Vivek V. Jog* and T. Senthil Murugan

A Critical Analysis on the Security Architectures of Internet of Things: The Road Ahead

DOI 10.1515/jisys-2016-0032
Received April 11, 2016; previously published online September 14, 2016.

Abstract: Internet of Things (IoT) has been a most important research area for almost a decade now, where a huge network of billions or trillions of "things" communicating with one another is facing many technical and application challenges. Although there are many uncertainties about its security and privacy, the literature presents different techniques to handle the security issues and challenges in order to develop a well-defined security architecture. This paper reviews 50 research papers that are related to the security of IoT. The security techniques were classified with respect to time consumption, energy consumption, power consumption, lightweight property, reliability, robustness, and smart applicability. Also, the security techniques were analyzed based on the considered attacks, application, utilized simulation tool, security model, and attributes. The objective of the survey is focused on the security loopholes arising out of the information exchange technologies used in IoT. Finally, the important research issues are addressed for the researchers to find the way for further research in the security of IoT. The survey signifies that multilevel and mutual authentication based on attribute-based profile modeling bring more security for access control and authentication.

Keywords: IoT, security, authentication, authorization, access control, application layer.

1 Introduction

The concept of Internet of Things (IoT) is spread throughout our day-to-day life, and the media and business people have identified it as a novel innovation. As the sensors are becoming more comprehensive while trying to satisfy the requirements of end users, using them in daily life is becoming an easy task. Now, the devices that are installed in domestic applications, industries, and smart city infrastructures are connected with the Internet. Such interconnections offer an entire set of data relating to the environment, status of the devices, etc., that can be collected, aggregated, and distributed in a proficient, secure, and private manner. As such devices are interconnected with the Internet, they can be accessed and managed from anywhere at any instance [1]. Figure 1 shows the general architecture of IoT. It has five major layers, including the device layer, network layer, middleware layer, security layer, and application layer [10].

(i) Device layer: The perception layer contains several types of data sensors such as barcodes, radiofrequency identification (RFID), mobiles, tablets, laptops, printers, etc. The function of this layer is the identification of distinctive objects and dealing with the real-world data collected by its corresponding sensors. (ii) Network layer: The function of the network layer is transmission of collected data acquired from the perception layer, to a specific information processing system by means of available communication networks such as the Internet, mobile networks, or other types of networks. (iii) Middleware layer: The middleware layer contains information processing systems that perform automated actions depending on the processed data result. Moreover, it connects the system with the database that offers storage capacity to the collected data. It is a service-based layer that guarantees similar kind of services among the associated devices. (iv)

***Corresponding author: Vivek V. Jog,** Department of Computer Science and Engineering, Vel Tech Dr.RR & Dr.SR Technical University, Chennai, Tamil Nadu 600062, India, e-mail: jog.vivek@gmail.com
T. Senthil Murugan: Department of Computer Science and Engineering, Vel Tech Dr.RR & Dr.SR Technical University, Chennai, Tamil Nadu 600062, India

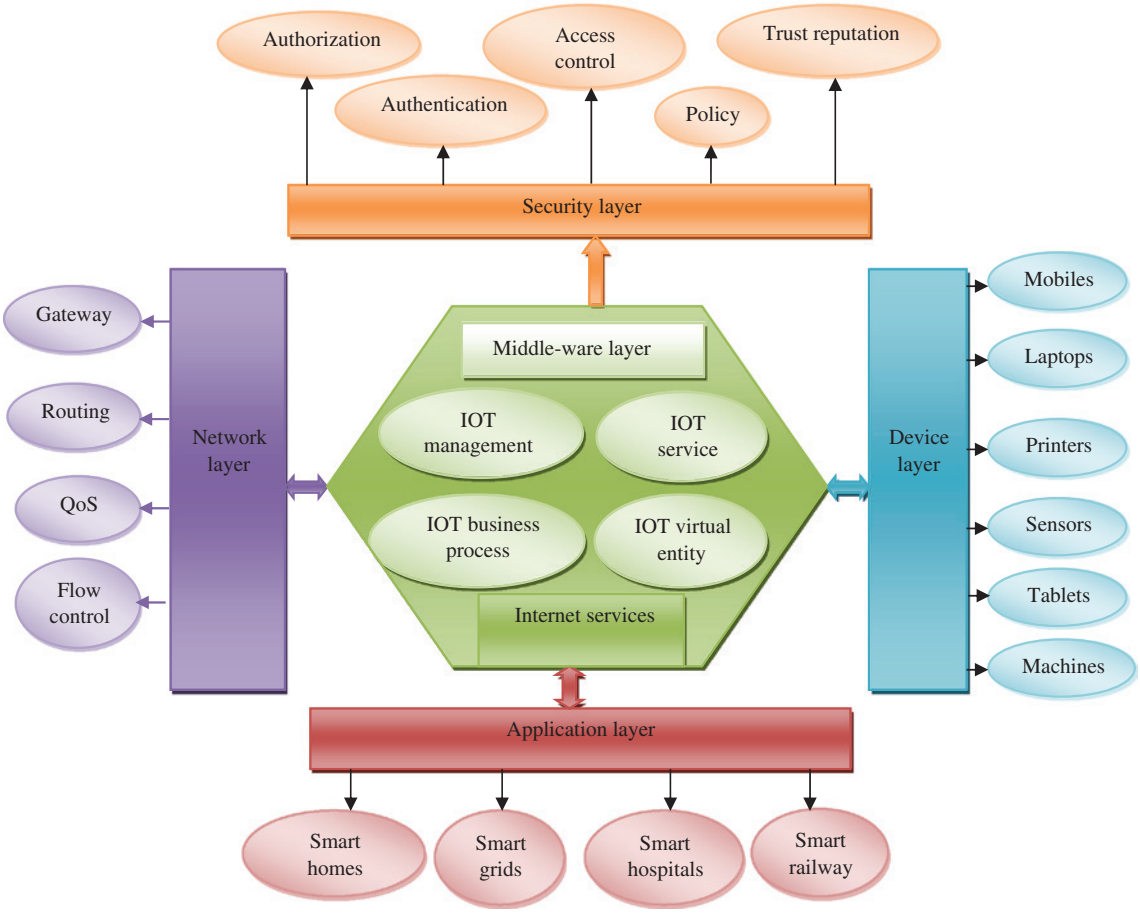

Figure 1: IoT Architecture.

Security layer: Important mechanisms such as authentication, access control, authorization, and policy are performed within the security layer. (v) Application layer: The application layer understands several practical uses of IoT depending on the user requirements and various types of industries, including smart home, smart hospitals, etc.

