Internet of Things xxx (xxxx) xxx

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Research article

Cryptographic technologies and protocol standards for Internet of Things

Sherali Zeadally [a,*], Ashok Kumar Das [b], Nicolas Sklavos [c]

[a] College of Communication and Information, University of Kentucky, Lexington, KY 40506 USA
[b] Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India
[c] Computer Engineering & Informatics Department, Polytechnic School, University of Patras, Patra Hellas 26504, Greece

ARTICLE INFO

Article history:
Received 17 May 2019
Revised 14 June 2019
Accepted 17 June 2019
Available online xxx

Keywords:
Cryptography
Internet of Things
Privacy
Protocol standards
Security
Smart devices

ABSTRACT

The Internet of Things (IoT) comprises physical/virtual networked objects that collect and exchange data with each other via the public Internet. As this exchange often takes place over public networks, many security attacks in an IoT environment are possible. First, we briefly review the security issues in the IoT environment. Next, we focus on recent cryptographic protocol standards that are in use or have been recommended for IoT devices to ensure secure communications. We also highlight the advantages and weaknesses of the several protocol standards for various IoT application scenarios including connected vehicles, health, smart home, and consumer appliances and devices. Finally, we discuss some challenges in the area of cryptographic protocol standards that still require to be addressed for IoT applications in the future.

1. Introduction

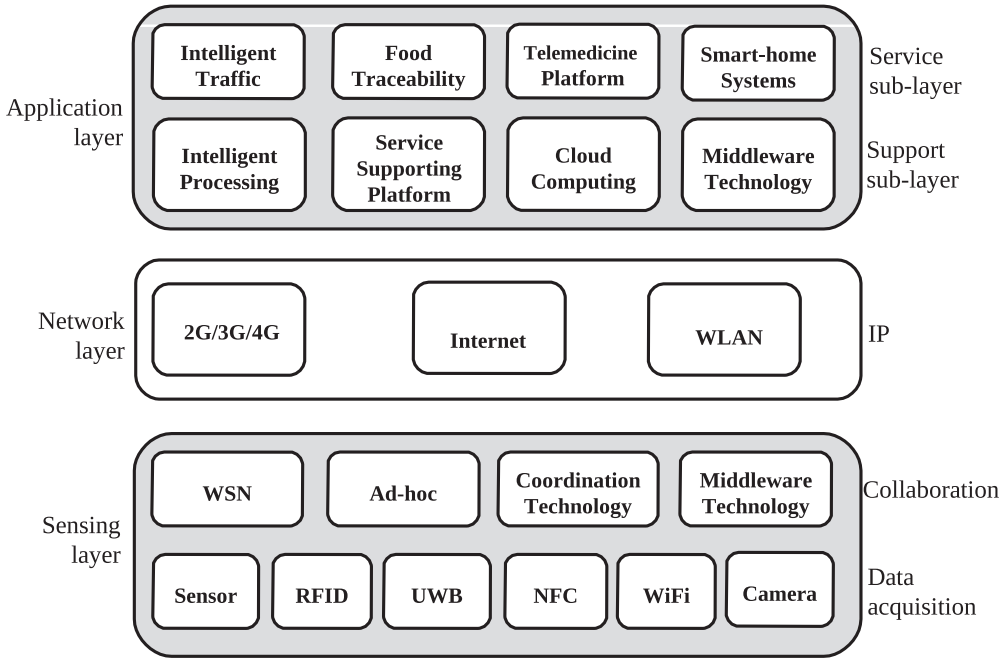
Recent advances in processors, storage, networking technologies, embedded systems along with improvements in software have covered the way for the new paradigm known as the Internet of Things (IoT). In IoT, many things with networking and processing capabilities communicate with each other locally or remotely using the Internet. In the IoT environment, a thing could be a virtual or physical object, a person or an animal attached with a unique identifier (i.e., device ID or IP address) [1]. A physical object may be a smartphone, sensor, camera, drone or vehicle, whereas a virtual object can be considered as an electronic ticket, book, wallet or agenda. In the future, it is expected that the majority of IoT devices will be smart in the sense that they can make decisions on their own.

The IoT vision aims to provide direct merger of the physical world with Internet-connected computer based systems to improve efficiency and cost as well as minimize human involvement. Thus, the IoT ecosystem includes network users, computing systems and interconnected physical/virtual devices with sensing as well as actuating capabilities. IoT devices communicate with each other using the standard Internet communication protocol. The evolution of IoT in recent years continues to be shaped by research developments in various other fields such as smart sensors, Radio-Frequency Identification (RFID), and communication protocols [2].

Fig. 1 illustrates the basic three-layer architecture model of IoT which consists of three layers namely, sensing, network and application. Together these layers support three basic tasks which include: (1) perception, (2) transmission, and (3)

* Corresponding author.
E-mail addresses: szeadally@uky.edu (S. Zeadally), ashok.das@iiit.ac.in (A.K. Das), nsklavos@ieee.org (N. Sklavos).

https://doi.org/10.1016/j.iot.2019.100075
2542-6605/



WLAN: Wireless Local Area Network; **WSN:** Wireless Sensor Network;
RFID: Radio Frequency Identification; **UWB:** Ultra-Wide Band; **NFC:** Near-Field Communication

Fig. 1. Basic three-layer architecture model of IoT (Adapted from: [3]).

processing. In the sensing layer, comprehensive perception is achieved by different types of sensors which collect real-time data. The network layer performs secure transmissions and transfers data from the sensing layer to the application layer. The intelligent control and processing of the collected data are implemented in the application layer [3].

1.1. Generic IoT network architecture

Fig. 2 depicts a generic IoT network architecture proposed by Challa et al. [1,4]. In this architecture, the authors considered four scenarios (e.g., transport, home, national and community). Based on the applications, several IoT smart devices (e.g., actuators and sensors) are deployed in the IoT environment. The connection among IoT devices is through the Internet via authorized Gateway Nodes (GWNs). The data collected by the smart devices can be further provided by some users (e.g., a doctor in healthcare application and a user in smart home application) depending on the application scenarios [5–7]. Cyber-physical systems (e.g., smart home, smart grid and intelligent transportation) are also parts of the IoT ecosystem [8].

