Elrawy *et al. Journal of Cloud Computing: Advances, Systems and Applications* (2018) 7:21
https://doi.org/10.1186/s13677-018-0123-6

Journal of Cloud Computing:
Advances, Systems and Applications

REVIEW Open Access

Intrusion detection systems for IoT-based smart environments: a survey

Mohamed Faisal Elrawy[1,2*], Ali Ismail Awad[3,4] and Hesham F. A. Hamed[5]

Abstract

One of the goals of smart environments is to improve the quality of human life in terms of comfort and efficiency. The Internet of Things (IoT) paradigm has recently evolved into a technology for building smart environments. Security and privacy are considered key issues in any real-world smart environment based on the IoT model. The security vulnerabilities in IoT-based systems create security threats that affect smart environment applications. Thus, there is a crucial need for intrusion detection systems (IDSs) designed for IoT environments to mitigate IoT-related security attacks that exploit some of these security vulnerabilities. Due to the limited computing and storage capabilities of IoT devices and the specific protocols used, conventional IDSs may not be an option for IoT environments. This article presents a comprehensive survey of the latest IDSs designed for the IoT model, with a focus on the corresponding methods, features, and mechanisms. This article also provides deep insight into the IoT architecture, emerging security vulnerabilities, and their relation to the layers of the IoT architecture. This work demonstrates that despite previous studies regarding the design and implementation of IDSs for the IoT paradigm, developing efficient, reliable and robust IDSs for IoT-based smart environments is still a crucial task. Key considerations for the development of such IDSs are introduced as a future outlook at the end of this survey.

Keywords: Intrusion detection systems, Internet of things, Smart environments

Introduction

Incredible developments in the routine use of electronic services and applications have led to massive advances in telecommunications networks and the emergence of the concept of the Internet of Things (IoT). The IoT is an emerging communications paradigm in which devices serve as objects or "things" that have the ability to sense their environment, connect with each other, and exchange data over the Internet [1, 2]. By 2022, one trillion IP addresses or objects will be connected to the Internet through IoT networks [3].

The IoT paradigm has recently been used in creating smart environments, such as smart cities and smart homes, with various application domains and related services. The goal of developing such smart environments is to make human life more productive and comfortable by solving challenges related to the living environment, energy consumption, and industrial needs [4]. This goal is directly reflected in the substantial growth in the available IoT-based services and applications across different networks. For example, the Padova Smart City in Italy is a successful example of a smart city based on an IoT system [5].

Smart environments consist of sensors that work together to execute operations. Wireless sensors, wireless communication techniques, and IPv6 assist in the expansion of smart environments. Such environments are wide ranging, from smart cities and smart homes to smart healthcare and smart services. The integration of IoT systems and smart environments makes smart objects more effective. However, IoT systems are susceptible to various security attacks, such as denial-of-service (DoS) attacks and distributed denial-of-service (DDoS) attacks. Such attacks can cause considerable damage to the IoT services and smart environment applications in an IoT network. Consequently, securing IoT systems has become a major concern [1]. For example, on Friday, October 21, 2016, a series of DDoS attacks were launched across the US that exploited the security vulnerabilities in IoT systems [6].

*Correspondence: m.f.elrawy@gmail.com
[1]Department of Electronics and Communication Engineering, MUST University, 6th of October, Egypt
[2]Institute of Public Administration, Abha, Asir, Saudi Arabia
Full list of author information is available at the end of the article

These attacks affected IoT devices, websites and online services such as Twitter, Netflix, and PayPal.

An intrusion detection system (IDS) is a security mechanism that works mainly in the network layer of an IoT system. An IDS deployed for an IoT system should be able to analyze packets of data and generate responses in real time, analyze data packets in different layers of the IoT network with different protocol stacks, and adapt to different technologies in the IoT environment [3]. An IDS that is designed for IoT-based smart environments should operate under stringent conditions of low processing capability, fast response, and high-volume data processing. Therefore, conventional IDSs may not be fully suitable for IoT environments. IoT security is a continuous and serious issue; thus, an up-to-date understanding of the security vulnerabilities of IoT systems and the development of corresponding mitigation approaches are required.

This article offers a comprehensive review of IDSs as a security solution for IoT-based smart environments. The primary goal of this study is to present the most recent designs and approaches for IDSs operating in IoT-based environments. Although related surveys have been published in the literature [3, 7], this article focuses on the important factors that affect IDS performance in smart environments, such as the detection accuracy, false positive rate, energy consumption, processing time, and performance overhead. In addition, this article introduces a solid foundation for the development of IDSs for IoT-based smart environments.

This study offers multiple key contributions. First, a full preliminary analysis of IoT systems, smart environments, and IDSs is presented. Second, the study confirms that traditional IDSs cannot satisfy IoT security requirements due to the large diversity of IoT networks and protocols. For instance, IPv6 over low-power wireless personal area networks (6LoWPAN) is not a protocol that is used in traditional telecommunications networks. Third, the common features that can be ported from traditional IDSs to IoT-based IDSs are emphasized. This third contribution emerges from the integration of the previous surveys [3, 7] to summarize the features, advantages and disadvantages of all IDSs designed for IoT-based systems. Fourth, this work introduces a future outlook on IDSs for IoT environments with a focus on the strengths and weaknesses of the current IDSs. Additionally, this study presents new recommendations for designing IDSs that satisfy the security requirements of IoT-based smart environments.

This survey focuses on IDSs for the IoT paradigm, independent of any specific technology or protocol; however, readers who are interested in learning more about IoT enabling technologies and protocols such as low-power wide-area network (LPWAN) technologies, long range (LoRa) technology, the low power WAN protocol for Internet of Things (LoRaWAN), the 6LoWPAN protocol, or the constrained application protocol (CoAP) may refer to [8–11] for further details.

The remainder of this paper is organized as follows. "The IoT paradigm" section discusses various definitions and architectures relevant to the IoT context. This section also highlights the importance of cloud computing systems for IoT-based smart environments and the challenges of applying this combination of systems in the real world. Definitions, goals and challenges related to smart environments, with a focus on smart cities, are discussed in "IoT and smart environments" section. "Security challenges in IoT-based smart environments" section reviews the security challenges in IoT-based smart environments in relation to the various layers of the IoT architecture and highlights some practical open challenges facing real-world IoT networks. "Intrusion detection systems (IDSs)" section provides preliminary information about the definitions relevant to IDSs, the different types of IDSs and the detection techniques used in these systems. A survey of IoT-oriented IDSs that either can be applied in or are specifically designed for smart environments is presented in "IDSs designed for IoT systems" section. "Discussion and future outlook" section discusses recommendations concerning IDSs implemented for IoT-based smart environments. Finally, conclusions and plans for future work are reported in "Concluding remarks" section. The organization of this paper is presented visually in Fig. 1.

The IoT paradigm

The IoT concept has been established since the founding of the Auto-ID Center at the Massachusetts Institute of Technology (MIT) in 1999. The Auto-ID Center created the electronic product code (EPC) number, which depends on radio frequency identification (RFID), in 2003. This idea is the crucial technology of the IoT [12].

However, the IoT is a well-established paradigm, and it is defined in several ways from various perspectives. Thiesse et al. [13] defined the IoT as consisting of hardware items and digital information flows based on RFID tags. The IoT definitions and architectures provided by various standards and industrial organizations will be described in the following.

The Institute of Electrical and Electronics Engineers (IEEE) defines the IoT as a collection of items with sensors that form a network connected to the Internet [12, 14]. The International Telecommunication Union (ITU) defines the IoT through three dimensions, as a network that is available anywhere, anytime, and by anything and anyone [15]. The European Telecommunications Standards Institute (ETSI), rather than using the expression "Internet of Things (IoT)", defines machine-to-machine (M2M) communications as an automated

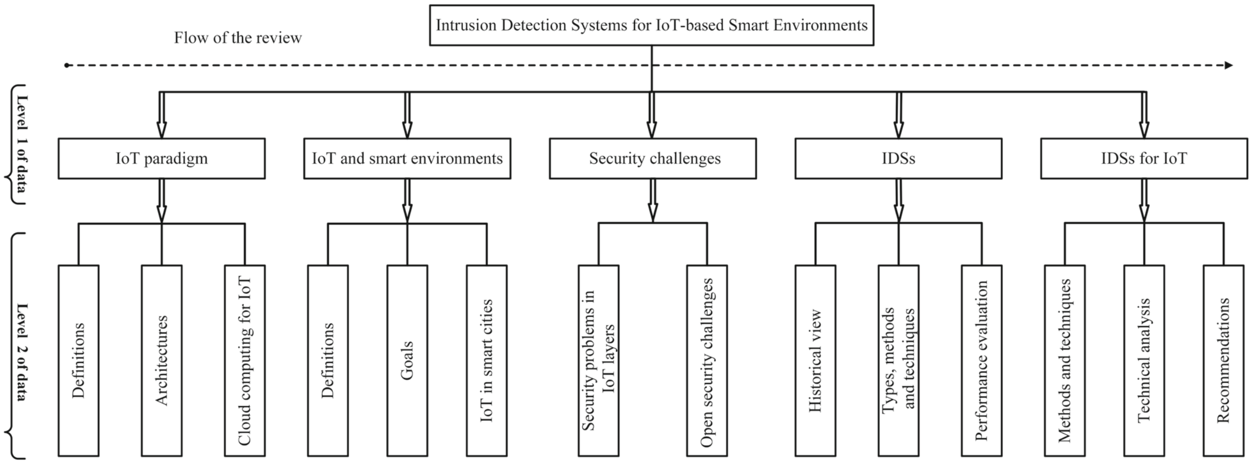

Fig. 1 The flow of this article, separated into two levels; level 1 describes the main topics, and level 2 describes the detailed points

communications system that makes decisions and processes data operations without direct human intervention [16].