1.1 Security Requirement

In IoT areas such as remote monitoring and intelligent transport systems, terminal nodes will gather information, which is then transmitted to the IoT platform, and then the platform will send commands to the terminal nodes through the relay devices. Therefore, it is difficult to protect the validity of both the terminal nodes and the platform in such networks [18]. In the security of IoT, several tasks that are to be performed are (i) inserting keying material in the development stage of the device, (ii) demanding new keying material while in operation, (iii) establishing access control policies in order to access the networks and services, (iv) using hardware security modules for protecting keys from tampering, (v) managing software update, and (vi) developing and selecting proficient cryptographic primitives. Traditional security systems provided by the IoT research community presents mainly point solutions; however, this seldom aids in understanding the big picture for securing IoT devices [20]. For the security of IoT, there are several works that are mainly focused on the security architectures and recommended countermeasures, secure communication and networking mechanisms, cryptography algorithms [52, 55], and application security solutions [27, 57].

Recent researches mainly focus on three security aspects, such as system security, network security, and application security. System security concentrates on the entire IoT system to recognize distinctive privacy and security challenges, to devise complete security frameworks, and to afford security measures and strategies. Network security mostly concentrates on wireless communication networks to frame key distribution algorithms, authentication protocols, advanced signature algorithms, access control mechanisms, and secure routing protocols. Specifically, authentication protocols are more common in dealing with security and privacy issues in IoT. Furthermore, heterogeneity and hierarchy should be considered while designing it. The major security goals of IoT are to ensure proper identity authentication mechanisms and provide confidentiality about the data, etc. The available models should implement security by making use of different requirements like data confidentiality, data integrity, data availability confidentiality, policy enforcement, and reputation [4, 30, 39, 44–46].

2 Review of Various Security Protocols of IoT

This section presents the survey of the different security architectures reported in the literature. The security architectures consider the important issues of authentication, authorization, access control, privacy, confidentiality, trust, and reputation. By considering these important issues, different security techniques have been developed in the perspective of time consumption, energy consumption, power consumption, lightweight property, reliability, robustness, and smart applicability. Here, the articles are classified into seven categories: (i) lightweight-based security techniques, (ii) robust security techniques, (iii) power-efficient techniques, (iv) time-efficient techniques, (v) energy-efficient security techniques, (vi) reliable security techniques, and (vii) smart security techniques.

2.1 Lightweight-Based Security Techniques

This section deals with the security techniques related to being lightweight. There are several works that focused on authentication as a security issue in developing security protocols. Accordingly, Hernandez-Ramos et al. [16] have introduced a lightweight authentication and authorization system to maintain smart objects. Moreover, such systems were structured in a security framework that is submissive with the Architectural Reference Model (ARM) newly introduced by the EU FP7 IoT-A project. Also, Kim and Kim [21] have presented a lightweight encryption scheme called PRINCE, and a technique to enhance the message space of PRINCE by enhancing XLS (eXtension by Latin Square). They examined the cryptographic requirements of the inverse-free lightweight encryption scheme and recommended how to expand a PRINCE-like encryption scheme to secure the IoT system.

Another significant lightweight architecture to handle authentication issues is given in Ref. [8], where Fan et al. introduced a lightweight RFID mutual authentication protocol (LRMAPC) with cache in the reader. It stores the recently visited key of tags in LRMAPC, such that recently visited tags are directly authenticated in the reader. LRMAPC can greatly minimize the cost of computation and transmission. Particularly, it can largely minimize the cost of computation if there are more tags to be authenticated. Using GNY Logic, the accuracy of LRMAPC is verified. Further, Raza et al. [37] presented a lightweight 6LoWPAN compressed with IKEv2 for key management for IEEE 802.15.4 link layer security. Hou et al. [17] formulated the lightweight authentication scheme named HB-MAP. In this scheme, the client needs to store only a little amount of messages and do a few bit-wise operations. The server will do the computation-consuming operations such as the generation of random challenges. Last, they carried out security vulnerabilities analysis of the HB-MAP protocol.

Ning et al. [32] concentrated on unit IoT and ubiquitous IoT (U2IoT) architecture to devise an aggregated-proof-based hierarchical authentication scheme (APHA) for the layered networks. Actually, the aggregated proofs were launched for multiple targets to attain forward and backward unspecified data

transmission. The directed path descriptors, homomorphism functions, and Chebyshev chaotic maps were employed together for mutual authentication. Several access authorities were allocated to attain hierarchical access control. In the meantime, the BAN logic formal analysis was carried out to confirm that APHA has no observable security deficiencies, and it was most likely existing for the U2IoT architecture and other IoT applications.

To handle the security and privacy issues in IoT, a lightweight no-pairing ABE scheme based on elliptic curve cryptography (ECC) was given by Yao et al. [54]. Instead of the bilinear Diffie-Hellman assumption, the security of the approach depends on the elliptic curve decisional Diffie-Hellman assumption, and was verified in the attribute-dependent selective-set model. Shi et al. [43] have presented a lightweight authentication scheme to satisfy the need of secure authentication for wireless Internet applications. The scheme was utilized in several authentication circumstances in mobile wireless Internet applications, and offered communication sessions with privacy and security from other networks. It was installed as an add-on module at the application layer, and does not require any modifications to the present Internet applications.

Lightweight security techniques typically provide the same or enhanced services as their heavier counterpart, but have a lighter footprint in various ways. Lightweight protocol codes perform faster than standard protocols. They tend to have a smaller overall size, to leave out unessential data, and might use a data compression technique to have a lighter effect on network communication.

2.2 Robust Security Techniques

There are several studies that considered authentication as an important issue and proved the security issues with a number of attacks. The attacks proved that security techniques are robust techniques in IoT. There are only a few articles in the literature dealing with robust architectures. Three recent articles on IoT are reviewed here. In view of that, Panwar and Kumar [33] have presented an effective Datagram Transport Layer Security (DTLS) mechanism that employs public certificates for authentication, which makes a robust DTLS security. They make use of a certificate authority that can provide the digital certificates to the client as well as the server, and can improve the communication efficiency. They have established a certificate of authority for preshared key communication.

