P.J Abdul Kalam Award for his innovative research works.

Ashok Kumar Das received a Ph.D. degree in computer science and engineering, an M.Tech. degree in computer science and data processing, and an M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. His current research interests include cryptography, wireless sensor network security, hierarchical access control, security in vehicular ad hoc networks, smart grid, Internet of Things (IoT), cyber-physical systems (CPS) and cloud computing, and remote user authentication. He has authored over 175 papers in international journals and conferences in the above areas, including over 150 reputed journal papers. Some of his research findings are published in top cited journals, such as the IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Smart Grid, IEEE Internet of Things Journal, IEEE Transactions on Industrial Informatics, IEEE Transactions on Vehicular Technology, IEEE Transactions on Consumer Electronics, IEEE Journal of Biomedical and Health Informatics (formerly IEEE Transactions on Information Technology in Biomedicine), IEEE Consumer Electronics Magazine, IEEE Access, IEEE Communications Magazine, Future Generation Computer Systems, Computers & Electrical Engineering, Computer Methods and Programs in Biomedicine, Computer Standards & Interfaces, Computer Networks, Expert Systems with Applications, and Journal of Network and Computer Applications. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He is on the editorial board of KSII Transactions on Internet and Information Systems, International Journal of Internet Technology and Secured Transactions (Inderscience), and Recent Advances in Communications and Networking Technology, is a Guest Editor for Computers & Electrical Engineering (Elsevier) for the special issue on Big data and IoT in e-healthcare, and has served as a Program Committee Member in many international conferences.

Rasheed Hussain received his M.S. and PhD degrees in Computer Engineering from Hanyang University, South Korea in 2010 and 2015, respectively. He also worked as Postdoctoral Fellow at Hanyang University, South Korea (Mar 2015 Aug 2015) and visiting researcher at University of Amsterdam (UvA), Netherlands (Aug 2015 Jun 2016). Currently he is working as Assistant Professor and coordinator of MS program in Secure System and Network Engineering (SNE) at Innopolis University, Russia. He serves as editorial board member of IEEE Internet Initiative, IEEE Access, and other journals as well as reviewer for many journals from IEEE, Elsevier, and Springer. His main research interests include information security, privacy, applied cryptography, vehicular networks and clouds, NDN, Internet of Things, Blockchain, and vehicular social networks.

Giancarlo Succi is currently Professor and Dean of Faculty of Computer Science and Software Engineering. He is also the of Head of Laboratory for Improving the Production of Software at Innopolis University, Russia. He holds a Laurea Degree in Electrical Engineering from the University of Genova, an M.Sc. in Computer Science from the State University of New York at Buffalo, and a PhD in Computer and Electrical Engineering again from the University of Genoa, Italy (December 1993). He has passed the habilitation certification as professional engineering both in Italy and in Canada and he has consulted for several organizations worldwide. He has been a Professor at the Free University of Bolzano-Bozen, Italy, University of Alberta, Edmonton, Canada, University of Calgary, Canada holding also various administrative positions. Giancarlo Succi has taught a variety of academic and industrial courses throughout his career in Software Engineering, Programming Languages, and Mobile, Distributed, and Centralized Operating Systems. He has organized various international conferences and other scientific and educational events. His research interests are in empirical software engineering, open source, mobile and energy aware systems, software reuse, and software product lines. He is the author of 5 and editor of 12 books and over than 370 publications.

Joel J. P. C. Rodrigues is Professor at the National Institute of Telecommunications (Inatel), Brazil and senior researcher at the Instituto de Telecomunicações, Portugal. Prof. Rodrigues is the leader of the Internet of Things research group (CNPq), Director for Conference Development - IEEE ComSoc Board of Governors, IEEE Distinguished Lecturer, Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, the President of the scientific council at ParkUrbis Covilh Science and Technology Park, the Past-Chair of the IEEE ComSoc Technical Committee on eHealth, the Past-chair of the IEEE ComSoc Technical Committee on Communications Software, Steering Committee member of the IEEE Life Sciences Technical Community and Publications co-Chair, and Member Representative of the IEEE Communications Society on the IEEE Biometrics Council. He is the Editor-in-Chief of two International Journals and an editorial board member of several top journals. He has authored or coauthored over 650 papers in refereed international journals and conferences, 3 books, and 2 patents. He had been awarded several Outstanding Leadership and Outstanding Service Awards by IEEE Communications Society and several best papers awards. He is member of the Internet Society, and a senior member ACM and IEEE.