The Coordination and Support Action for Global RFID-related Activities and Standardisation (CASAGRAS) project has created a new concept of the IoT that encompasses two viewpoints: the connection of physical objects with virtual objects over a global network without any human intervention to the greatest extent possible [17] and the incredible increase in IoT applications within traditional networks due to the extent of IoT marketing [17].

Moreover, Cisco, an industrial organization, works on IoT technology under the title of the Internet of Everything (IoE). Cisco has summarized the IoE concept as a network that consists of people, data, things, and processes. Thus, information and actions are created in and moved through this network [18].

IoT system architectures

Regarding IoT design, IEEE is working on a project (IEEE P2413) to determine the IoT architectural framework. The scope of this project is to describe the IoT domains and the various applications in these domains [19]. This IoT architecture is divided into three layers: the application layer, the networking and data communications layer, and the sensing layer.

According to [20–22], the general architecture of the IoT is divided into five layers that span three domains, namely, the application domain, the network domain, and the physical domain; thus, the IoT can be customized to fit the needs of different smart environments. The application domain encompasses management and utilization. The network domain is responsible for data transmission. The physical domain is responsible for information collection. The layers of the general IoT architecture are shown in Fig. 2. The functionality of the different layers is discussed in the following.

The perception layer is a hardware layer that consists of sensors and physical objects in different forms. These hardware elements provide identification, information storage, information collection, and information

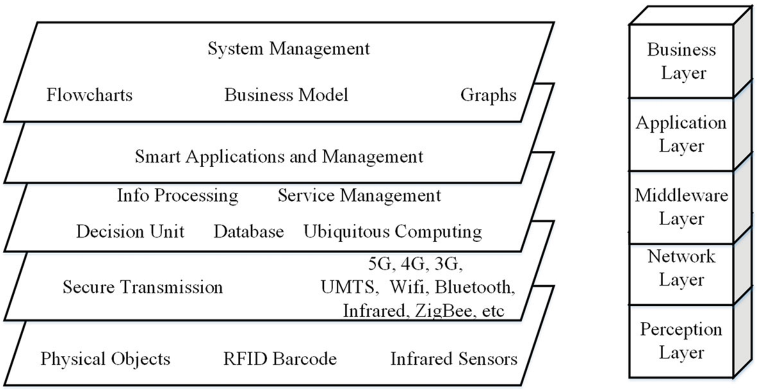

Fig. 2 The general architecture for the IoT. The general architecture for the IoT, which consists of five layers according to [22]

processing. The information output from this layer is sent to the next layer (the network layer) to be transmitted to the processing system [22].

The network layer is a transmission layer that transfers the information from physical objects or sensors to the processing system over secure lines using a communication system. This communication system can be either wired or wireless and can be based on different technologies, depending on the physical object or sensor components. The information output from this layer is sent to the next layer (the middleware layer) [22].

The middleware layer is responsible for service management over IoT devices to create connections between IoT devices that provide the same service. Moreover, the middleware layer stores the information coming from the network layer in a database to facilitate decision-making on the basis of information processing operations [22].

The application layer is responsible for the global management of IoT applications. The application layer depends on the information processed in the middleware layer. Moreover, the application layer depends on the specifics of the different implemented IoT applications, such as smart industry, building, city, and health applications [22].

The business layer is also responsible for the global management of IoT applications as well as service management over IoT devices. The business layer creates a business model that depends on the information processed in the application layer and on the analysis of the results of these information processing operations [22].

Cloud computing and the IoT

IoT systems connect an enormous number of devices and sensors exchanging an enormous amount of data and supporting a massive number of services. The management and analysis of these data pose certain special requirements, such as powerful processing, massive storage and high-speed networking capabilities [23].

Cloud computing offers high computational power, a massive storage capacity, and configurable resources with virtualization capabilities for manipulating the large amounts of data collected from IoT-based smart environments. With the integration of cloud computing systems and IoT-based smart environments, smart things can be easily accessed and managed at any time and place, and better services can be provided through the IoT model [23, 24].

According to [25], one of the important challenges in employing a cloud computing system for the IoT is the synchronization between different cloud vendors. A second challenge is achieving compatibility between general cloud service environments and IoT requirements. Security challenges are the main factor hindering the adoption of cloud computing by businesses and government organizations [26]. Thus, the ability to respect the necessary security constraints to fulfill the needs of the IoT in a cloud computing platform is a vital requirement. A robust and efficient security solution such as an IDS is one possible option. Moreover, standardization, enhancement, and management for the deployment of IoT systems and their connection to the cloud are additional challenges that should be taken into consideration.

IoT and smart environments

The objective of smart environments is to make human life more comfortable and more efficient by using sensors. IoT-based smart environments enable the effective realization of smart objects. By means of an IoT network, sensors can be monitored and controlled remotely. According to Navigant Research, the global smart city services market is expected to increase from 93.5 billion US dollars in 2017 to 225.5 billion US dollars by 2026 [27].

Ahmed et al. [28] state that "The term smart refers to the ability to autonomously obtain and apply knowledge, and the term environment refers to the surroundings". A smart city is one type of smart environment. The core element of a smart city is an integrated information center operated by the IoT service provider, which provides information on services such as electricity, water, and gas.

Smart health, smart industry, smart buildings and smart homes are other types of smart environments. The objective of such smart environments is to provide services via smart methods based on the information collected by IoT-enabled sensors. The architecture of such IoT-based smart environments is shown in Fig. 3.

Smart environments based on the IoT paradigm have certain special characteristics, and hence, special needs arise in the deployment of such environments. For instance, remote monitoring and remote control capabilities are required to allow smart objects to collect and process data and to execute operations remotely. Moreover, the ability to make decisions is an important characteristic in such a system. A smart object should be able to make intelligent decisions without human intervention by using data mining and other techniques for extracting useful data.

By virtue of these characteristics, smart environments offer certain features that can be used to enhance the quality of service (QoS) of user applications. Real-time information is one of these features. Smart objects can collect and analyze data and make intelligent decisions in real time. Moreover, the cost-effectiveness of cloud applications can be used to increase the QoS of smart environment applications. The integration of smart and IoT environments offers new opportunities with respect to the QoS of services and applications.

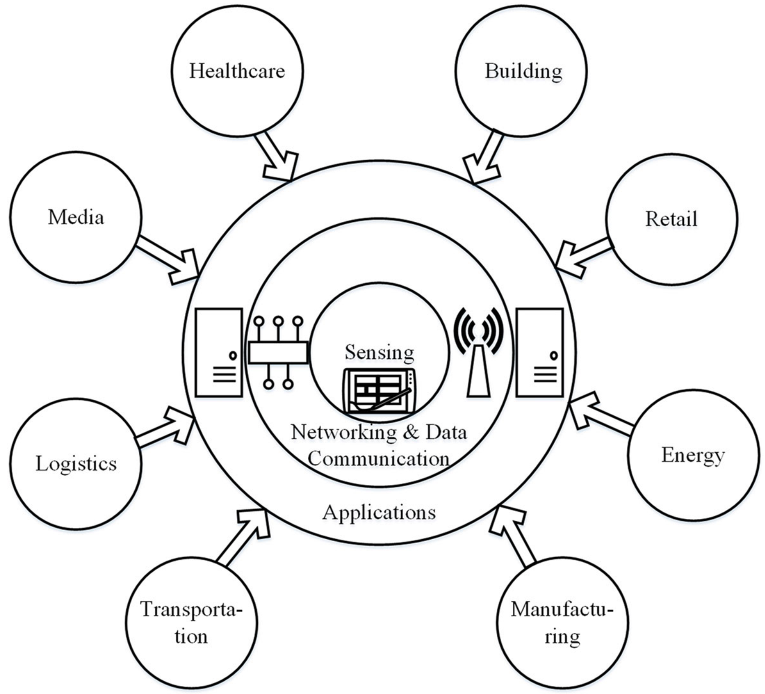

Fig. 3 IoT-based smart environments. The architecture of the IoT and the extent of the IoT market according to [14]

IoT technology for developing smart cities

Many national governments are working on the information and communication technology (ICT) infrastructure to solve the problems arising in traditional public management affairs. One of the most modern and effective solutions is to establish a smart city [5]. The smart city concept is one facet of the idea of smart environments.

There are many benefits of converting traditional public services and resources into a form that takes advantage of the smart city concept, including increasing the quality of public services and reducing the operating costs of public administration [29]. However, the management and execution of public services in a smart city require a powerful network, such as an IoT network.

Additionally, there are many barriers to the establishment of an IoT-based smart city. The novelty, complexity and technical challenges of IoT systems present the greatest difficulty. Furthermore, in the absence of widely accepted definitions for smart city operations, political and financial barriers prevent the smart city concept from being effectively applied.

The Padova Smart City in Italy is a successful example of a smart city that has overcome these barriers. The main goal of establishing the Padova Smart City is to develop ICT solutions for public administration systems using different types of data and technology [5].