Jan et al. [19] presented a robust mutual authentication approach to authenticate the identities of the contributing devices before involving them in communication. The connection overhead is minimum in this method, and it provides a robust defense solution to combat several kinds of attacks. Leo et al. [26] developed a combined architecture for data and service transactions in IoT scenarios. The architecture model was primarily dedicated to set and handle merged environment for authority delegation mechanism, identity-based capability, and dynamic context information. This architecture supported the security management by applying the SOA technique depending on Web services. It promoted the usage of the SOAP and REST principles related to the characteristics and nature of devices and services. In such a situation, the SMGW manage all security features.

The robust security techniques have the following advantages: (i) A robust protocol can be one that does not break easily for the various attack models; that is, a security architecture in which any individual application can fail without disturbing the system or other applications can be said to be robust. (ii) Robust is also sometimes used to mean the architecture designed with a full complement of capabilities. Thus, in the context of IoT, the security protocols were designed for continuous operation with a very low failure rate.

2.3 Power-Efficient Techniques

One more major issue in security architecture development is power efficiency. In the literature, there are two significant works on power efficiency in security protocols. Urien et al. [49] proposed a protocol called LLCPS, i.e. the Logical Link Control protocol (LLCP) secured by TLS. LLCPS allowed an extensive choice of trusted ser-

vices for the IoT in Near-Field Communication (NFC), which allows proximity communications with retiring throughputs (hundreds of kbit/s) and low power consumption (a few mW). The proposed LLCPS protocol was efficiently used for payment, transport, access control, or file transfer applications.

Altolini et al. [3] proposed the implementation and performance evaluation of security functionalities at the link layer of IEEE 802.15.4-compliant IoT devices. Particularly, the encryption and authentication mechanisms were completely implemented in software and used the hardware ciphers offered by the IoT platform. Furthermore, they explained all the characteristics of the implementation and, at last, they provided the experimental results to measure the performance of the consequent encryption and authentication scheme for certain implementation approaches. Furthermore, they provided the quantitative results on energy consumption, memory footprint, and the execution time of particular implementation approaches, and examined several significant trade-offs.

A power-efficient architecture has the critical advantage of less memory usage. This architecture has power-economic benefits, which have the advantages of heat and light, thus greatly saving money on electricity bills.

2.4 Time-Efficient Techniques

Computation time is a significant parameter for developing the security architectures for IoT. Some of the proficient security architectures for IoT security are reviewed here. Gu and Wu [13] introduced a mutual authentication protocol for RFID tags that complies with ISO 18000-6B standard. It was employed in the low-cost tags as it needs only around 1000 gates. By performing security and performance analysis, the protocol was accepted as an efficient one. Giuliano et al. [12] tackled the security issue for non-IP devices that are able to connect by a short range with a mediator gateway, which can be seen as a short-range extension of conventional access network, in order to efficiently capture the IoT traffic. Specifically, a security algorithm was presented for both uni- and bidirectional terminals, based on the capability of the terminals. The security algorithms depend on a local key renewal, and only the local clock time is considered to perform it. Performance was analyzed by considering the maximum number of terminals that can be managed by one mediator gateway and the maximum packet delay as a function of the number of terminals in the area.

Moosavi et al. [31] proposed the security architecture. In this architecture, distributed smart e-health gateways perform the authentication and authorization of a remote end user, so that the medical sensors are relieved from doing these tasks. The architecture is based on the certificate-based DTLS handshake protocol, as it was the foremost IP security solution for IoT. A prototype IoT-based health-care system is developed for testing the authentication and authorization architecture. The prototype was made up of a Pandaboard, a TI SmartRF06 board, and WiSMotes. The CC2538 module incorporated into the TI board works as a smart gateway, and WiSMotes works as medical sensor nodes. The architecture was very secured than a centralized delegation-based architecture, as a highly secure key management method is used between sensor nodes and the smart gateway.

Han et al. [14] proposed a simulator, called DPWSim, in order to aid the use of IoT. DPWSim featuring secure messaging, dynamic discovery, service description, service invocation, and publish-subscribe eventing can be utilized to prototype, develop, and test products in terms of DPWS communication protocols. It can also maintain the relationship between the designers, developers, and manufacturers in developing a product. Borgohain et al. [5] examined several authentication systems employed for improved security and private relocation of an individual's login identifications. The first part described the multifactor authentication (MFA) systems, which may not be suitable to IoT but offers good security to a user's identifications. Following MFA, a short explanation about the working principle of communication between the third-party clients and private resources on the OAuth protocol framework, and an examination about the delegation-based authentication system in IP-based IoT, is presented.

Farash et al. [9] presented the enhanced security architecture of user authentication and key agreement scheme (UAKAS). This design facilitated the similar function with enhanced security level and allowed the

heterogeneous wireless sensor networks to grow dynamically without manipulating any party involved in UAKAS. The results of security analysis by BAN-logic and AVISPA tools proved the security properties of the scheme. de Fuentes et al. [7] dealt with the problem by providing the concept of Probabilistic Yoking Proofs and establishing three main measures to calculate their security, cost, and fairness. The message structure found in classical grouping proof constructions is combined with an iterative Poisson sampling process by the proposed solution. Here, the probability of each object being sampled changes with respect to time. A number of mechanisms were introduced by them to apply fluctuations to each object's sampling probability, and they proposed several sampling strategies.

Savola and Abie [40] investigated the security objective decomposition methods for an IoT e-health application. These methods lead to the growth of significant security parameters that are relevant to the security, contextual, and threat changes, and they are important for patient-centric IoT solutions utilized in various environments. To utilize these benefits, a context-aware Markov game theoretic model was formulated for security metrics and the risk impact assessment, to noticeably assess and authenticate the run-time adaptivity of IoT security solutions. Mahalle et al. [29] developed the Identity Authentication and Capability based Access Control (IACAC) model with protocol valuation and performance evaluation. The concept of capability for access control was initialized to safeguard IoT from various attacks like man-in-the-middle, replay, and denial-of-service (DoS) attacks. This technique presented a hybrid approach of authentication and access control for IoT devices. The outcomes of other associated studies were been examined to verify the results. Finally, the protocol was assessed by using a security protocol verification tool, and the verification outcomes revealed that IACAC was secure against the above-mentioned attacks.

Hu et al. [18] proposed a mutual identity authentication and key update scheme that is employed in the IoT with multihop relay devices in the middle link. In the IOT paradigm, terminal nodes have inadequate computation capabilities, and the obtained information is sent to the layer using relay devices. Thus, by using the relay devices, the technique inflicts less computation and communication requirements on terminal nodes, increases the computational overhead, and also authenticates the relay devices in some way and recessively, thereby securing the terminal nodes and relay devices from being compromised. Lai et al. [24] presented a conditional privacy-preserving authentication with access linkability (CPAL) for roaming service, which provides universal secure roaming service and multilevel privacy preservation. CPAL presented a nameless user linking function by using a group signature technique, which does not only effectively conceal user identities but also facilitates the authorized entities to connect all the available data of the identical user without obtaining the user's real identity.