1.2. Proliferation of IoT devices

As the cost of various IoT devices continues to decrease and various new IoT application scenarios emerge, we have been witnessing a rise in the deployment of all kinds of IoT devices in various sectors (health, transport, smart grid, and so on). The number of IoT devices enhanced to 31% year-over-year to 8.4 billion in 2017, and it is approximated that 30 billion devices will be by 2020. The IoT's global market value is also estimated to have 7.1 trillion US dollars by the year 2020 [2]. Since the number of connected IoT smart devices is expected to continue to increase in future, it is expected that various types of vulnerabilities will emerge in the IoT environment in the near future.

Several recent vulnerabilities have been discovered with a huge impact more than ever before [9]. For example, there were attacks on controller area networks, which are mounted in all modern cars. These attacks can seriously interrupt vehicle safety functions. Therefore, rather than being based on specific products or specific vendors, such vulnerabilities have a much wider impact.

As the number of IoT products as well as platforms keeps growing, the number of professional security organizations, initiatives and standards for IoT have also started to emerge. According to the analysis provided in [9], currently over 300 to 400 different IoT platform products are available. For example, is an end to end reference architecture along with family of products are included in the Intel® IoT platform. It collaborates with the third party solutions in order to deliver various services including the trusted data delivery to the cloud [10].

Please cite this article as: S. Zeadally, A.K. Das and N. Sklavos, Cryptographic technologies and protocol standards for Internet of Things, Internet of Things, https://doi.org/10.1016/j.iot.2019.100075

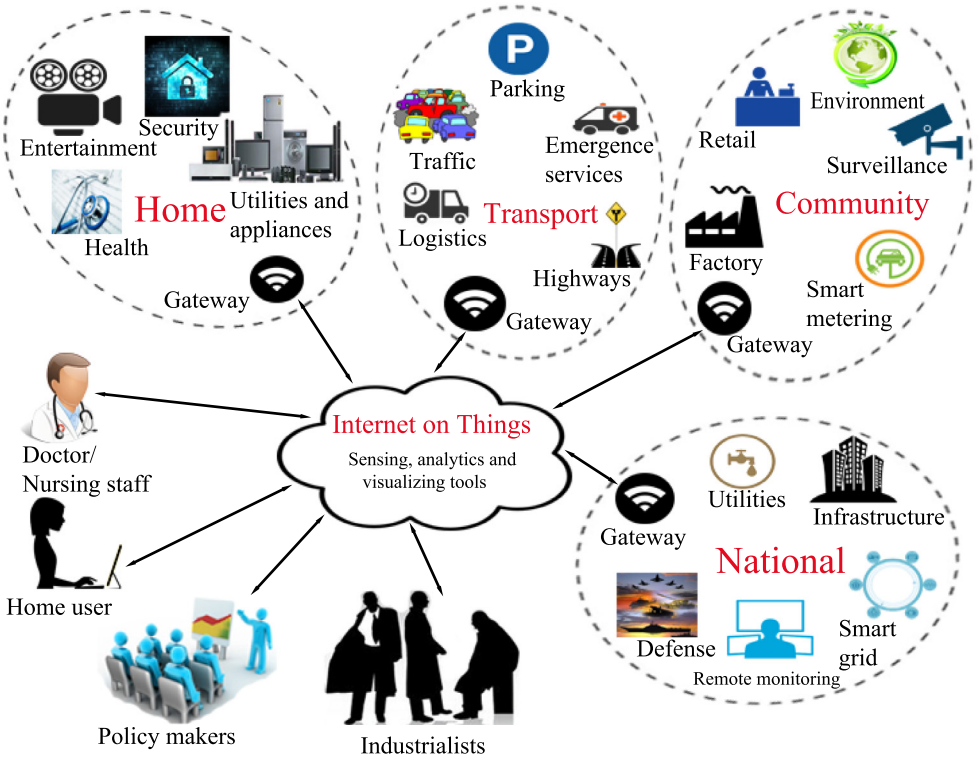


Fig. 2. A generic IoT networking architecture (Adapted from: [1,4]).

The product manufacturers for IoT devices and appliances, particularly on the consumer side, deliver poorly implemented security solutions [9]. Many of these devices are riddled with security vulnerabilities and are a significant threat when connected to the Internet not only to the local network but to other Internet-connected devices as well. Current IoT products are mostly being developed and sold to consumers with ease of use, deployment, and low prices in mind instead of security by design. At present, convenience brought about by IoT products and applications overrides security and privacy issues for consumers [11]. However, as security and privacy awareness and requirements increase around these consumer IoT products, manufacturers will need to invest more to ensure robust security and privacy for IoT devices and applications.

1.3. Research contributions

The main contributions of this work are summarized as follows.

- We discuss various security issues as they pertain to IoT devices. In this work, we only focus on the encryption protocols and digital signatures for the IoT environment. We have already discussed other security issues such as key management, user authentication, device authentication, access control, user access control, privacy preservation and identity management in a previous publication [12].
- Next, we review current standard cryptographic security protocols that have been proposed for IoT devices by leading international standardization organizations.
- We compare these cryptographic protocol standards for various domains such as connected vehicles, consumer IoT, health and medical devices, and smart homes.
- Finally, some future research directions are highlighted.

The rest of the paper is organized as follows. Section 2 briefly reviews some of the security issues related to IoT devices. Section 3 presents cryptographic protocol standards for IoT. Section 4 compares them for different IoT environments. Finally, we make some concluding remarks in Section 5.

2. Security of IoT devices

Security in an IoT environment includes the security of IoT devices, communication channel as well as applications. Next, we present the threat model for the IoT environment and its security requirements.