The implementation of the IoT paradigm for creating smart environments, particularly smart cities, faces several technical challenges. Among these, precision, latency and available bandwidth have important effects in many smart environments, such as industrial and healthcare environments. Because of the need to support an increasing number of users and smart objects in IoT networks and the corresponding generation of increasingly large amounts of data, scalable computing platforms, such as cloud computing, are necessary. Such platforms can improve the performance of data management services in IoT systems and the QoS of smart environment applications [30].

Security challenges in IoT-based smart environments

The security of IoT systems is a serious issue due to the increasing numbers of services and users in IoT networks. The integration of IoT systems and smart environments makes smart objects more effective. However, the impacts of IoT security vulnerabilities are very dangerous in critical smart environments used in fields such as medicine and industry. In IoT-based smart environments without robust security systems, applications and services will be at risk. Confidentiality, integrity, and availability are three important security concepts of applications and services in IoT-based smart environments; thus, to address these concerns, information security in IoT systems requires greater research focus [2]. For example, IoT-based smart homes face security and privacy challenges that span all layers of the IoT architecture [31].

The creation of smart environments in the real world faces two notable barriers: the security of IoT systems and the complexity and compatibility of IoT environments. Attacks such as DoS or DDoS attacks on IoT networks affect IoT services and thus affect the services provided by smart environments.

Researchers study the security challenges of the IoT from many different points of view, one of which is the security vulnerability of IoT communication protocols [32]. This survey focuses on IDSs for the IoT paradigm, independent of any specific protocol; thus, this study focuses on the security challenges facing IoT systems on the basis of the IEEE definition and the general IoT architecture.

The security challenges in IoT systems are related to security issues arising in the different IoT layers. Physical damage, hardware failure, and power limitations are challenges faced in the physical layer. DoS attacks, sniffing, gateway attacks, and unauthorized access are challenges relevant to the network layer. Malicious code attacks, application vulnerabilities, and software bugs are challenges faced in the application layer [33].

According to [34], the security-related problems of any IoT system can be categorized into four types: authentication and physical threats, confidentiality risks, data integrity issues and privacy problems. The relations between these groups are shown in Fig. 4. The security problems arising in the different IoT layers are concisely discussed below.

- The authentication-related problem and physical threats are the first challenges that affect an IoT system. The perception layer includes many IoT devices, such as sensors, that depend on their own security systems; thus, they are susceptible to physical attacks.
- Confidentiality-related risks arise between IoT devices and the gateways in the network layer. The resource-constrained nature of the low-level devices in IoT systems poses an indirect challenge with regard to the confidentiality of data transmission in IoT networks [35].
- The third class of security challenges concerns the data integrity between services and applications. Data integrity problems emerge when spoofing attacks or noise affect an IoT system. DoS, DDoS, and probe attacks are arbitrary attacks that can harm IoT applications and services.
- The challenges of the fourth type are related to privacy. Information privacy is an important aspect of security in IoT systems [36]. Different IoT components use different types of object identification technologies; thus, every object has its own identification tag, which carries personal, location and movement information. Managing and monitoring the applications and services in an IoT system mean placing information privacy at risk; for example, using a system based on a deep packet inspection technique for trusted operations within an IoT system is considered to be a violation of information privacy [37]. Any intrusive accesses to the management system without permission threaten the information privacy of the IoT users [34].

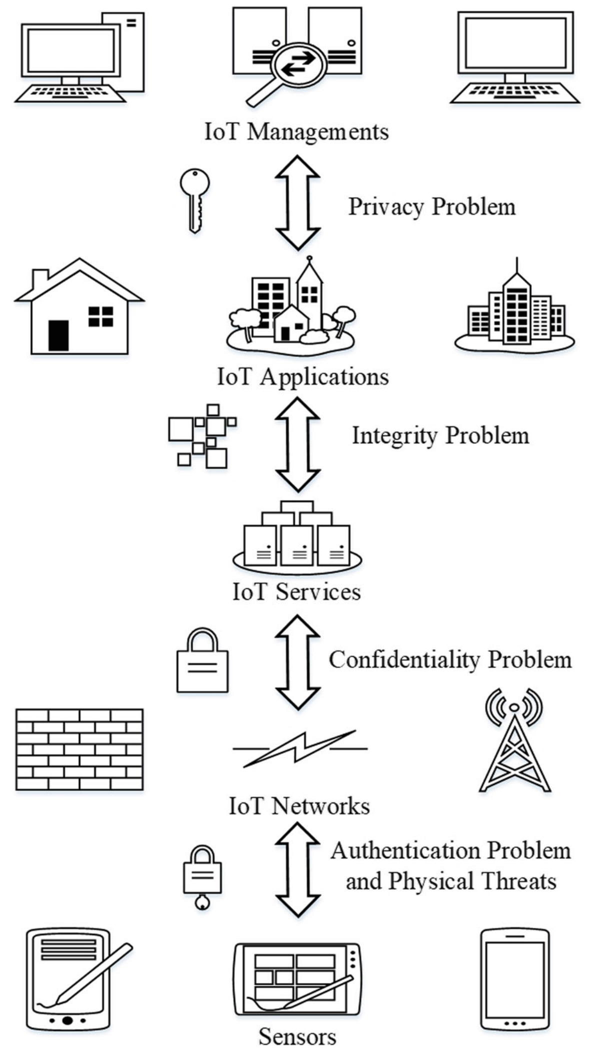

Fig. 4 The security challenges in the different IoT layers. The four types of security problems arising in the IoT model are associated with the different layers of the IoT architecture

Real-world applications of IoT systems face many open challenges. The open security challenges affecting IDS operations identified by [20, 22, 33, 38] are discussed below.

- A smart environment that integrates IoT technology is considered to be a complex system because it consists of different products from different companies based on different technologies that do not share a universal language. Therefore, standardization is another important aspect of security in IoT systems. Creating a standard IoT architecture based on one standard technology for all vendors and manufacturers would enhance the interoperability of the security functionalities of all objects and sensors in an IoT system. The success of this integration will depend on collaboration among companies to create a universal standard. Such standardization will greatly facilitate IoT network security.
- A single successful penetration of one or more end devices can threaten the security of an entire IoT system and cause harm to its applications and services, especially from an industrial point of view [39]. Thus, the implementation of a strong security mechanism in an IoT system depends on the strength of the security for individual IoT devices, which in turn depends on power and memory factors. Consequently, power and memory limitations are considered to pose indirect security challenges in IoT systems. To address these challenges, lightweight security solutions and lightweight encryption and decryption methods are required. These solutions and methods must be applicable in different IoT domains and must satisfy the security requirements without affecting the QoS.

Intrusion detection systems (IDSs)

IDSs: a historical overview

Monitoring and analyzing user information, networks, and services through passive traffic collection and analysis are useful tools for managing networks and discovering security vulnerabilities in a timely manner [40, 41]. An IDS is a tool for monitoring traffic data to identify and protect against intrusions that threaten the confidentiality, integrity, and availability of an information system [42]. The operations of an IDS are schematically illustrated in Fig. 5.

The operations of an IDS can be divided into three stages. The first stage is the monitoring stage, which relies on network-based or host-based sensors. The second stage is the analysis stage, which relies on feature extraction methods or pattern identification methods. The final stage is the detection stage, which relies on anomaly or misuse intrusion detection. An IDS captures a copy of the data traffic in an information system and then analyzes this copy to detect potentially harmful activities [43].

The concept of an IDS as an information security system has evolved considerably over the past 30 years. During these years, researchers have proposed various methods and techniques for protecting different types of systems using IDSs. In 1987, Denning presented an intrusion detection model that could compare malicious attack behavior against the normal model for the system of interest [44].

In 2000, Axelsson [45] surveyed 20 research projects on IDSs. He listed fourteen IDSs relying on host-based methods, two IDSs relying on network-based methods and three IDSs relying on both host-based and network-based methods. However, the IDS model used in those studies was out of date and depended on the local machine more than on the network traffic during the analysis stage.

In 2013, Ganapathy et al. [46] presented a survey on intelligent techniques for feature selection and classification-based intrusion detection in networks. This survey considered fuzzy techniques, neural networks, genetic algorithms, neuro-genetic algorithms, particle swarm intelligence and rough sets for Internet security protection and QoS enhancement. Moreover, these authors proposed new feature selection and classification

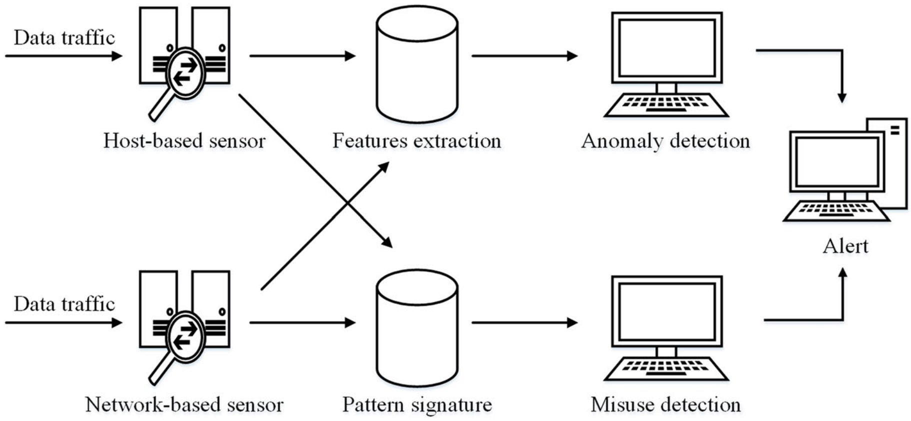

Fig. 5 IDS operations. IDS operations can be divided into the monitoring stage, the analysis stage and the detection stage

algorithms. In their experiment, they used 19 flow-based features comprising basic features, packet content features and traffic features.