The time-efficient architecture requires less computation time to perform the authentication process, which reduces the power and energy significantly.

2.5 Energy-Efficient Security Techniques

The security architectures of IoT related to energy-efficient techniques are reviewed in this section. He and Zeadally [15] explained about the required security measures of RFID authentication schemes, and provided ECC-based RFID authentication schemes in terms of performance and security. Even though many of them do not fulfill all the security needs and have acceptable performance, they established that the ECC-based authentication methods are relevant for the health-care environment in terms of their performance and security.

Vucinic et al. [51] presented OSCAR as an architecture for end-to-end security in IoT. It was dependent on the concept of object security that connects security with the application payload. The architecture integrated authorization servers that offer clients with access secrets that allow them to demand resources from constrained CoAP (Constrained Application Protocol) nodes. The nodes reply with the requested resources that were signed and encrypted. The scheme inherently supported multicast, asynchronous traffic, and caching.

Zhao [56] utilized the custom data packet encapsulation mechanism to reduce the cost of data resources. Depending on the cross-platform communication descriptions, joined with secure encryption and decryption,

signature, and authentication algorithm, a secure communication system of things model for the differentiation of things communication environment, which provides a standard packet structure, called smart business security IOT application ISSAP (Protocol Intelligent Service Security Application Protocol), was established. Kozlov et al. [23] explained the overall architecture for IoT and discussed about the well-known and new threats to security, privacy, and trust at various architecture levels, with attacker-centric and system approaches.

Shafagh et al. [41] proposed a system for safely storing IoT data in the cloud database. At the same time, query processing on the encrypted data is allowed. In order to achieve this, they encrypted the IoT data with a set of cryptographic methods. To enable this on resource-limited devices, their system depends on optimized algorithms that speed up the partial homomorphic and order-preserving encryptions by 1–2 orders of magnitude. Peretti et al. [35] presented a scheme called BlinkToSCoAP, achieved by the combination of three software libraries implementing energy-efficient versions of the DTLS, CoAP, and 6LoWPAN protocols over TinyOS. Moreover, a complete experimentation was presented that examines the performance of DTLS security blocks. The experiments examined BlinkToSCoAP messages exchanged between two Zolertia Z1 devices, which allowed evaluations in terms of energy consumption, memory footprint, latency, and packet overhead.

A two-way authentication security scheme for the IoT was implemented by Kothmay et al. [22]. It depends on the previous Internet standards, particularly the DTLS protocol. This security scheme is dependent on the commonly used public key cryptography (RSA), and functions over standard low-power communication stacks. They thought that by depending on a well-known standard, the engineering techniques, existing implementations, and security infrastructure can be used again, which facilitated a simple security uptake. They provided an implemented system architecture for the security system depending on a low-power hardware platform that is appropriate for IoT.

The main benefits of an energy-efficient security architecture are that (i) it has less energy consumption and (ii) it is more performance oriented.

2.6 Reliable Security Techniques

Nowadays, reliable and flexible security mechanism becomes a major concern. Some of the latest approaches for IoT presented in the literature are discussed here. Lake et al. [25] explained about use case scenarios and a secure architecture framework. Gessner et al. [11] presented trust-enhancing security functional components for the resolution infrastructure as a fundamental part of IoT. A preliminary requirement analysis and a critical control points assessment lead to the trust-enhancing security functional components to cover the basic IoT resource access control (AuthZ and AuthN), and the necessary functions including key exchange and management, identity management, and trust and reputation management. This composition of components with their interdependencies offers secure communication among subjects to assure an unbreakable communication, and hence includes devoted features of data integrity and confidentiality, service trust, and privacy of users. Keoh et al. [20] presented a clear evaluation of solutions for secure communication in IoT, particularly the standard security protocols to be employed in combination with the CoAP, which is an application protocol particularly personalized for the requirements of adjusting the constrictions of IoT devices. As the DTLS has been selected as the channel security under CoAP, they also considered the new standardization efforts to improve the DTLS for IoT applications. This incorporates the use of (i) a raw public key in DTLS; (ii) enlarging the DTLS record layer to guard multicast communication; and (iii) profiling DTLS for minimizing the size and complication of implementations on embedded devices.

Xu et al. [53] introduced an architecture called TAEC (Trustworthy Agent Execution Chip), to use the high-security, cost-effective software and hardware platform for the safe operation of agents. This technique is for fixing TAEC on every sensor node, to provide autonomic trusted hardware execution environment for agents. Pohls et al. [36] formulated a framework to ensure a configurable balance between reliability and privacy by considering security and privacy mechanisms in their early design stage. The RERUM scheme comprises architecture built on new network protocols and interfaces, and the design of smart

objects hardware. To emphasize the challenges and evaluating the scheme, RERUM used various Smart City applications that were installed and evaluated in the real-world test beds in the two Smart Cities that participated in the project.

A reliable architecture does not silently continue and deliver results that include uncorrected corrupted data. Instead, it detects and, if possible, corrects the corruption, for example by retrying an operation for transient (soft) or intermittent errors, or else, for uncorrectable errors, isolating the fault and reporting it to a higher-level recovery mechanism.

2.7 Smart-Level Security Techniques

Techniques that do not fall under the categories discussed above are reviewed in this section. Urien et al. [50] proposed a model for secure NFC services depending on the peer-to-peer (P2P) mode. NFC was a convenient communication technology, aided by smartphones or a consumer device that looks like a capable technology for the IoT. It was widely employed in several applications, for instance, transport, payment, access control, and most commonly for small information exchanges. LLCP manages the NFC P2P sessions. LLCPS was introduced as a TLS security layer working over LLCP. It imposes data privacy and integrity, and also provides identity to smart objects.

Maarten et al. [28] explained about a usage control toolkit for handling the above problems. The usage control toolkit describes the rules in managing the access to data and resources in IoT, i.e. the policies can be defined for different contexts such as work, personal life etc., and for different roles. Shah et al. [42] proposed a scheme to improve the available access control systems. This method of improving the access control system makes sure that the system is wireless, thus reducing the wiring problems. The explained prototype has the function of taking inputs from a smart card reader or a biometric sensor. These inputs were executed inside the controller (TM4C123GXL-based on ARM Cortex-M4).