Please cite this article as: S. Zeadally, A.K. Das and N. Sklavos, Cryptographic technologies and protocol standards for Internet of Things, Internet of Things, https://doi.org/10.1016/j.iot.2019.100075

2.1. Threat model

We follow the similar threat model as discussed in [12]. In the IoT environment, users and smart devices frequently transfer via insecure (public) communication channels because they are linked through the Internet making such channels prone to various types of attacks. Some of the common attacks in the IoT environment include replay, man-in-the-middle, impersonation, denial-of-service, physical IoT device capture, privileged insider, and stolen-verifier attacks. We have provided an in-depth discussion of these attacks in [12].

We present the threat model for IoT below.

- The broadly accepted common threat model, known as the Dolev-Yao (DY) threat model [13], permits any two entities/parties in IoT to exchange over a public medium. Under this model, an adversary $\mathcal{A}$ has the capability not only to capture the messages being transmitted during communication, but also alter, delete or even insert counterfeit information. Moreover, the end point communicating parties, such as users and IoT smart devices, may not be reliable.
- The current *de facto* standard model, known as the Canetti & Krawczyk's adversary model (CK-adversary model) [14,15] can also be applied to IoT. The CK-adversary model can be used to evaluate the security of authenticated key exchange protocols in IoT. The CK-adversary model permits $\mathcal{A}$ to perform all the operations possible under the DY model and also to negotiate the secret information including the states and keys in a session. In authenticated key exchange protocols, the security of such protocols should ensure that if short term secrets or keys in a session are leaked, other secret information of the communicating entities in the network should not be revealed [16].
- IoT smart devices are not generally made with tamper-resistant hardware because of high costs. This enables an adversary $\mathcal{A}$ to easily extract the secret credentials stored on the smart devices when the adversary is in possession of these devices. $\mathcal{A}$ can then use the extracted credentials to compromise the secure communication among the IoT smart devices and users.
- The *GWN* (shown in Fig. 2) in the IoT environment is a fully reliable. It also assumes that $\mathcal{A}$ cannot compromise the *GWN* because it can be physically secured by putting it in a secure place [7].

2.2. Security requirements

Security of IoT devices is currently receiving a lot of attention from researchers and designers because of various issues which include:

- *Leakage of private information:* In user authentication protocols, a user's smart card may store several secret credentials. If an adversary extracts the data from the lost/stolen smart card of a legitimate user, the adversary can launch a user impersonation attack and break the session key of the security protocol. Consider the following scenario where the IoT smart devices attached to the Industrial IoT (IIoT) communicate with humans including their private, personal information [17]. In the IIoT environment, a lot of information is gathered and then disclosed to the Internet without approval by an explicit person. In this way, IoT smart devices constitute a threat for privacy [18]. This requires privacy preservation of the information in the manufacturing industries wherein IIoT is mostly used. Hence, it is important to protect private information of the smart devices and users from an adversary [19].
- *Access to home devices:* Another application of IoT, namely, the smart home environment wherein the physical theft of IoT devices is possible [7]. As mentioned in the threat model (Section 2.1), an adversary $\mathcal{A}$ can take out the secret information available in IoT smart devices that are physically captured by $\mathcal{A}$. With the help of the extracted secret credentials, it may be possible for $\mathcal{A}$ to launch an attack such as the device impersonation attack.
- *IoT botnet:* With an increase of IoT devices [20], there is also an increase in the number of cyberattacks as well as botnets [21]. A collection of compromised servers or computers (zombies) are infected with malware in a typical botnet. These zombies permit an adversary to dominate and set up the intended activities on behalf of the adversary. In contrast, in an IoT botnet, various compromised IoT smart objects, such as cameras, sensors and wearable devices that are infected with malware enable the adversary to control the IoT smart objects for carrying out activities as in a traditional botnet. The main difference between the traditional and IoT botnets is that in the case of the latter, infected IoT devices continue to distribute their malware to many other devices [22]. An IoT botnet has larger scale as compared to a traditional botnet [21]. However, new cyber-storm clouds are also gathering. Based on the information available by Check Point Software Technologies Ltd. [22], a brand new Botnet, called 'IoTroop' has been invented, which can evolve and recruit the IoT sensing devices at a far greater pace and with more potential damage than the Mirai botnet of 2016. Since IoT botnets continue to emerge, they are being exploited to initiate Distributed Denial-of-Service (DDoS) attacks. IoT devices typically run Linux and Unix-based systems. Therefore, an attacker often targets the executable and linkable format binaries for Intel architectures, which are found in embedded systems' firmware.

Due to the above issues and the threat model discussed in Section 2.1, similar to any other networks (e.g., Wireless Sensor Network (WSN) & Ad Hoc Networks) shown in Fig. 1, we also need to meet the following general security requirements in IoT [12]:

- *Authentication:* It is needed to authenticate various nodes, such as IoT smart devices, users as well as gateway nodes prior to their access to a constricted resource, or divulging important private data.

Please cite this article as: S. Zeadally, A.K. Das and N. Sklavos, Cryptographic technologies and protocol standards for Internet of Things, Internet of Things, https://doi.org/10.1016/j.iot.2019.100075

- *Integrity:* It is needed to ensure that the considered message or entity has not been altered in transit in order to ensure integrity.
- *Privacy (Confidentiality): Privacy* enables users to have control over information about them. This control includes who can collect and store the information, the type of information collected, and to whom such information can be disclosed later [23]. In contrast, *data confidentiality* ensures that private or confidential information is not disclosed to unauthorized individuals [23]. It is then needed to protect a communication channel's privacy from the illegal reveal of private information in the IoT environment.
- *Availability:* Only allow authorized users should be allowed access to the relevant network services even under DoS or DDoS attacks on the system.
- *Non-repudiation:* An illegal party should be prohibited from hiding his/her malicious activities.
- *Authorization:* Only the believable IoT smart objects should be allowed to provide network service.
- *Freshness:* It should be ensured that only fresh messages are exchanged and no old messages be sent again by an attacker intentionally.