In 2014, Mitchell and Chen [47] surveyed 60 papers on IDSs designed for wireless environments. Their survey revealed the strengths and weaknesses of IDS techniques for wireless local area networks (WLANs), wireless mesh networks (WMNs), wireless personal area networks (WPANs), wireless sensor networks (WSNs), cyber-physical systems (CPSs), ad hoc networks and mobile telephony.

Mitchell and Chen [47] proved that an anomaly-based IDS is the most suitable design for mobile telephony systems. However, such IDSs face challenges in terms of their high false positive rate and computational complexity [47]. High false positive and false negative rates reduce the QoS of a mobile network system. If any user packet is dropped by mistake, the user will suffer a billing error, and the user packet will be delayed [47]. Anomaly-based IDSs also face challenges with regard to illegal analysis methods, such as packet-based methods, that infringe on user privacy [47]. This survey proposed the detection latency as a critical metric for use in future research.

Also in 2014, Butun et al. [48] surveyed 18 papers focusing on mobile ad hoc networks (MANETs) and 17 papers focusing on WSNs in their survey on IDSs in WSNs. These authors discussed the feasibility of using systems designed for MANETs in WSNs. The possible security attacks against WSNs were divided into two categories: passive attacks and active attacks. These authors proved that IDSs are very important for the security of WSNs and that an IDS designed for a WSN must have certain special characteristics, including low power consumption. A WSN is a resource-constrained environment, so the effectiveness of an IDS in a WSN depends on its effect on the energy consumption of the network.

Butun et al. [48] recommended the use of a hierarchical IDS model to solve the energy consumption issue in WSNs. In accordance with the relevant application requirements, Butun et al. [48] recommended using a distributed IDS scheme for mobile applications, a centralized IDS scheme for stationary applications and a hierarchical IDS scheme for cluster-based applications.

IDSs: types and methods

The implementation of an IDS depends on the environment. A host-based intrusion detection system (HIDS) is designed to be implemented on a single system and to protect that system from intrusions or malicious attacks that will harm its operating system or data [49].

A HIDS generally depends on metrics in the host environment, such as the log files in a computer system [50]. These metrics or features are used as input to the decision engine of the HIDS. Thus, feature extraction from the host environment serves as the basis for any HIDS. The operational structure of a HIDS and its location in the network are shown in Fig. 6.

A network-based intrusion detection system (NIDS) sniffs network traffic packets to detect intrusions and malicious attacks [50]. A NIDS can be either a software-based system or a hardware-based system. For example, Snort NIDS is a software-based NIDS [51]. The operational structure of a NIDS and its location in the network are shown in Fig. 7.

Network expansion and increasing traffic volumes necessitate the implementation of IDSs as hardware

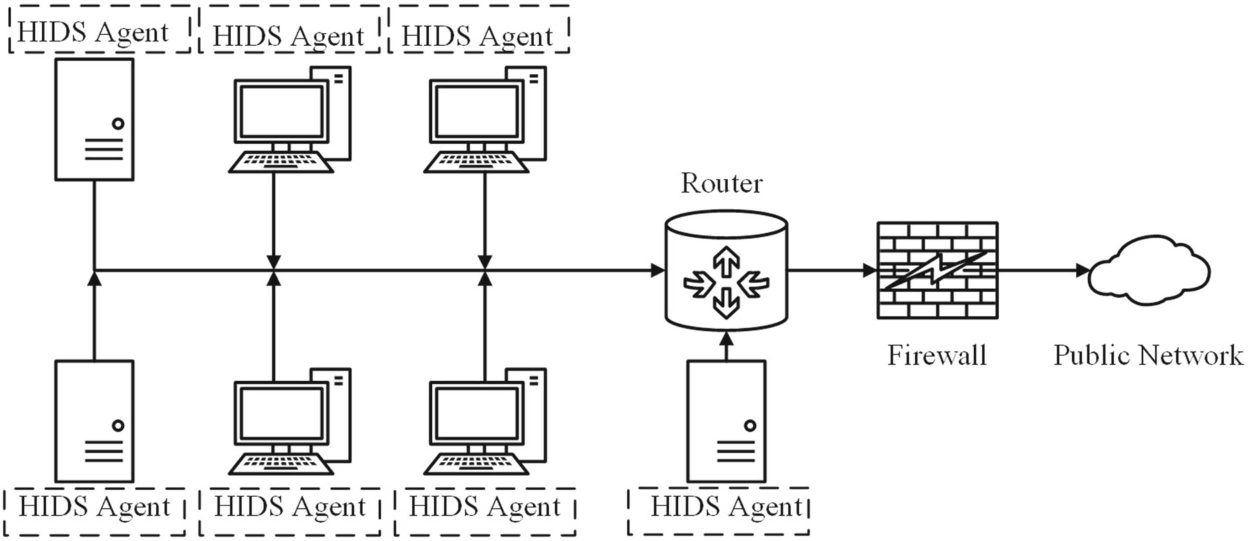

Fig. 6 Generic architecture of a host-based IDS (HIDS). The operational structure of a HIDS and its location in the network

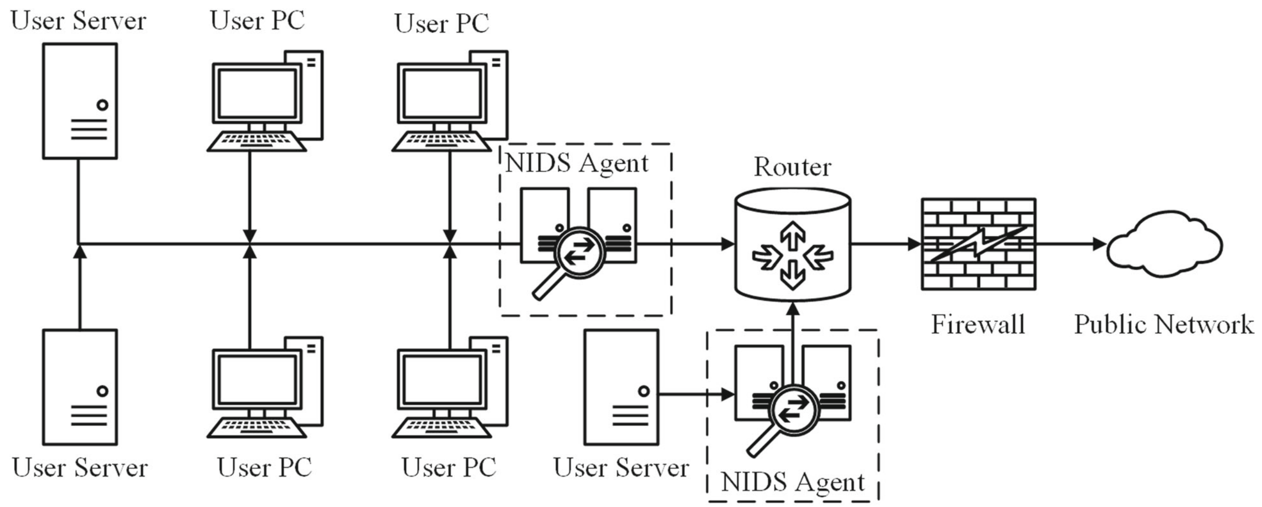

Fig. 7 Generic architecture of a network-based IDS (NIDS). The operational structure of a NIDS and its location in the network

systems, such as a smart sensor architecture [52]. For example, field programmable gate arrays (FPGAs) can be used as the basis of a hardware-based NIDS. The special characteristics of FPGAs, such as their ability to support high-speed interfaces, dynamic reprogramming and very high-volume data processing, make FPGAs very suitable for use in NIDSs [53].

IDSs: detection techniques

An IDS depends on algorithms for implementing the various stages of intrusion detection. There are a vast number of algorithms for all IDS types and methods. Some of these IDS algorithms will be discussed briefly in the section titled 'IDSs Designed for IoT Systems'.

Additionally, some of these IDS algorithms can be used for multiple different detection techniques. Thus, this section focuses on lightweight anomaly-based IDS algorithms that can be used in IoT-based environments depending on the complexity, execution time and detection time requirements. Principal component analysis (PCA) is a lightweight algorithm that can be used for various detection techniques in IDSs; thus, the PCA algorithm will be discussed as a representative example in the following.

Mori et al. [54] have stated that "principal component analysis (PCA) is a commonly used descriptive multivariate method for handling quantitative data and can be extended to deal with mixed measurement level data." Thus, PCA has been widely applied in various fields. As described by [55], PCA generates a set of variables depending on the variance-covariance structure of the original variables. These new variables are linear combinations of the original variables and are fewer in number than the original variables.

In IDSs, PCA is used as a dimensionality reduction and detection technique. Elrawy et al. [56] used the PCA approach to create an anomaly-based statistical and data mining IDS that depends on the division of the principal components into the most and least significant principal components. In this system, the detection stage relies on the major principal component score and the minor principal component score. In addition, PCA has been used in intrusion detection techniques based on payload modeling, statistical modeling, data mining and machine learning [56–58].