Sivaraman et al. [47] focused on some of the smart-home appliances existing in the market, and considered their operation to expose various security and privacy issues. Implementing and practicing security in different devices vary based on several factors, such as device capabilities, mode of operation, and the manufacturer. This leads to the development of a design that employs additional security measures in the network. They used software-defined networking to implement dynamic security rules that can change depending on the situation, such as time-of-day or occupancy of the house. Park and Bang [34] employed the Jeju-VTS middleware to support information exchange on sea traffic. They framed a system that enables Inter-VTS Data Exchange Format (IVEF) service simulation in an IoT environment. To do this, they used an Android mobile phone and a personal computer for the emulation of a ship on cruise and VTS center. Alqassem and Svetinovic [2] presented security-relevant policies to reduce the identified forms of security attacks and to decrease the susceptibilities in the upcoming growth of the IoT systems. At last, it was employed on an IoT smart grid scenario.

Riahi et al. [38] investigated a technique for designing security mechanisms and its usage for IoT. They stated that the general method to security problems does not remove all the characteristics linked to this novel concept of communication, sharing, and actuation. Actually, the IoT concept includes new features, mechanisms, and risks that cannot be entirely considered through the classical formulation of security problems. Torjusen et al. [48] incorporated runtime verification enablers in the feedback adaptation loop of the ASSET adaptive security framework in order to achieve self-adaptive security and privacy properties in the e-health settings. The enablers make machine-processable formal models of the system state and context presented at run time, make requirements to describe the purposes of authentication, and enable dynamic environment supervision and adaptation.

The benefits of the IoT enable humans to control, effectively and easily, things that are up close or remotely. For example, the user can manage his car engine and control it from his computer. However, the best case is when different “things” communicate with each other using the Internet Protocol. For example, a refrigerator can communicate with a shopping center and buy supplies without human intervention.

3 Analysis and Discussion

This section presents the detailed analysis of the reviewed literature. The security techniques are analyzed based on the considered attacks, application, utilized simulation tool, security model, and attributes. Every work utilized different attributes and the simulation tool for proving the secure communication.

Analysis based on attributes: Table 1 shows the security attributes considered in different works. Important security attributes, such as trust, privacy, feedback, certificate, and reputation, were taken into consideration for developing more secure algorithms. Accordingly, trust was mainly considered in Refs. [2, 11, 28, 29, 36, 53] and privacy was utilized in Ref. [24]. The feedback was included in Ref. [16] and a certificate was included for authentication in Refs. [23, 38]. Furthermore, trust and privacy were effectively integrated to achieve better security in Ref. [48]. Trust and reputation were effectively integrated in Refs. [22, 33] to ensure better security. Table 1 proves that these attributes are essential for the new security protocol to be developed in IoT.

Analysis based on security model: Figure 2 shows the bar graph of the number of papers that utilized different security mechanisms. Commonly, security mechanisms such as communication, authorization, authentication, access control, service discovery, and verification were included in the security models to obtain better features. The security features were included in communication phase [56] and authorization [20, 51]. The works in Refs. [5, 16, 31] considered both authentication and authorization in the security protocol. The works in Refs. [29, 50] considered both authentication and access control for the security model. Access control [12, 42], service discovery [14], and verification [48] are also included as effective security concerns in the security models. More important, the approach in Ref. [2] considered three security mechanisms, including access control, authentication, and authorization [2]. From Figure 2, it can be understood that the security model that will consider all these mechanisms will be the effective security protocol for IoT.

Table 1: Analysis Based on Attributes.

Attributes	Works
Trust	[2, 11, 28, 29, 36, 53]
Privacy	[24]
Feedback	[16]
Certificate	[23, 38]
Trust and privacy	[48]
Trust and reputation	[22, 33]

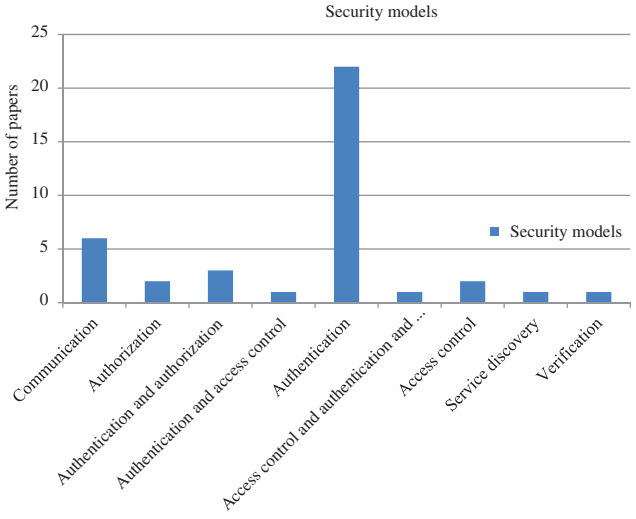

Figure 2: Bar Chart Based on the Security Model.

Analysis based on simulation tool: Table 2 shows the simulation tool utilized for implementation of IoT and the platforms. Mainly, four different categories of implementation are suggested, such as IEEE standard, simulator, embedded kit, and cloud platforms. IEEE 802.15.4 was utilized for implementation in the approaches in Refs. [3, 16, 20, 31, 35, 37], and IEEE 802.11b was used in Ref. [24]. Different simulators such as OPENSSL [50], DPWSim [14], Cooja emulator [8], AVISPA tools [17], SecKit [49], Color Petri Net [13], IVEF software development kit [34], and OpenMotes [41] were used for implementing the IoT security model. Also, some embedded kits such as NetDuino Plus 2 boards [19], Atmel AT97SC3203S TPM [22], and TM4C123GXL [42] were also suggested for the implementation. Amazon cloud was used for simulation in Ref. [47].

Analysis based on application: Even though IoT comprises devices, applications, networks, and smart devices, some of the works mainly focused on particular applications to develop a security model (Table 3). Accordingly, RFID was mainly considered in Refs. [2, 7, 8, 13, 42], and physical devices in Refs. [20, 31]. Healthcare application [24, 31, 40, 48] was mostly considered in the literature, and the works in Refs. [23, 26, 36, 47] made use of smart-level applications to show the security proof.