In an IoT network, sometimes an IoT device may leave the network or may also join the network. The following properties should also be fulfilled in addition to the above security requirements:

- *Forward secrecy:* In this case, when an IoT smart device exits the network, it should not be able to acquire future messages.
- *Backward secrecy:* A newly joined IoT smart device in the network must not have access to any previously exchanged messages.

3. Cryptographic technologies and protocol standards for IoT

Salman and Jain [24] recently provided a detailed survey of various protocols for IoT. They emphasized that various standards by the "Institute of Electrical and Electronics Engineers (IEEE)", "Internet Engineering Task Force's (IETF)" and International Telecommunication Union (ITU) are essential for enabling the fast growth of IoT.

We emphasize that security is one of the most interpretative challenges in IoT platforms. As a result, several standards, drafts as well as research work have been proposed. Although there are some security features within IoT protocols, it is not enough to fully secure the IoT systems [24].

In this review article, we review cryptographic technologies and protocol standards that have been recommended for use by IoT systems and devices. We also reviewed some of the recent recommendations made by the National Institute of Standards and Technology (NIST) [25].

3.1. Cryptographic techniques

Cryptographic mechanisms are required to secure IoT data at rest or in transit. These techniques provide several security requirements, such as confidentiality, data integrity, entity authentication, message authentication, key management, non-repudiation, trustworthy data platforms, and digital signatures.

Das et al. [12], in their previous work, presented a generalized taxonomy of various security protocols needed for the IoT environment. Their taxonomy included various important security services such as key management, user and device authentication, access control, privacy preservation, and identity management. They also presented a detailed comparative analysis of recently proposed IoT-related state-of-art security protocols for various security and functionality features. Furthermore, they discussed various security challenges that need to be addressed to improve IoT security in the future. In contrast to the previously published work [12], in this review paper, we focus on various encryption protocols, digital signatures, Information Security Management Systems (ISMS) and system security engineering relevant to the IoT environment.

3.1.1. Encryption protocols

In this section, we discuss areas in the IoT ecosystem where cryptographic protocols and standards are implemented.

- *Wearables security:* Wearable devices play important roles in healthcare. The wireless communication among wearable devices and between them and the servers may be susceptible to various malicious attacks which can affect safety and privacy of the patient health data. Due to resource limitations of wearable devices, current cryptographic protocol standards that are being used to provide security for wearables include Secure Hash Algorithm (SHA) & Advanced Encryption Standard (AES).
- *Device security:* Encryption protocol standards used for IoT device security include Public Key Exchange (PKE), Transport Layer Security (TLS) and Wi-Fi Protected Access II (WPA2) [26].
- *Network security:* The standards for network security support various security necessities along with the recommendations on processes and methods to achieve various activities, such as secure management and operation. Several network security standards exist for different types of networks that are applicable to IoT systems. Some of these network security standards applicable to IoT systems include [25]:

Please cite this article as: S. Zeadally, A.K. Das and N. Sklavos, Cryptographic technologies and protocol standards for Internet of Things, Internet of Things, https://doi.org/10.1016/j.iot.2019.100075

– Third Generation Partnership Project (3GPP) Long-Term Evolution (LTE) is used for high-speed wireless communication for mobile smart phones. It provides various security services, such as secure access to services for IoT users, secure transmission of signaling data and user data, and secure access to mobile stations including mutual authentication along Universal Subscriber Identity Module (USIM) and User Equipment (UE) [27]. The security standards used in LTE include Advanced Encryption Standard (AES) and Cipher-based Message Authentication Code (AES-CMAC) [28].
– The Bluetooth wireless standard enables the exchange of information over short range communication from fixed and mobile IoT devices. The preliminary security services provided in the Bluetooth standard include authentication, confidentiality, authorization and message integrity [29]. The Bluetooth device authentication mechanism uses a challenge-response method. A device which interacts in an authentication process is known as the claimant or the verifier. The claimant attempts to prove its identity whereas the verifier validates the claimant's identity. The challenge-response protocol permits the devices to validate each other by verifying the knowledge of a secret key called the Bluetooth link key [29]. The latest Bluetooth 4.2 core specification provides various mechanisms to secure communication between devices and also to establish trusted connections [30]. The Elliptic Curve Diffie-Hellman (ECDH) key agreement, FIPS-approved Hash Message Authentication Code Secure Hash Algorithm 256-bit (HMAC-SHA-256) and FIPS-approved AES-Counter with CBC-MAC (AES-CCM) are used in the Bluetooth as cryptographic protocol standards [29].
– Zigbee 3.0 relies on the IEEE 802.15.4 standard specifications that supports 2.4 GHz global frequency band. Using the ZigBee 3.0 specification, the IoT components from different IoT systems/applications are able to communicate each other [31]. The security measures supported by ZigBee networks include access control lists, key-based encryption of communications, and frame counters. Using an access control list, only already decided nodes can take part in the network. The key-based encryption is used in network communications in order to prevent (unauthorized) external parties from interpreting ZigBee network data [31]. Thus, the security measures are applied to avoid intrusion from potentially hostile entities and also from neighboring ZigBee networks. The 128-bit AES-based encryption is used for network communications in order to prevent external agents from interpreting ZigBee network data [31].

For wide area data transmissions such as those involving the cloud infrastructure, encryption protocol standards (e.g., Secure Sockets Layer (SSL) and Internet Protocol Security (IPSec)) are used.

- *Cloud security:* It is necessary to protect the information stored in the cloud for confidentiality reasons [32]. In cloud computing, a remote server stores the data. Thus, a user has no jurisdiction over the stored data. Whether it is an external or internet intruder, there is a threat to the data confidentiality. From cloud service providers point of view, it is essential to assure the availability of information, which is directly associated to their business engrossment [32,33]. Encryption protocol standards used to secure data in the cloud include SSL and Internet Protocol Security (IPSec).

We discuss the following well-known cryptographic algorithm standards that protect the confidentiality or privacy of information next.