Misuse-based intrusion detection

A misuse-based intrusion detection technique uses a database of known signatures and patterns of malicious codes and intrusions to detect well-known attacks [59]. Network packet overload, the high cost of signature matching, and the large number of false alarms are three disadvantages of misuse-based IDSs [60]. In addition, the severe memory constraints in some types of networks, such as WSNs, result in low performance of misuse-based IDSs because of their need to store a large database of attack signatures [61].

Moreover, the signature and pattern databases in signature-based IDSs and pattern-matching IDSs need to be continuously updated. Such misuse-based IDSs are designed to detect malicious attacks and intrusions based on previous knowledge.

Anomaly-based intrusion detection

In an anomaly-based intrusion detection technique, a normal data pattern is created based on data from normal users and is then compared against current data patterns in an online manner to detect anomalies [62]. Such anomalies arise due to noise or other phenomena that have some probability of being created by hacking tools.

Thus, anomalies are unusual behaviors caused by intruders that leave footprints in the computing environment [63]. These footprints are detected in order to identify attacks, particularly unknown attacks.

An anomaly-based IDS operates by creating a model of the normal behavior in the computing environment, which is continuously updated, based on data from normal users and using this model to detect any deviation from normal behavior [64]. The advantages and disadvantages of various anomaly-based intrusion detection techniques are shown in Table 1. These techniques will be discussed in the following.

Table 1 A short comparison between anomaly IDS techniques with a focus on the advantages and disadvantages of each technique

Technique	Advantages	Disadvantages
Data mining	1- Models are created automatically	1- Based on historical data
	2- Applicable in different environments	2- Depends on complex algorithms
	3- Suitable for online datasets	
Machine learning	1- High detection accuracy	1- Requires training data
	2- Suitable for massive data volumes	2- Long training time
Statistical model	1- Suitable for online datasets	1- Based on historical behavior
	2- System simplicity	2- Detection accuracy depends on statistical and mathematical operations
Rule model	1- Suitable for online datasets	1- Based on a set of rules
	2- System simplicity	2- High false positive rate
Payload model	1- High detection accuracy for known attacks	1- Privacy issues
		2- Long processing time
Protocol model	1- High detection accuracy for a specific type of attack	1- Designed for a specific type of protocol
Signal processing model	1- High detection accuracy	1- Depends on complex pattern-recognition methods
	2- Low false positive rate	

- A data mining approach is a means for extracting knowledge from a large amount of data, analogous to extracting gold from numerous rocks and sand [65]. The extracted knowledge is defined as interesting patterns in the data [66]. Such a pattern can describe the behavior of data from users or networks in a computing environment. The ability to automatically generate models that depend on the traffic description is one of the advantages of the data mining approach. Moreover, this approach can be applied in generalized IDSs and in any computing environment [67]. The data mining approach works perfectly for an online data stream that is unbounded, continuous and rapidly increasing in volume [68]. A procedure consisting of a rule learning stage, a clustering stage, a classification stage, and a regression stage is applied in the design of an IDS based on this approach [68].
- Machine learning is a technique that depends on two stages: the training or learning stage and the detection or testing stage [69]. The training stage depends on mathematical algorithms or functions that use normal data as a reference input to learn the characteristics of the computing environment. Then, in the detection stage, these characteristics are used for detection and classification [70]. Supervised learning is one type of machine learning technique in which the characteristics of the training dataset are used in the learning phase to create a classification model, which is then used to classify new unseen instances [71]. Unsupervised learning is a type of machine learning technique that depends on the features of the data without using clustered training data [71].

  A pattern classification method in machine learning depends on pattern recognition, whereas a single classifier method depends on a single machine learning algorithm [72, 73].
- The statistical model approach depends on statistical mathematical operations [74]. The statistics of historical user behavior are used to create a normal model, and any deviations from this model are then detected. These deviations are considered abnormal data. The statistical model approach uses statistical mathematical operations applied to a training dataset to detect abnormal traffic from the observed traffic patterns [75].
- The rule model approach depends on the creation of rules for the computing environment. These rules are extracted from data traffic patterns. A rule-model-based IDS detects any anomalous data traffic that breaks these rules and considers any such anomaly as an attack [76]. The rule creation process depends on the historical system behavior. Thus, the system must be monitored for a long time to avoid an excessively high false positive rate.

- The payload model approach depends on the packet traffic of a specific port or user for a given application. In a signature-based IDS, the payload model is based on pattern matching to identify attack packets with specific characteristics [77]. By contrast, an anomaly-based IDS that uses the payload model approach creates a model that depends on bytes or calculations from bytes that describe the normal characteristics of the packet payload [57].
- The protocol model approach depends on monitoring protocols in different layers of the computing environment. An IDS based on this approach detects anomalies associated with a specific protocol or a protocol that is not present in the normal model. A specification-based approach, a parser-based approach or an approach based on application protocol keywords can be used to analyze the protocols in a computing environment [78].
- The signal processing model approach depends on traffic analysis using signal processing methods. An IDS based on this approach creates a normal pattern by capturing the statistics of normal data traffic and the data distribution over time, and any deviation from this pattern is considered to be an anomaly [79].

Specification-based intrusion detection

The concept of a specification-based IDS was proposed by Ko et al. [80] in 1997. They proposed a monitoring and detection system based on security specifications that determine the normal behavior of the system to be protected. These security specifications are created based on the functions and security policies for this system. Thus, operating sequences that are not included in the system behavior are considered security violations [81].

The most important challenge in designing a robust specification-based IDS is creating a formalism that captures the valid operating sequences of the system. Therefore, the cost of defining the specification "trace policy" and the difficulty of evaluating and verifying the specifications limit the real-world applicability of specification-based IDSs. A specification-based IDS learns the root characteristics of attacks and detects known attacks like a misuse-based IDS, and it also has the ability of anomaly-based IDSs to detect unknown attacks, such as operating sequences that are not included in the normal behavior of the system [82–84].

IDSs: performance evaluation

The measures used to assess IDS performance depend on four factors, namely, the numbers of true positives (α), true negatives (δ), false positives (γ) and false negatives (β), as described in Table 2. Following [85, 86], these factors and the performance metrics for IDSs are described below.

Table 2 The two-dimensional confusion matrices that define the main factors considered in IDS performance evaluation when predicting the anomaly and normal classes

		Predicting the anomaly class	
		Attack	Normal
Actual	Attack	α_A	β_A
Class	Normal	γ_A	δ_A
		Predicting the normal class	
		Normal	Attack
Actual	Normal	α_N	β_N
Class	Attack	γ_N	δ_N

When predicting the anomaly class, a true positive (α_A) is a correct classification that indicates an intrusion. A true negative (δ_A) is a correct classification that indicates no intrusion. A false positive (γ_A) is an incorrect classification that indicates an intrusion when there is no intrusion. A false negative (β_A) is an incorrect classification that indicates no intrusion when there is an intrusion. The true positive rate (TPR), which describes the probability of detecting intrusions, is calculated as:

$$TPR = \frac{\alpha_A}{\alpha_A + \beta_A} \tag{1}$$

The false positive rate (FPR), which describes the probability of incorrectly identifying normal behavior as an intrusion, is calculated as:

$$FPR = \frac{\gamma_A}{\gamma_A + \delta_A} \tag{2}$$

The recall (R), which describes the percentage of the total relevant records in a database that are retrieved by searching, is calculated in the same way as the TPR. The precision (P), which describes the percentage of relevant records among the records retrieved, is calculated as:

$$P = \frac{\alpha_A}{\alpha_A + \gamma_A} \tag{3}$$

The F-score (F), which describes the balance between P and R, is calculated as:

$$F = \frac{2 * P * R}{P + R} \tag{4}$$

The overall success rate, which describes the percentage of correct classifications, is calculated as:

$$SuccessRate = \frac{\alpha_A + \delta_A}{\alpha_A + \delta_A + \gamma_A + \beta_A} \tag{5}$$

$$ErrorRate = 1 - SuccessRate \tag{6}$$

When predicting the normal class, the same definitions and equations can be used, except with the parameters α_N, β_N, γ_N and δ_N.

IDSs designed for IoT systems

Due to the security challenges facing IoT systems, methods that can proactively identify new attacks are most suitable for protecting IoT networks. Thus, a robust IDS that can detect new attacks in IoT-based smart environments is required. An overview of the IDSs that have been proposed for IoT systems is shown in Table 3.

According to the recommendations in recent surveys of IDSs for IoT systems [3, 7], this paper focuses on the features of all IDS methods for the IoT that can be applied in smart environments. IoT systems require special security measures with particular characteristics that are not offered by traditional IDSs.

Liu et al. [87] proposed an artificial immune IDS for IoT networks. This system can adapt to the IoT environment and automatically learn new attacks. The system is based on machine learning and a signature-based model. The adopted machine learning approach is designed after the mechanisms of artificial immune systems. The objective of the system is to increase the security of the IoT network; thus, it is a network IDS. This system has two main features: self-adaptation to new environments and self-learning of new attacks.

Kasinathan et al. [88] proposed an IDS that detects DoS attacks based on 6LoWPAN in IoT networks. They proposed a DoS detection architecture that consists of an IDS probe, a DoS protection manager and a Suricata IDS [89]. They designed this system based on a study of the vulnerabilities present in IP-based WSNs. The Suricata [89] IDS runs on a host computer; thus, the advantage of this system is that it can overcome the problem of power consumption, thus conserving power resources in WSNs.