Analysis based on attacks: The performance of the security models is proved by testing with different security attacks. The literature of IoT considers replay, spoofing, DoS, cybil, man-in-the-middle, resource enervation, flood, password, and key attacks. The replay attack was used as security proof in Refs. [12, 16, 34, 43, 51]. The spoofing attack was used in Ref. [8], and DoS was applied in Refs. [24, 31, 56]. Similarly, cybil [19], man-in-the-middle [9, 14, 32, 34], resource enervation [29], flood [29], password [9], and key [21] attacks were also applied to maintain the security of the IoT model. Figure 3 shows the pie chart based on attacks

Table 2: Analysis Based on Simulation.

Categories	Platforms
IEEE standards	IEEE 802.15.4 [3, 35, 16, 20, 31, 37], IEEE 802.11b [24]
Simulators	OPENSSL [50], DPWSim [14], Cooja emulator [51], AVISPA tools [9], SecKit [28], Color Petri Net [48], IVEF software development kit [34], OpenMotes [41]
Embedded kits	NetDuino Plus 2 boards [19], Atmel AT97SC3203S TPM [22], TM4C123GXL [42]
Cloud platforms	Amazon cloud [47]

Table 3: Analysis Based on Application.

Categories	Platforms
Tags based	RFID [2, 7, 8, 13, 42]
Network based	Multi-hop relay networks [18], wireless sensor network [9], mobile network [43]
Devices based	Physical devices [20, 31]
Application based	Health care [24, 31, 40, 48]
Smart home based	Smart level [23, 26, 36, 47]

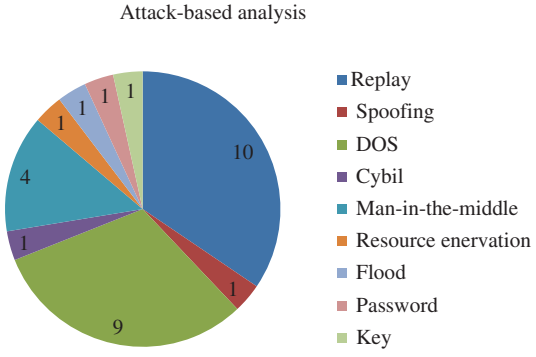

Figure 3: Pie Chart Based on Attacks.

utilized by different techniques of IoT. Accordingly, replay and DoS attacks are mostly used for security proof in IoT.

Even though real-time scenario includes different attack models, some works effectively handled these attack models by using a variety of concepts or ideas. For example, a password-guessing attack can be effectively handled by utilizing two passwords for the authentication phase. The impersonation attack can be handled by providing multiple validations for verifying identity. The server-spoofing attack can be handled by developing mutual authentication protocols. The stolen-verifier attack can be easily avoidable by storing encrypted information. The reply attack can be handled by mostly transferring the hashed values through the channel. Even if the hashed values are caught by the adversary by placing devices, replying to the message is not possible. It would require desired knowledge to perform the same tasks as in a real IoT device. The man-in-the-middle attack cannot authenticate both the IoT device and the server separately through the presence of the trusted access control.

4 Gaps and Issues

The development of IoT is a step-by-step process. There are still many problems to be solved, such as low-power nodes and computing, low-cost and low-latency communication, identification and positioning technologies, self-organized distributed systems technology, and distributed intelligence [6]. In the IoT network, with the help of a proper authentication process and point-to-point encryption, illegal access to the sensor nodes to spread fake information can be prevented. The most common kind of attack is the DoS attack, which impacts the network by driving a lot of useless traffic toward it through a number of botnets fuelled by the system of interconnected devices. This attack can be avoided by developing a proper authorization procedure. After the authentication/authorization process, routing algorithms can be implemented to ensure the privacy of data exchange between the sensor nodes and the processing systems. Also, the safety control mechanisms monitor the system for any kind of intrusion and, finally, data integrity methods can be implemented to make sure that the data received on the other end is the same as the original one. On the other hand, privacy of the data can be guaranteed by symmetric and asymmetric encryption algorithms such as RSA, DSA, BLOWFISH, and DES, etc., which prevent unauthorized access to the sensor data while being collected or forwarded to the next layer.

As for hiding sensitive information, anonymity of the location and identity can be obtained using the K-Anonymity approach, which ensures the protection of information like the identity and location, etc., of the user. Moreover, to prevent other malicious activities from miscreant users, anti-DOS firewalls and up-to-date spywares and malwares can be introduced.

The method in Ref. [18] is vulnerable to various attacks, and sharing tokens can be lost or stolen easily. The technique in Ref. [22] may have a chance of compromising the server, which risks hacking of information; however, dynamic update can provide key protection against eavesdropping. The technique in Ref. [18] can overwhelm a server by flooding it with connection requests [32], and that in Ref. [15] is vulnerable to storage attacks because the authentication scheme requires the secret key y stored in it. Malpractice can occur from the server side itself, so mutual authentication is required in the technique in Ref. [51]. Even though the technique in Ref. [24] presents multilevel authentication, it affects the computational overhead. The technique in Ref. [9] failed to maintain the key by performing updates frequently.

The following key challenges still need to be considered in developing secure communication protocols:

- The security architecture should ensure the security protocol jointly for access control and authenticity to fundamentally support multicast, asynchronous traffic, and caching.
- The detection of a malicious operation that occurs in between two nodes should be effectively achieved, and the alteration of messages should be identified to overwhelm man-in-middle attacks.
- Verification of both the transmitter and receiver (client and server) is very essential because both nodes can be compromised.

- Update is required at every stage to guarantee security, and the keys stored in the platform and terminal nodes need to be monitored simultaneously.
- Dynamic maintenance involving detecting and removing unauthorized nodes from the network should be carried out to reduce attacks, delays, and overhead.
- Assessing the credibility of the entity based on previous communications with the nodes and reputations with other nodes is essential.
- Integrating mutual authentication with cryptographic mechanism takes a long time to detect the nature of nodes.

After analyzing the literature, future works can be focused on the direction of multilevel and mutual authentications based on attribute-based profile modeling, to bring more security for access control and authentication. Here, authentication may require for every transmission to overwhelm the various attacks. In order to provide authentication for every transmission, threat profile-based mutual authentication can be developed with various attributes related to IDS capabilities, antivirus capabilities, firewall capabilities, secured file storage capabilities, interoperability, secured job execution, and feedback entry. Also, information about the success or failure of the last transmission can also be stored in the threat profile. These profiles can be updated dynamically for every transmission of information. Based on these security attributes and the reputation factor, authentication can be done using mutual and multilevel authentication. Here, multilevel authentication can be performed based on the importance of the data request. Based on the level of data importance, the level of authentication can be determined. If the data has higher importance, more number of levels can be used for authentication.