Symmetric cryptographic encryption protocols: AES block cipher [34] is part of the "International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 18033-3:2010 standard" which specifies encryption systems (ciphers) for providing data confidentiality service. AES is considered as the desired block cipher for the "Institute of Electrical and Electronics Engineers (IEEE) 802.11 wireless technologies" in order to provide security over wireless networks, and is used to implement in version 1.3 of the "Internet Engineering Task Force's (IETF) Transport Layer Security (TLS) protocol" [25]. In addition, the AES standard has widespread market acceptance in terms of testing as well as implementation in hardware and software [25].

Asymmetric cryptographic encryption protocols: Public key cryptography standards are also broadly available. The IETF developed many asymmetric cryptography standards, such as "RSA and Elliptic Curve Cryptography (ECC)" for Internet applications which include "Simple Mail Transfer Protocol (SMTP – RFC 2821), Internet Message Access Protocol (IMAP –RFC 3501), Secure File Transfer Protocol (SFTP – RFC 959) and IoT" [35]. The IEEE 1363 working group also published several standards for public key cryptography, which include "IEEE 1363.1–2008 (public key cryptographic techniques based on hard problems over Lattices), IEEE 1363–2000 (common public-key cryptographic techniques), IEEE 1363.3–2013 (identity-based cryptographic techniques using pairings), IEEE 1363a-2004 (additional public-key cryptographic techniques beyond those in IEEE standard 1363–2000), and IEEE 1363.2–2008 (password-based public-key cryptographic techniques)".

Encryption protocol standards for resource-constrained devices: In various IoT environments such as wireless sensor networks, healthcare, cyber-physical systems, and smart grid, IoT devices are often highly resource-constrained and typically communicate via wireless communication technologies such as Zigbee and Bluetooth. A lightweight cryptographic protocol makes use of only a few cryptographic operations along with the use of security parameters that are of small sizes (e.g., smaller key sizes and message sizes) which will reduce the computation and communication costs for the IoT devices. Lightweight cryptography standards are therefore needed because of the limited resources (computing, storage and so on) available on these devices. Based on the recently published report in [25], NIST recommended some lightweight cryptography standards for the IoT environment, which are presented in Table 1. In Table 2 also presents various well-known, commercial IoT products and their relevant encryption technologies.

Please cite this article as: S. Zeadally, A.K. Das and N. Sklavos, Cryptographic technologies and protocol standards for Internet of Things, Internet of Things, https://doi.org/10.1016/j.iot.2019.100075

Table 1
Lightweight cryptography standards for the IoT environment.

Standard	Year	Description
ISO/IEC–29192-1	2012	It covers "General information technology including security mechanisms, lightweight cryptography (Part 1)".
ISO/IEC–29192-2	2012	It covers "Information technology for security mechanisms, lightweight cryptography for block ciphers (Part 2)".
ISO/IEC–29192-3	2012	It covers "Information technology for security mechanisms, lightweight cryptography for stream ciphers (Part 3)".
ISO/IEC–29192-4	2013	It covers "Information technology for security mechanisms, lightweight cryptography for asymmetric techniques (Part 4)".
ISO/IEC–29192-5	2016	It covers "Information technology for security mechanisms, lightweight cryptography for hash functions (Part 5)".

Table 2
Commercial IoT products and their encryption technologies.

Commercial IoT product	Encryption technology used
Samsumg SmartThings [36]	AES
ARM mbed [37]	AES-CBC
Apple Homekit [38]	AES, SHA-512
Ericsson Calvin [39]	RSA, SHA-256
Kura [40]	AES, SHA-1
Microsoft Azure [41]	AES, Triple Data Encryption Standard (3DES)
Google's Brillo/Weave [42]	SSL/TLS, OAuth 2.0 Authentication
Amazon AWS [43]	Elliptic Curve Diffie-Hellman, RSA

Table 3
Cryptography protocol standards for ISMS in IoT-based cloud services.

Standard	Description
ISO/IEC 27036-4;2016	Covers "Information technology – Information security for supplier relationships – Part 4: Guidelines for security of Cloud services"
ISO/IEC 27018:2014	Covers "Code of practice for protection of personally identifiable information in public clouds acting as PII processors"
ISO/IEC DIS 19941	Covers "Information technology – Cloud computing – Interoperability and portability"
ISO/IEC FDIS 19944	Covers "Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use"
ISO/IEC 27017:2105	Covers "Code of practice for information security controls based on ISO/IEC 27002 for cloud services"

3.1.2. Digital signatures

A digital signature assures that the claimed signer has signed the message and that the message was not altered after the signature was generated using the signer's private key. A verifier who is having the signer's public key can validate the signer's signature. Digital signature is widely used in various technologies, such as Connected Vehicle Systems (CVS) and in cryptographic-enabled protocols (e.g., "IP Security (IPSec), Secure/Multipurpose Internet Mail Extension (S/MIME), and Transport Layer Security (TLS)"). Consider the following batch verification case in IoT. The authentication of every message being transmitted in an IoT environment becomes a challenging task because of the resource limitations of the IoT devices. Therefore, individual verification of digital signatures leads to reduction in the real-time IoT system's performance. In contrast, if the signatures are validated in batches, it leads to significant reduction in the verification time. Hence, with batch verification in IoT, digital signature plays an important role [44].

Some commonly used digital signature algorithms are "RSA with Public-Key Cryptography Standards (PKCS) 1 or Probabilistic Signature Scheme (PSS) padding schemes [45]; Digital Signature Algorithm (DSA) (FIPS 180–4); and Elliptic curve DSA (ESDSA) (FIPS 186–4)" [46]. RSA with PKCS is used for batch verification [44] in IoT. Since RSA with PKCS is expensive for resource-limited IoT devices, the lightweight ESDSA [46] is preferred for batch verification in IoT.

3.2. Information security management systems (ISMS)

The Information security management system (ISMS) standards issued by NIST can be defined as "a collection of processes and their respective security controls for establishing a governance, risk, and compliance structure for information security for an organizational unit, an organization, or a set of processes controlled by a single organizational entity" [25]. There are several ISMS standards with market acceptance which can be typically applied to IoT systems or particular IoT applications. Table 3 presents some of the standards which are of direct relevance to cloud services in the IoT environment.