Moreover, Kasinathan et al. [90] proposed an enhanced IDS for detecting DoS attacks based on 6LoWPAN in IoT networks. This system depends on the DoS detection architecture presented in [88]; its main new elements are a frequency agility manager (FAM) and security incident and event management system (SIEM). These elements together create a monitoring system that can monitor large networks.

Jun and Chi [91] proposed an IDS integrated with complex event-processing (CEP) technology. The benefit of CEP technology is the ability to identify complex patterns via real-time data processing. The event-processing IDS architecture consists of an event filtering unit, an event database unit, a CEP unit and an action engine unit. The system depends on an event-processing model that uses the rule model approach to detect intrusions.

The main features of this system are that it operates in real time and shows high performance in detecting intrusions in an IoT system using an event-processing mechanism.

Krimmling and Peter [92] proposed a NIDS that depends on machine learning for anomaly-based and signature-based intrusion detection. The system framework is designed for smart public transport applications that use CoAP. The main features of this system are its applicability to CoAP applications and its reliance on a lightweight algorithm.

Butun et al. [93] proposed a NIDS for WSNs that combines the statistical model approach and the rule model approach. The system is based on a downward-IDS and an upward-IDS in accordance with the hierarchical WSN structure. The downward-IDS detects abnormal behavior of the member nodes, and the upward-IDS detects abnormal behavior of the cluster heads. The main features of this system are its applicability to hierarchical WSNs and its dependence on WSN clustering.

Surendar and Umamakeswari [82] proposed a constraint-based specification IDS for IoT networks using 6LoWPAN. This system maintains efficiency in terms of QoS metrics while detecting sinkhole attacks. The system isolates malicious nodes and reconstructs the network without these nodes. This IDS is a specification-based IDS that depends on behavioral rules and uses the protocol model approach.

The main features of this system are that it detects sinkhole attacks, preserves QoS and isolates malicious nodes.

In addition, Le et al. [83] proposed a specification-based IDS for IoT networks using 6LoWPAN for the detection of several topology attacks against the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), such as sinkhole, rank, local repair, neighbor, and destination oriented directed acyclic graph (DODAG) information solicitation (DIS) attacks. In a DIS attack, for example, the attacker increases the overhead in the network by using malicious nodes to send DIS messages [94] with fake IP addresses to the malicious nodes' neighbors, forcing these other nodes to generate DODAG information objective (DIO) messages [83, 94]. The proposed IDS depends on analyzing the protocol behavior from trace files to learn the route establishment and maintenance procedures for a stable topology. The main features of this system are its high efficiency in detecting RPL topology attacks in an energy-efficient manner and its applicability to large-scale networks.

Moreover, Bostani and Sheikhan [84] proposed a hybrid IDS for IoT networks using 6LoWPAN for the detection of several RPL attacks. This system depends on specification-based intrusion detection modules, serving as IDS agents, in the router nodes and an anomaly-based intrusion detection module, serving as the main IDS, in the root node. The main features of this system are a reduction in the number of communication messages due to the lack of additional control messages or monitor nodes in the IDS design and its applicability to large-scale networks.

Table 3 A comparison of IDSs designed for IoT systems, with a focus on the types, techniques and features of these systems with respect to their adaptability to IoT-based smart environments

Reference	Type	Technique	Features
Liu et al. (2011) [87]	NIDS	Machine learning & Signature model Hybrid intrusion detection	1- Self-adaption 2- Self-learning
Kasinathan et al. (2013) [88]	NIDS	Rule model & Signature model Hybrid intrusion detection	1- Detection of DoS attacks in 6LoWPAN 2- Decreased false alarm rate
Kasinathan et al. (2013) [90]	NIDS	Rule model & Signature model Hybrid intrusion detection	1- Monitoring of large networks 2- Light weight and scalability 3- Detection of DoS attacks in 6LoWPAN
Jun and Chi (2014) [91]	NIDS	Rule model Anomaly-based intrusion detection	1- Real-time detection 2- High performance in real time
Krimmling and Peter (2014) [92]	NIDS	Machine learning & Signature model Hybrid intrusion detection	1- Applicability to CoAP applications 2- Light weight
Butun et al. (2015) [93]	NIDS	Statistical model & Rule model Hybrid intrusion detection	1- Applicability to hierarchical WSNs 2- Dependence on WSN clustering
Surendar and Umamakeswari (2016) [82]	NIDS	Protocol model Specification-based intrusion detection	1- Detection of sinkhole attacks in 6LoWPAN 2- QoS preservation 3- Isolation of malicious nodes
Le et al. (2016) [83]	NIDS	Protocol model Specification-based intrusion detection	1- Energy efficiency 2- Detection of RPL attacks in 6LoWPAN 3- Applicability to large-scale networks
Bostani and Sheikhan (2017) [84]	NIDS	Protocol model & Machine learning Hybrid intrusion detection	1- Detection of RPL attacks in 6LoWPAN 2- Real-time detection 3- Reduced number of communication messages
Garcia-Font et al. (2017) [95]	NIDS	Machine learning & Signature model Hybrid intrusion detection	1- Applicability to WSNs 2- Applicability to large-scale networks
Fu et al. (2017) [96]	NIDS	Protocol model & Signature model Hybrid intrusion detection	1- Classification of attacks into categories 2- Use of GUI tools
Deng et al. (2018) [97]	NIDS	Machine learning & Data mining Hybrid intrusion detection	1- Light weight 2- Improved detection efficiency with a low FPR
Amouri et al. (2018) [99]	NIDS	Protocol model & Machine learning Hybrid intrusion detection	1- Low computational complexity 2- Low resource requirements
Liu et al. (2018) [100]	NIDS	Machine learning & Data mining Hybrid intrusion detection	1- Adaptability to high-dimensional spaces 2- Reduced detection time 3- High accuracy on high-volume data
Abhishek et al. (2018) [101]	NIDS	Statistical model Anomaly-based intrusion detection	1- Real-time detection 2- Based on theoretical foundations with no need for training data
Oh et al. (2014) [102]	HIDS	Pattern matching Misuse-based intrusion detection	1- Reduced memory size requirements 2- Reduced processing workload 3- Increased speed 4- Scalable performance for a large number of patterns
Summerville et al. (2015) [103]	HIDS	Payload model Anomaly-based intrusion detection	1- Low latency 2- Ultralight weight 3- High throughput in hardware or software implementation
Mohan et al. (2016) [37]	HIDS	Rule model & Signature model Hybrid intrusion detection	1- Simplicity 2- Self-learning
Arrignton et al. (2016) [104]	HIDS	Machine learning Anomaly-based intrusion detection	1- High-efficiency monitoring 2- Cancellation of environment noise
Gupta et al. (2013) [105]	Hybrid IDS	Machine learning Anomaly-based intrusion detection	1- Real-time detection 2- Adaptability to wireless networks 3- Ability to operate as both a NIDS and a HIDS
Raza et al. (2013) [106]	Hybrid IDS	Protocol model & Machine learning Hybrid intrusion detection	1- Detection of RPL attacks in 6LoWPAN 2- Real-time detection 3- Light weight 4- Energy efficiency
Khan and Herrmann (2017) [107]	Hybrid IDS	Protocol model Anomaly-based intrusion detection	1- Light weight 2- Energy efficiency 3- Applicability in healthcare environments

Garcia-Font et al. [95] proposed a NIDS for WSNs that depends on a machine learning approach and a signature model. They used a signature-based detection engine and an anomaly-based detection engine to improve the detection rate and the FPR. The system is designed to help smart city administrators detect intrusions using the IDS and an attack classification schema. The objective of the system is to detect intrusions in WSNs in different smart city environments. The main feature of this system is its applicability to large-scale WSNs.

Fu et al. [96] proposed a NIDS that depends on signature-based and protocol-based anomaly detection. The proposed IDS structure focuses on detecting attacks on IoT networks without being affected by the heterogeneity of such a network. The detection method depends on comparing the abstracted action flows in the data packets against three databases based on the protocol type information for each packet. These databases are a standard protocol library, an abnormal action library and a normal action library. The proposed approach consists of an event monitor, an event database, an event analyzer, and a response unit. This approach provides a uniform intrusion detection method for IoT networks based on automata theory. The main features of this system are the classification of attacks into three categories and the development of graphical user interface (GUI) tools to graphically present the abstract action flows and detect possible intrusions.

Deng et al. [97] proposed a NIDS that depends on the fuzzy c-means clustering (FCM) algorithm and the PCA algorithm. The system combines a machine learning approach with a data mining approach to improve the accuracy of intrusion detection for IoT networks. The PCA algorithm is used for feature selection and reduction. The FCM algorithm is used as a clustering method. The KDD-CUP99 dataset [98] was used to evaluate the proposed system. The main features of this system are its light weight and its ability to improve the detection efficiency by achieving a low FPR.

Amouri et al. [99] proposed a NIDS based on the protocol model approach and machine learning. This system consists of two detection stages. In the first stage, namely, local detection, network behavior data are collected by dedicated sniffers to generate a set of correctly classified instances (CCIs) using a supervised learning approach based on decision trees. In the second stage, namely, global detection, CCIs are collected by supernodes to generate time-based profiles called the accumulated measures of fluctuation (AMoFs) for malicious and normal nodes separately.

The main features of this system are its low computational complexity and low resource requirements.