5 Conclusion

This paper presented a general survey of all the security issues addressed in IoT. The aim of the study was to find the challenges and issues regarding security, and to review the different security architectures available in the literature. In order to accomplish these tasks, we have analyzed 50 research papers related to IoT security, and the techniques were categorized into seven categories: (i) lightweight-based security techniques, (ii) robust security techniques, (iii) power-efficient techniques, (iv) time-efficient techniques, (v) energy-efficient security techniques, (vi) reliable security techniques, and (vii) smart security techniques. Again, the security techniques were analyzed based on the considered attacks to prove the security, application, utilized simulation tool, security model, and attributes. Also, different strategies for handling all the different attacks were discussed. Based on the analysis, the findings can help researchers in developing new security architectures by addressing the critical challenges faced by the recent security architectures. The final conclusion is that multilevel and mutual authentication based on attribute-based profile modeling brings more security for access control and authentication in IoT.

Bibliography

[1] A. Al Shidhani and V. Leung, Fast and secure reauthentications for 3GPP subscribers during WiMAX-WLAN handovers, *IEEE Trans. Depend. Secure Comput.* **8** (2011), 699–713.
[2] I. Alqassem and D. Svetinovic, A taxonomy of security and privacy requirements for the Internet of Things (IoT), in: *Proceedings of IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, pp. 1244–1248, 2014.
[3] D. Altolini, V. Lakkundi, N. Bui, C. Tapparello and M. Rossi, Low power link layer security for IoT: implementation and performance analysis, in: *Proceedings 9th International on Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 919–925, 2013.
[4] L. Atzori, A. Iera and G. Morabito, The Internet of Things: a survey, *Comput. Netw.* **54** (2010), 2787–2805.
[5] T. Borgohain, A. Borgohain, U. Kumar and S. Sanyal, Authentication systems in Internet of Things, *Int. J. Adv. Netw. Appl.* **6** (2015), 2422–2426.

[6] S. Chen, H. Xu, D. Liu, B. Hu and H. Wang, A vision of IoT: applications, challenges, and opportunities with China perspective, *IEEE Internet Things J.* **1** (2014), 349–359.
[7] J. M. de Fuentes, P. Peris-Lopez, J. E. Tapiador and S. Pastrana, Probabilistic yoking proofs for large scale IoT systems, *Ad Hoc Netw.* **32** (2015), 43–52.
[8] K. Fan, C. Liang, H. Li and Y. Yang, LRMAPC: a lightweight RFID mutual authentication protocol with cache in the reader for IoT, in: *Proceedings of IEEE International Conference on Computer and Information Technology*, pp. 276–280, 2014.
[9] 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 Netw.* **36** (2016), 152–176.
[10] M. U. Farooq, M. Waseem, A. Khairi and S. Mazhar, A critical analysis on the security concerns of Internet of Things (IoT), *Int. J. Comput. Appl.* **111** (2015), 1–6.
[11] D. Gessner, A. Olivereau, A. Olivereau and A. Serbanati, Trustworthy infrastructure services for a secure and privacy-respecting Internet of Things, in: *Proceedings of IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 998–1003, 2012.
[12] R. Giuliano, F. Mazzenga, A. Neri and A. M. Vegni, Security access protocols in IoT networks with heterogenous non-IP terminals, in: *Proceedings of the IEEE International Conference on Distributed Computing in Sensor Systems*, pp. 257–262, 2014.
[13] Y. Gu and W. Wu, A light-weight mutual authentication protocol for ISO 18000-6b standard RFID system, in: *Proceedings of IEEE International Conference on Communications Technology and Applications*, pp. 21–25, 2009.
[14] S. N. Han, G. M. Lee, N. Crespi, N. V. Luong, K. Heo, M. Brut and P. Gatellier, DPWSim: a devices profile for web services (DPWS) simulator, *IEEE Internet Things J.* **2** (2015), 221–229.
[15] D. He and S. Zeadally, An analysis of RFID authentication schemes for Internet of Things in healthcare environment using elliptic curve cryptography, *IEEE Internet Things J.* **2** (2014), 72–83.
[16] J. L. Hernandez-Ramos, M. P. Pawlowskis, A. J. Jara, A. F. Skarmeta and L. Ladid, Towards a lightweight authentication and authorization framework for smart objects, *IEEE J. Select. Areas Commun.* **33** (2015), 690–702.
[17] F. Hou, C. Yang, J. Liu, Y. Zhang, J. Tian and Y. Zhang, HB-MAP protocol: a new secure bidirectional light-weight authentication protocol of HB, in: *Proceedings of IEEE Ninth International Conference on e-Business Engineering (ICEBE)*, pp. 151–155, 2012.
[18] T. Hu, J. Wang, G. Zhao and X. Long, An improved mutual authentication and key update scheme for multi-hop relay in Internet of Things, in: *Proceedings of 7th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, pp. 1024–1029, 2012.
[19] M. A. Jan, P. Nanda, X. He, Z. Tan and R. P. Liu, A robust authentication scheme for observing resources in the Internet of Things environment, in: *Proceedings of IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 205–211, 2014.
[20] S. L. Keoh, S. S. Kumar, and H. Tschofenig, Securing the Internet of Things: a standardization perspective, *IEEE Internet Things J.* **1** (2014), 265–275.
[21] H. J. Kim and K. Kim, Toward an inverse-free lightweight encryption scheme for IoT, in: *Proceedings of Conference on Information Security & Cryptography*, 2014.
[22] T. Kothmay, C. Schmitt, W. Hu, M. Brunig and G. Carle, A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication, in: *Proceedings of IEEE 37th Conference on Local Computer Networks Workshops (LCN Workshops)*, pp. 956–963, 2012.
[23] D. Kozlov, J. Veijalainen and Y. Ali, Security and privacy threats in IoT architectures, in: *Proceedings of the 7th International Conference on Body Area Networks*, pp. 256–262, 2012.
[24] C. Lai, H. Li, X. Liang, R. Lu, K. Zhang and X. Shen, CPAL: a conditional privacy-preserving authentication with access linkability for roaming service, *IEEE Internet Things J.* **1** (2014), 46–57.
[25] D. Lake, R. Milito, M. Morrow and R. Vargheese, Internet of Things: architectural framework for eHealth security, *J. ICT Stand.* **1** (2014), 301–328.
[26] M. Leo, F. Battisti, M. Carli and A. Neri, A federated architecture approach for Internet of Things security, in: *Proceedings of Euro Med Telco Conference (EMTC)*, pp. 1–5, 2014.
[27] X. Li, R. Lu, X. Liang, X. Shen, J. Chen and X. Lin, Smart community: an Internet of Things application, *IEEE Commun. Mag.* **49** (2011), 68–75.
[28] B. Maarten, N. Ricardo, B. Gianmarco. N. Igor, S. Gary and T. Elias, *Dynamic Context-Aware Scalable and Trust-based IoT Security, Privacy Framework*, River Publisher, Denmark, 2014.
[29] P. N. Mahalle, B. Anggorojati, N. R. Prasad and R. Prasad, Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things, *J. Cyber Secur. Mobil.* **1** (2013), 309–348.
[30] D. Miorandi, S. Sicari, F. DePellegrini and I. Chlamtac, Internet of Things: vision, applications and research challenges, *Ad Hoc Netw.* **10** (2012), 1497–1516.
[31] S. R. Moosavi, T. N. Gia, A. M. Rahmani, E. Nigussie and S. Virtanen, SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways, *Proc. Comput. Sci.* **52** (2015), 452–459.
[32] H. Ning, H. Liu and L. T. Yang, Aggregated-proof based hierarchical authentication scheme for the Internet of Things, *IEEE Trans. Parallel Distrib. Syst.* **26** (2015), 657–667.