3.3. System security engineering

System security engineering standards relate design and planning tasks that satisfy security requirements in order to reduce a systems susceptibility to threats, enforce organizational security policy, and increase system resilience. Several

Please cite this article as: S. Zeadally, A.K. Das and N. Sklavos, Cryptographic technologies and protocol standards for Internet of Things, Internet of Things, https://doi.org/10.1016/j.iot.2019.100075

Table 4
System security engineering standards.

Standard	Description
ISO/IEC 15026-2:2011	Covers "Systems and software engineering – Systems and software assurance – Part 2: Assurance case".
ISO/IEC 15026-4:2012	Covers "Systems and software engineering – Systems and software assurance – Part 4: Assurance in the life cycle".
ISO/IEC 20243:2015	Covers "Information Technology – Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products".

Table 5
Comparison of cryptographic protocol standards for various IoT application domains.

Core Areas of Standardization	Standards	Connected Vehicles	Consumer IoT	Health IoT & Medical Devices	Smart Home/ Buildings
Cryptographic Mechanisms	IEEE ISO TC 307 ISO TC 68 ISO/IEC JTC 1	SA SU	SA SU	SS SU	SA SU
ISMS	ISO/IEC JTC 1 ISO TC 223	SS SU	SS SU	SS SU	SS SU
Network Security	3GPP IEC IEEE IETF ISO/IEC JTC1	SN NI	SN NI	SN NI	SN NI
System Security Engineering	IEC ISO/IEC JTC 1 IEEE	SS SU	SN SU	SS SU	SN SU

SA: Standards Available; SS: Some Standards; SN: Standards Needed; I: Implemented; SU: Slow Uptake; NI: Not Implemented.

draft/approved system security engineering standards exist that are associated to IoT systems or particular IoT systems (e.g., healthcare applications). These standards are relevant for IoT systems because of the following reasons: (1) they identify, specify, design, and develop protective measures to address system vulnerabilities, (2) they assess and understand susceptibility to threats in the actual/projected domain of operation, and (3) they identify and assess exposures in the system and its domain of operation [25]. Table 4 presents various relevant international standards.

4. Comparison of cryptographic protocol standards for IoT

This section compares the protocol standards for IoT that we have discussed earlier (Section 3) and we discuss their market impact in terms of their deployment in commercial IoT products. We also identify some of the limitations of the standards such as use of software patches to fix security flaws, detecting malware in software, and requirement of updates and/or new standards needed to direct IoT networks that have the prospective for voluntary connections (due to the networking) without a system view [25].

Table 5 presents a summary of the current status of cryptographic protocol standards for various IoT application domains and their implementation in the market place based on the report developed by NIST [25]. The following standardization organizations are considered in the comparative study: "Institute of Electrical and Electronics Engineers (IEEE)", "International Organization for Standardization (ISO)", "International Electrotechnical Commission (IEC)", "Third Generation Partnership Project (3GPP)", and "Internet Engineering Task Force (IETF)" [25].

Table 5 uses the following notations:

- *Standards available (SA):* Standard organizations have developed cryptographic protocol standards.
- *Some standards (SS):* Standardization organizations have approved cryptographic protocol standards which exist but there may be requirements for additional revisions and/or standards to existing standards in some specific application area.
- *Standards needed (SN):* New cryptographic protocol standards development projects are being reviewed by many standardization organizations.
- *Implemented (I):* Two or more standards-based implementations are accessible for majority of the cybersecurity standards accepted by the standardization organizations.
- *Slow uptake (SU):* Market implementations do not yet incorporate many cryptographic protocol standards approved by standardization organizations.
- *Not implemented (NI):* Cryptographic protocol standards are still under development or new standards need to be developed prior to their implementation in products on the market.

Please cite this article as: S. Zeadally, A.K. Das and N. Sklavos, Cryptographic technologies and protocol standards for Internet of Things, Internet of Things, https://doi.org/10.1016/j.iot.2019.100075

NIST studied the impact of cryptographic protocol standards on commercial IoT products and identified the following issues [25]:

- *Cryptographic techniques:* The AES standard has strong market acceptance. For example, it is included in testing and validation of thousands of implementations of commercial IoT products. However, recently approved RFID standards [47] and lightweight cryptographic standards have no commercial implementations or only one commercial implementation (e.g., "the RFID standard ISO 17367:2009 (Supply chain applications of RFID –Product tagging) defines the basic features of RFID for use in the supply chain when applied to product tagging" [48]).
- *Information security management systems (ISMS):* ISMS provides management requirements for IoT devices, such as medical devices and their related services [25]. As reported by NIST in [25], there are many ISMS standards that can be applicable to IoT systems or particular IoT applications (e.g., healthcare).
- *Network security:* Several existing standards, such as 3GPP, IES, IEEE, IETF and ISO/IEC JTC1, are used in commercial IoT product implementations.
- *System security engineering:* It is not clear so far if the system security engineers apply system engineering practices when they design and implement IoT systems. For example, it is not clear whether the generic system engineering standards (e.g., ISO/IEC 15026) takes into account of IoT systems as part of the IT system [25,49].