Liu et al. [100] proposed a NIDS that depends on the suppressed fuzzy clustering (SFC) algorithm and the PCA algorithm. This system combines machine learning and data mining to improve the accuracy of intrusion detection in high-dimensional space. The PCA algorithm is used for feature extraction. A novel prejudgment-based intrusion detection method using PCA and SFC is applied that divides the dimension-reduced data into high-risk and low-risk data. The main feature of this system is its adaptability to high-dimensional spaces, such as the IoT space. Moreover, the efficiency and effectiveness of the IDS are optimized by reducing the detection time and increasing the accuracy by means of a frequency self-adjustment algorithm.

Abhishek et al. [101] proposed a NIDS that depends on the packet drop probability (PDP) in an IoT device to monitor gateways and detect malicious gateways. The system uses the statistical model approach for anomaly-based intrusion detection using a likelihood ratio test to detect malicious gateways, which corrupt the communications between IoT devices and access points. One of the disadvantages of this system is that it can only detect malicious getaways that affect downlink packets; it does not consider malicious getaways that affect uplink packets from IoT devices. The main features of this system are that it is based on theoretical foundations instead of requiring training data and that it can detect malicious gateways in real time.

Oh et al. [102] proposed a lightweight malicious-pattern-matching IDS. They stressed that traditional IDSs are not applicable for smart objects due to the limited memory size and battery life of these objects. Thus, a powerful and lightweight IDS is required because of these restrictions. Oh et al. proposed the auxiliary skipping (AS) algorithm, the early decision with boundary searching (EBS) algorithm, and an approach that uses both AS and EBS (AS-EBS).

These algorithms reduce the number of matching operations that must be performed [102]. The system depends on a pattern-matching approach based on signature detection. The advantage of this system is that it can be applied to smart objects with limited memory size and battery life. The main features of this system are the reduced memory size required for matching operations, the reduced workload for processing on smart objects, the increased speed of processing, and its scalable performance for a large number of patterns.

Summerville et al. [103] proposed an ultralightweight deep packet anomaly detection approach that can be implemented on small IoT devices. The system is designed with a dependence on the bitwise AND operation and uses a payload model approach for anomaly-based intrusion detection. The main features of this system are its low latency, high throughput and ultralight weight.

Mohan et al. [37] proposed a HIDS that depends on signature-based and rule-based anomaly detection. The system uses the traditional signature-based technique in combination with Snort-rule-based intrusion detection. Thus, the system can detect known attacks using the signature database and unknown attacks using SNORT rules. The main challenge of this system is privacy because the system uses a deep packet inspection technique to detect attacks. The main features of this system are its simplicity and self-learning capability.

Arrignton et al. [104] proposed a HIDS that depends on a machine learning approach for anomaly-based intrusion detection. The machine learning approach is based on the mechanisms of artificial immune systems. The main features of this system are its use of a behavioral modeling IDS (BMIDS) to decide whether behavior is acceptable and its increased detection sensitivity achieved by canceling out environmental noise.

Gupta et al. [105] confirmed that the threat of attacks in IoT systems affects not only the computational environment but also human life and the economy. For this reason, they proposed a computational-intelligence-based IDS for wireless communications and IoT systems. They proposed a three-tier architecture as the basis of an intelligent IDS suitable for wireless networks; this architecture consists of an information storage unit, a computational intelligence and optimization unit, and a clustering and intrusion reporting unit. This system depends on a machine learning approach for anomaly-based intrusion detection.

The machine learning approach applied in this IDS is based on the swarm intelligence (SI) paradigm, which is a specific type of computational intelligence (CI) paradigm [105]. The system targets IP addresses to detect attacks; thus, it has the disadvantage that it cannot be applied in regions of WSNs that do not use the TCP/IP protocol. The main feature of this system is its ability to operate as both a NIDS and a HIDS.

Raza et al. [106] proposed a hybrid-based IDS for IoT networks using 6LoWPAN for the detection of several RPL attacks. They proposed the SVELTE IDS, which consists of a 6LoWPAN mapper unit, an intrusion detection unit and a mini-firewall unit. The 6LoWPAN mapper unit collects information about the RPL network. The intrusion detection unit analyzes the data from the 6LoWPAN mapper unit to detect intrusions. The mini-firewall unit filters unwanted traffic. This system is designed for distributed and centralized IDS placement strategies. The main features of this system are its light weight and energy efficiency.

Khan and Herrmann [107] proposed three algorithms based on the protocol model approach using a trust management mechanism for IoT networks. One of these algorithms is neighbor based trust dissemination (NBTD), which can be used to implement a NIDS in a border router using the centralized approach. The second algorithm is tree based trust dissemination (TTD), which can be used to implement a HIDS in a small network with extra-high communication costs using the distributed approach. The third algorithm is clustered neighbor based trust dissemination (CNTD), which can be used to implement a NIDS using the distributed approach to reduce the number of packet exchanges compared with the NBTD algorithm. The main features of these algorithms are their light weight, energy efficiency and applicability in healthcare environments.

Performance analysis

In this section, a descriptive statistical analysis is applied to the reviewed papers based on several performance metrics: the TPR, FPR, energy consumption, processing time and performance overhead. The suitability of an IDS for IoT-based smart environments depends on these metrics; thus, they are the focus of this study.

In a traditional communication network, the performance of an IDS depends on the TPR and FPR only. In an IoT-based smart environment, the energy consumption, processing time and performance overhead of an IDS are also of critical interest. Because of the power and memory limitations of IoT devices, these metrics are very important to the QoS of an IoT system. Therefore, they are important performance metrics for an IDS designed for IoT-based smart environments.

Table 4 summarizes the technical details of the surveyed papers in terms of the important performance metrics of the proposed IDSs and their effects on smart environments. In Table 4, the symbol - indicates that no experimental result is available for the corresponding metric. The symbol * indicates that no numerical result was determined for this metric. The terms MAX and MAX range refer to the maximum result or maximum range result, respectively, for this metric.

Table 4 merely summarizes the experimental results from the surveyed papers; it is not intended as a comparison of these results. The experiments reported in these papers were performed under different conditions and using databases of different sizes. Thus, a standard IoT workbench with a standard IoT database would be required to conduct a fair comparison.

Tables 3 and 4 illustrate that the majority of researchers focus on three parameters during the testing stage: the TPR, FPR and processing time. Thus, IDSs are designed based on four features. First, such a system should be compatible with IoT systems. Second, it should be able to detect attacks in real time. Third, it should depend on lightweight algorithms. Fourth, it should be scalable.

Tables 3 and 4 show that some previous IDS studies did not present experimental results, whereas others presented only system methodologies that were not subjected to real experiments. Only a few previous IDS studies

Table 4 A descriptive statistical analysis of the surveyed IDSs in terms of the important performance metrics affecting IDS suitability in IoT systems

Reference	TPR (%)	FPR (%)	Energy (J)	Processing time (s)	Performance overhead
Liu et al. (2011) [87]	-	-	-	-	-
Kasinathan et al. (2013) [88, 90]	MAX range TP = (20-25)	Zero	-	*	-
Jun and Chi (2014) [91]	*	*	-	MAX 0.422	MAX memory = 730 MB MAX CPU = 62%
Krimmling and Peter (2014) [92]	*	*	-	-	-
Butun et al. (2015) [93]	MAX range (90-100)	at MAX TPR Zero	-	-	-
Surendar and Umamakeswari (2016) [82]	*	*	MAX range for one node (0.09-0.1)	-	*
Le et al. (2016) [83]	MAX 100	at MAX TPR 6.78	for one node 0.12	120	-
Bostani and Sheikhan (2017) [84]	MAX 100	at MAX TPR 2.98		-	-
Garcia-Font et al. (2017) [95]	MAX range (50-60)	at MAX TPR (25-30)	-	-	-
Fu et al. (2017) [96]	*	*	-	*	-
Deng et al. (2018) [97]	96.8	1.6	-	*	-
Amouri et al. (2018) [99]	100	*	-	3000	-
Liu et al. (2018) [100]	MAX 97.4	1.5	-	MAX range (0.5-0.6)	-
Abhishek et al. (2018) [101]	MAX 100	at MAX TPR 5.5	-	-	-
Oh et al. (2014) [102]	100	Zero	-	MAX at best performance = 40	-
Summerville et al. (2015) [103]	MAX 100	*	-	-	-
Mohan et al. (2016) [37]	*	*	-	-	-
Arrignton et al. (2016) [104]	*	*	-	-	-
Gupta et al. (2013) [105]	-	-	-	-	-
Raza et al. (2013) [106]	MAX range (80-100)	at MAX TPR Zero	for one node 2.88	120	Memory 1.76 KB
Khan and Herrmann (2017) [107]	MAX 100	at MAX TPR 1.1	*	-	*

The symbol (-) indicates that no experimental result is available for the corresponding metric. The symbol * indicates that no numerical result was determined for this metric. The terms MAX and MAX range refer to the maximum result or maximum range result, respectively, for this metric. The terms CPU, memory, TP, TPR, and FPR denote the utilization of the central processing unit (as a percentage), the memory consumption (in bytes), the number of anomalies correctly classified, the probability of detecting intrusions (as a percentage) and the probability of incorrectly identifying normal data as an intrusion (as a percentage), respectively. The energy and processing time values are measured in units of joules and seconds, respectively

have presented practical results for the performance metrics that characterize the suitability of IDSs for IoT-based smart environments. Thus, the development of IDSs for IoT-based smart environments is still in an incipient phase.