[33] M. Panwar and A. Kumar, Security for IoT: an effective DTLS with public certificates, in: *Proceedings International Conference on Advances in Computer Engineering and Applications (ICACEA)*, pp. 163–166, 2015.
[34] N. Park and H. C. Bang, Mobile middleware platform for secure vessel traffic system in IoT service environment, *Secur. Commun. Netw.* **9** (2014), 500–512.
[35] G. Peretti, V. Lakkundi and M. Zorzi, BlinkToSCoAP: an end-to-end security framework for the Internet of Things, in: *Proceedings of 2015 7th International Conference on Communication Systems and Networks (COMSNETS)*, pp. 1–6, 2015.
[36] H. C. Pohls, V. Angelakis, S. Suppan, K. Fischer, G. Oikonomous, E. Z. Tragos, R. D. Rodriguez and T. Mouroutis, RERUM: building a reliable iot upon privacy- and security- enabled smart objects, in: *Proceedings of Wireless Communications and Networking Conference Workshops (WCNCW)*, pp. 122–127, 2014.
[37] S. Raza, T. Voigt and V. Jutvik, Lightweight IKEv2: a key management solution for both the compressed IPsec and the IEEE 802.15.4 security, in: *Proceedings of the IETF Workshop on Smart Object Security*, 2012.
[38] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou and A. Bouabdallah, A systemic approach for IoT security, in: *Proceedings of IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 351–355, 2013.
[39] A. Rizzardi, D. Miorandi, S. Sicari, C. Cappiello and A. Coen-Porisini, Networked smart objects: moving data processing closer to the source, in: *2nd EAI International Conference on IoT as a Service*, October 2015.
[40] R. M. Savola and H. Abie, Metrics-driven security objective decomposition for an EHealth application with adaptive security management, in: *Proceedings of the International Workshop on Adaptive Security*, 2012.
[41] H. Shafagh, A. Hithnawi, A. Dröscher, S. Duquennoy and W. Hu, Poster: towards encrypted query processing for the Internet of Things, in: *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, pp. 251–253, 2015.
[42] C. M. Shah, V. B. Sangoi and R. M. Visharia, Smart security solutions based on Internet of Things (IoT), *Int. J. Curr. Eng. Technol.* **4** (2014), 3401–3404.
[43] M. Shi, X. Shen and J. W. Mark, A light weight authentication scheme for mobile wireless Internet applications, in: *Proceedings of IEEE WCNC*, pp. 2126–2131, New Orleans, LA, March 16–20, 2003.
[44] S. Sicari, A. Rizzardi, L. A. Grieco and A. Coen-Porisini, Security, privacy and trust in Internet of Things: the road ahead, *Comput. Netw.* **76** (2015), 146–164.
[45] S. Sicari, A. Rizzardi, L. A. Grieco, T. Monteil and A. Coen-Porisini, Secure OM2M service platform, in: *12th IEEE International Conference on Autonomic Computing, Self-IoT 2015*, 7–10 July 2015.
[46] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello and A. Coen-Porisini, A secure and quality-aware prototypical architecture for the Internet of Things, *Inf. Syst.* **58** (2016), 43–55.
[47] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli and O. Mehani, Network-level security and privacy control for smart-home IoT devices, in: *Proceedings of Eight International Workshop on Selected Topics in Mobile and Wireless Computing*, pp. 163–167, 2015.
[48] A. B. Torjusen, D. Trcek, H. Abie and Å. Skomedal, Towards run-time verification of adaptive security for IoT in eHealth, in: *Proceedings of the European Conference on Software Architecture Workshops*, 2014.
[49] P. Urien, LLCPS: a new security framework based on TLS for NFC P2P applications in the Internet of Things, in: *Proceedings of the 10th Annual IEEE Consumer Communications and Networking Conference*, pp. 845–846, 2013.
[50] P. Urien, LLCPS: a new secure model for Internet of Things services based on the NFC P2P model, in: *Proceedings of IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, pp. 1–6, 2014.
[51] M. Vucinic, B. Tourancheau, F. Rousseau, A. Duda, L. Damon and R. Guizzetti, OSCAR: object security architecture for the Internet of Things, in: *Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (IEEE WoWMoM 2014)*, 2014.
[52] X. Wang, X. Sun, H. Yang and S. A. Shah, An anonymity and authentication mechanism for Internet of Things, *J. Convergence Inform. Technol.* **6** (2011), 98–105.
[53] X. Xu, N. Bessis and J. Cao, An autonomic agent trust model for IoT systems, *Proc. Comput. Sci.* **21** (2013), 107–113.
[54] X. Yao, Z. Chen and Y. Tian, A lightweight attribute-based encryption scheme for the Internet of Things, *Future Gen. Comput. Syst.* **49** (2015), 104–112.
[55] G. Zhao, X. Si, J. Wang, X. Long and T. Hu, A novel mutual authentication scheme for Internet of Things, in: *Proceedings of Int. Conf. Model., Identification Control*, pp. 563–566, 2011.
[56] Y. Zhao, Research on data security technology in Internet of Things, *Appl. Mech. Mater.* **433–435** (2013), 1752–1755.
[57] L. Zhou and H. C. Chao, Multimedia traffic security architecture for the Internet of Things, *IEEE Netw.* **25** (2011), 35–40.