NIST has also identified several standardization areas where more work is needed [25] to improve IoT security in the future:

- *Cryptographic techniques:* A blockchain is considered as "a growing list of records (called blocks) which are linked (connected) using cryptographic techniques". Each block of a blockchain has a cryptographic hash of the previous block along with a timestamp and transaction data. It is being increasingly used in several application areas, such as identity management systems [50] and Industry 4.0 [51]. Future cryptographic protocol standards need explore blockchain technology for IoT security mechanisms. For instance, consider the smart home application in the IoT environment [52]. The smart home miner is responsible for centrally processing of incoming and outgoing transactions to and from the smart home. The miner could incorporate with the home's Internet gateway that can be deployed between the IoT devices and the home gateway. Apart from the security task of the miner, such as authentication, authorization and auditing of transactions, the miner may also accomplish some additional functions, such as distributing and updating keys, changing the transactions structure as well as forming and managing the cluster. In this scenario, the miner may gather all transactions into a block and append the full block to the blockchain.
- *ISMS:* Management system standards based on the "standard ISO/IEC 27002 for IoT applications" are not covered by the 27000 series standard which describes information security control objectives arising from risks to the integrity, availability and confidentiality of information.
- *Network security:* Current standards need updates and/or new standards need to be developed in order to address IoT networks that generate spontaneous connections without any knowledge of the entire system.
- *System security engineering:* We need to check if the generic system security engineering standards (e.g., ISO/IEC 15026) can be applied to IoT systems.

5. Conclusion and future research directions

In this review article, we described various security threats faced by current IoT systems and we reviewed current cryptographic security standards for IoT devices and systems. Based on the recent findings of NIST, we presented a comparative study of the various protocol standards for several IoT application domains followed by the standardization areas for cryptographic protocols where more work is needed to support IoT security in the future.

Several future research directions are worth investigating. As pointed out by NIST in [25], the 80-bit key size of a symmetric key cryptographic algorithm (e.g., Double Data Encryption Standard (2DES)) provides the equivalent security for the 1024-bit RSA and 160-bit ECC [53]. ECC provides the same security as that for RSA with much smaller key length and it is included as an accepted cryptographic protocol standard (ISO/IEC 29192-4:2013). Since ECC allows the same level of security as compared to RSA but with much smaller keys and signatures, ECC has become a more popular cryptographic solution in several Internet protocols, such as "TLS version 1.3 (RFC 8446), Datagram Transport Layer Security (DTLS) (RFC 6347), and Internet Key Exchange for IPSec (RFC 7296)". Moreover, lightweight cryptographic protocol standards need to be applied to resource-constrained devices which are frequently round in IoT systems. Therefore, lightweight symmetric encryption algorithms as defined in standard ISO/IEC 29192–2 and also the lightweight public key-based ECC cryptosystem, need to be considered for future IoT applications and systems.

Declaration of competing interest

We do not have any conflicts of interest.

Please cite this article as: S. Zeadally, A.K. Das and N. Sklavos, Cryptographic technologies and protocol standards for Internet of Things, Internet of Things, https://doi.org/10.1016/j.iot.2019.100075

Acknowledgments

The authors thank the anonymous reviewers and the editor for their valuable feedback on the paper which helped us to improve its quality and presentation.

References

[1] S. Challa, M. Wazid, A.K. Das, N. Kumar, A.G. Reddy, E.J. Yoon, K.Y. Yoo, Secure signature-based authenticated key establishment scheme for future IoT applications, IEEE Access 5 (1) (2017) 3028–3043.
[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of Things: a survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2347–2376.
[3] O. Mouaatamid, M. Lahmer, M. Belkasmi, Internet of Things security: layered classification of attacks and possible countermeasures, Electron. J. Inf. Technol. 9 (2016) 66–80.
[4] M. Wazid, A.K. Das, R. Hussain, G. Succi, J.J.P.C. Rodrigues, Authentication in cloud-driven IoT-based big data environment: survey and outlook, J. Syst. Archit. 97 (2019) 185–196.
[5] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.
[6] M. Wazid, A.K. Das, V. Odelu, N. Kumar, M. Conti, M. Jo, Design of secure user authenticated key management protocol for generic IoT network, IEEE Internet Things J. 5 (1) (2018) 269–282.
[7] M. Wazid, A.K. Das, V. Odelu, N. Kumar, W. Susilo, Secure remote user authenticated key establishment protocol for smart home environment, IEEE Trans. Dependable Secure Comput. (2017), doi:10.1109/TDSC.2017.2764083.
[8] L. Atzori, A. Iera, G. orabito, The Internet of Things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.
[9] J. Grimm, The proliferation of IoT devices will lead to more data breaches, 2018, http://www.information-management.com/opinion/the-proliferation-of-internet-of-things-devices-will-lead-to-more-data-breaches. Accessed on August.
[10] Intel ® IoT platform, 2018, https://www.intel.in/content/www/in/en/internet-of-things/infographics/iot-platform-infographic.html. Accessed on July.
[11] A.J. Perez, S. Zeadally, Privacy issues and solutions for consumer wearables, IT Prof. 20 (4) (2018) 46–56.
[12] A.K. Das, S. Zeadally, D. He, Taxonomy and analysis of security protocols for internet of things, Future Gene. Comput. Syst. 89 (2018) 110–125.
[13] D. Dolev, A. Yao, On the security of public key protocols, IEEE Trans. Inf. Theory 29 (2) (1983) 198–208.
[14] R. Canetti, H. Krawczyk, Analysis of key-exchange protocols and their use for building secure channels, in: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques– Advances in Cryptology (EUROCRYPT'01), Springer, Innsbruck (Tyrol), Austria, 2001, pp. 453–474.
[15] R. Canetti, H. Krawczyk, Universally composable notions of key exchange and secure channels, in: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques– Advances in Cryptology (EUROCRYPT'02), Amsterdam, The Netherlands, 2002, pp. 337–351.
[16] V. Odelu, A.K. Das, M. Wazid, M. Conti, Provably secure authenticated key agreement scheme for smart grid, IEEE Trans. Smart Grid 9 (3) (2018) 1900–1910.
[17] F.Z. Berrehili, A. Belmekki, Privacy preservation in the internet of things, in: Proceedings of the Advances in Ubiquitous Networking (UNet'16), Springer, Singapore, 2017, pp. 163–175.
[18] A.J. Perez, S. Zeadally, J. Cochran, A review and an empirical analysis of privacy policy and notices for consumer Internet of Things, Secur. Priv. (2018), doi:10.1002/spy2.15.
[19] J. Srinivas, A.K. Das, M. Wazid, N. Kumar, Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things, IEEE Trans. Dependable Secure Comput. (2018), doi:10.1109/TDSC.2018.2857811.
[20] Information, Matters. the business of data and the Internet of Things (IoT), 2018, http://informationmatters.net/internet-of-things-statistics/.Accessed on August.
[21] A quick history of IoT botnets, 2018, https://blog.radware.com/uncategorized/2018/03/history-of-iot-botnets/.
[22] D. Palmer, Mirai botnet adds three new attacks to target IoT devices, 2018, http://www.zdnet.com/.
[23] W. Stallings, Cryptography and Network Security: Principles and practice, fifth ed., Pearson, Delhi, India, 2011.
[24] T. Salman, R. Jain, A survey of protocols and standards for Internet of Things, CoRR (2019) Abs/1903.11549.
[25] M. Hogan, B. Piccarreta, NIST interagency report (NISTIR) 8200, interagency report on status of international cybersecurity standardization for the Internet of Things (IoT), 2018, https://csrc.nist.gov/publications/detail/nistir/8200/draft. Accessed on August 2018.
[26] Iot Device Security: Built-In, Not Bolt-On, NXP Semiconductors, 2018. http://www.digi.com/pdf/digi-iot-device-security-nxp-wp.pdf.
[27] L. He, Z. Yan, M. Atiquzzaman, LTE/LTE-a network security data collection and analysis for security measurement: A survey, IEEE Access 6 (2018) 4220–4242.
[28] J. Cichonski, J.M. Franklin, M. Bartock, Guide to LTE security, 2017, https://doi.org/10.6028/NIST.SP.800-187.
[29] J. Padgette, J. Bahr, M. Batra, M. Holtmann, R. Smithbey, L. Chen, K. Scarfone, Guide to Bluetooth Security, NIST Special Publication 800–121 Revision 2, 2017. http://www.design-reuse.com/articles/39779/security-considerations-for-bluetooth-smart-devices.html.
[30] H.V. Ravikiran, Security considerations for bluetooth smart devices, 2018, http://www.design-reuse.com/articles/39779/security-considerations-for-bluetooth-smart-devices.html.
[31] , Zigbee 3.0 Stack User Guide, NXP Semiconductors, 2018. http://www.nxp.com/docs/en/user-guide/JN-UG-3113.pdf.
[32] R. Wang, Research on data security technology based on cloud storage, Proc. Eng. 174 (2017) 1340–1355.
[33] Y. Peng, W. Zhao, F. Xie, Z.h. Dai, Y. Gao, D.q. Chen, Secure cloud storage based on cryptographic techniques, J. China Univ. Posts Telecommun. 19 (2012) 182–189.
[34] , Advanced Encryption Standard (AES), FIPS PUB 197, National Institute of Standards and Technology (NIST), U. S. Department of Commerce, 2018. November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Accessed on April.
[35] The Internet of Things, 2018b, https://www.ietf.org/topics/iot/.
[36] Smartthings support, 2017, http://support.smartthings.com/hc/en-us/articles/204392790-Z-Wave-general-info.
[37] ARM Mbed, 2016, http://tls.mbed.org/kb/how-to/encrypt-with-aes-cbc.
[38] D. Hamilton, Apple's homekit security vs. IoT botnets – There's only so much apple can do, 2016, http://www.macobserver.com/analysis/homekit-security-iot-botnets/.
[39] J.M.R. Gil, Secure Domain Transition of Calvin Actors, Master's thesis, Department of Electrical and Information Technology, Faculty of Engineering, LTH, Lund University, 2016.
[40] Kura: interface cryptoservice, 2018, http://download.eclipse.org/kura/docs/api/0.7.0/org/eclipse/kura/crypto/CryptoService.html.
[41] Azure encryption overview, 2018, http://docs.microsoft.com/en-us/azure/security/security-azure-encryption-overview.
[42] B. Beare, Brillo/weave part 1: high level introduction, 2016, http://support.smartthings.com/hc/en-us/articles/204392790-Z-Wave-general-info.
[43] AWS key management service, 2018, http://docs.aws.amazon.com/kms/latest/developerguide/overview.html.
[44] A.S. Kittur, A. Jain, A.R. Pais, Fast verification of digital signatures in IoT, in: Proceedings of the Fifth International Symposium on Security in Computing and Communication (SSCC'17), Manipal, India, 2017, pp. 16–27.
[45] R.L. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126.

Please cite this article as: S. Zeadally, A.K. Das and N. Sklavos, Cryptographic technologies and protocol standards for Internet of Things, Internet of Things, https://doi.org/10.1016/j.iot.2019.100075

[46] D. Johnson, A. Menezes, The Elliptic Curve Digital Signature Algorithm (ECDSA), Departmet of C & O, University of Waterloo, Canada, 1999 Technical report corr 99-34. August 23.
[47] RFID Standards, 2018, http://www.radio-electronics.com/info/wireless/radio-frequency-identification-rfid/iso-epcglobal-iec-standards.php.
[48] S. Tranchard, New ISO RFID standard will help trace products in the supply chain, 2010, http://www.iso.org/news/2010/02/Ref1293.html.
[49] B. Brown, Systems engineering and IoT, 2016, https://www.ibm.com/blogs/internet-of-things/systems-engineering/.
[50] C. Lin, D. He, X. Huang, M.K. Khan, K.K.R. Choo, A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems, IEEE Access 6 (2018) 28203–28212.
[51] C. Lin, D. He, X. Huang, K.K.R. Choo, A.V. Vasilakos, BSein: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0, J. Netw. Comput. Appl. 116 (2018) 42–52.
[52] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: the case study of a smart home, in: Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 2017, pp. 618–623.
[53] E. Barker, Recommendation for key management, 2018, Special Publication 800–57 Part 1 Rev. 4, NIST, 01/2016. Accessed on May.

Please cite this article as: S. Zeadally, A.K. Das and N. Sklavos, Cryptographic technologies and protocol standards for Internet of Things, Internet of Things, https://doi.org/10.1016/j.iot.2019.100075