Discussion and future outlook

Integrity, confidentiality, and availability are three important factors in IoT systems. In most cases, applications that use the IoT model are considered to be vital, such as industrial and medical applications. On the one hand, these applications can be real-time applications; thus, network delay and latency directly affect their performance. On the other hand, attacks such as DoS, DDoS, probing, and RPL attacks can degrade the usability of these applications. Thus, security issues can be considered a life-threatening concern in e-health systems, for example [108]. Consequently, powerful security measures are required in IoT networks. Such a security mechanism must protect the IoT network and its resources without impacting the system's performance or user privacy.

Moreover, IoT-based smart environments consist of a wide range of devices, sensors and IoT objects from different vendors and based on different IoT platforms. Thus, interoperability issues prevent the emergence of IoT technology at a large scale [109]. Interoperability and standardization issues must be considered in designing IDSs for IoT-based smart environments.

IoT networks suffer from power efficiency problems; thus, a lightweight IDS that requires only a small number of computational operations is needed. In a HIDS, the IoT devices must simultaneously perform the necessary computational operations for the IDS and for IoT services. Thus, power resources and battery life must be considered in HIDS designs. Because of the power and memory limitations of IoT systems, the energy consumption, processing time and performance overhead of an IDS are important performance metrics. Thus, these metrics must be considered when designing IDSs for IoT-based smart environments. These issues should receive greater focus in research on HIDSs for such environments.

Privacy is another important factor in IoT systems. Deep packet inspection techniques are considered a violation of privacy. Such techniques and other techniques with similar characteristics are therefore undesirable. Moreover, the blocking of normal data packets affects IoT applications and services. This effect is very harmful, particularly for vital and real-time applications, such as industrial and medical applications. Therefore, introducing a smart system without deep packet inspection requires trusting that the operations in the IoT system will prevent any unauthorized access to IoT objects, thus helping to solve the user privacy problem. A new IDS design with a very low FPR and a very high detection accuracy is required for application in vital and real-time applications because traditional IDSs cannot satisfy these requirements.

An IDS based on a hybrid intrusion detection technique is required to detect different types of attacks from different computational environments. The IDS must be compatible with the 6LoWPAN protocol to detect attacks in WSNs in IoT networks. Furthermore, an autonomous IDS that can detect intrusions without human intervention is required for application in the IoT environment.

IDS placement is also a serious issue that must be considered when designing any type of IDS, whether it is a NIDS or a HIDS. The placement of the IDS in the IoT network will affect the overall efficiency of the IDS. There are two general IDS placement strategies: centralized and distributed. The centralized strategy offers the advantage of centralized management but can also lead to system processing overload, which may affect the QoS in IoT networks. The distributed strategy has the advantages of reducing the amount of monitored traffic and increasing the processing capacity. However, implementing an IDS in different regions of an IoT network is a challenge due to the associated management issues.

Finally, there is a need for both normal and anomaly databases that are up to date and integrated with IoT applications and services. These databases will be very useful for testing different IDS types and techniques in IoT environments. The ability to perform successful and meaningful IDS comparisons will depend on these databases.

Concluding remarks

As the numbers of IoT users, services, and applications increase, an urgent need for a robust and lightweight security solution that is suitable for use in IoT environments is emerging. Furthermore, IoT networks are the basis of smart environments; thus, any deficiencies in the security of these IoT networks will directly influence the smart environments on which they are based. Attacks such as DoS, DDoS, probing, and RPL attacks affect the services and applications offered in IoT-based smart environments; thus, the security of IoT environments is a very serious issue. An IDS is one possible solution for this issue. This has paper presented a survey of IDSs designed for IoT environments. Recommendations for designing a robust and lightweight IDS were also discussed.

In this survey, several papers were investigated. These papers mainly study the design and implementation of IDSs for use in the IoT paradigm that can be applied in smart environments. The features of all IDS methods presented in these papers were summarized. Moreover, this paper proposed some recommendations that must be considered when designing an IDS for the IoT, such as the need for a powerful and lightweight system with a suitable placement strategy that does not adversely affect the integrity, confidentiality, and availability of the IoT environment. This study showed that there is a need to design an integrated IDS that can be applied in IoT-based smart environments. This design will need to be tested on a unified IoT database. The question of the placement strategy must be considered in this design.

Future work will investigate the design of a high-performance hybrid IDS specifically designed for IoT-based smart environments based on the recommendations of this study. Moreover, the security vulnerabilities of IoT enabling technologies and protocols will be considered in the IDS design. In addition, the IDS will be implemented on programmable reconfigurable hardware devices, such as FPGAs, to facilitate adaptation to IoT-based smart environments. The design should be suitable for both distributed and centralized placement strategies and have the ability to detect different types of attacks.

Abbreviations

6LoWPAN: IPv6 over low-power wireless personal area networks; AMoF: Accumulated measure of fluctuation; AS: Auxiliary skipping; AS-EBS: Auxiliary skipping and early decision with boundary searching; BMIDS: Behavior modeling IDS; CCIs: Correctly classified instances; CEP: Complex event processing; CI: Computational intelligence; CNTD: Clustered neighbor based trust dissemination; CoAP: Constrained Application Protocol; CPSs: Cyber-physical systems; CPU: Central processing unit; DDoS: Distributed denial-of-service; DIO: DODAG information objective; DIS: DODAG information solicitation; DODAG: Destination oriented directed acyclic graph; DoS: denial-of-service; EBS: Early decision with boundary searching; EPC: Electronic product code; FAM: Frequency agility manager; FCM: Fuzzy c-means clustering; FPGA: Field programmable gate array; FPR: False positive rate; GUI: Graphical user interface; HIDS: Host-based intrusion detection system; ICT: Information and communication technology; IDS: Intrusion detection system; IoE: Internet of Everything; IoT: Internet of Things; IP: Internet Protocol; IPv6: Internet Protocol version 6; LoRa: Long range; LoRaWAN protocol: Low Power WAN Protocol for Internet of Things; LPWAN: Low-power wide-area network; MANETs: Mobile ad hoc networks; M2M: Machine-to-machine; NBTD: Neighbor based trust dissemination; NIDS: Network-based intrusion detection system; PCA: Principal component analysis; PDP: Packet drop probability; QoS: Quality of service; RFID: Radio frequency identification; RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks; SFC: Suppressed fuzzy clustering; SI: Swarm intelligence; SIEM: Security incident and event management system; TCP: Transmission Control Protocol; TPR: True positive rate; TTD: Tree based trust dissemination; WLAN: Wireless local area network; WMN: Wireless mesh network; WPAN: Wireless personal area network; WSN: Wireless sensor network

Funding

Not applicable.

Availability of data and materials

Not applicable.

Authors' contributions

All authors contributed to the structure of the paper, the analysis of the results, and the writing process. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Author details

[1]Department of Electronics and Communication Engineering, MUST University, 6th of October, Egypt. [2]Institute of Public Administration, Abha, Asir, Saudi Arabia. [3]Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, SE-97187 Luleå, Sweden. [4]Faculty of Engineering, Al-Azhar University, P.O. Box 83513 Qena, Egypt. [5]Faculty of Engineering, Minia University, P.O. Box 61111 Minia, Egypt.

Received: 17 February 2018 Accepted: 4 November 2018
Published online: 04 December 2018

References

1. King J, Awad AI (2016) A distributed security mechanism for resource-constrained IoT devices. Informatica (Slovenia) 40(1):133–143
2. Weber M, Boban M (2016) Security challenges of the internet of things. In: 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, Opatija. pp 638–643
3. Gendreau AA, Moorman M (2016) Survey of intrusion detection systems towards an end to end secure internet of things. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, Vienna. pp 84–90
4. Kafle VP, Fukushima Y, Harai H (2016) Internet of things standardization in ITU and prospective networking technologies. IEEE Commun Mag 54(9):43–49
5. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M (2014) Internet of things for smart cities. IEEE Internet Things J 1(1):22–32
6. IoT Bots Cause Massive Internet Outage. https://www.beyondtrust.com/blog/iot-bots-cause-october-21st-2016-massive-internet-outage/. Accessed 22 Oct 2016
7. Zarpelão BB, Miani RS, Kawakani CT, de Alvarenga SC (2017) A survey of intrusion detection in internet of things. J Netw Comput Appl 84:25–37
8. Ayoub W, Mroue M, Nouvel F, Samhat AE, Prévotet J (2018) Towards IP over LPWANs technologies: LoRaWAN, DASH7, NB-IoT. In: 2018 Sixth International Conference on Digital Information, Networking, and Wireless Communications (DINWC). IEEE, Beirut. pp 43–47
9. Aras E, Ramachandran GS, Lawrence P, Hughes D (2017) Exploring the security vulnerabilities of LoRa. In: 2017 3rd IEEE International Conference on Cybernetics (CYBCONF). IEEE, Exeter. pp 1–6
10. Butun I, Pereira N, Gidlund M (2018) Analysis of LoRaWAN v1.1 security. In: Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects, SMARTOBJECTS '18. ACM, New York. pp 5–156
11. Čolaković A, Hadžialić M (2018) Internet of things (IoT): A review of enabling technologies, challenges, and open research issues. Comput Netw 144:17–39
12. IEEE The institute, Special Report:The Internet of Things. http://theinstitute.ieee.org/static/special-report-the-internet-of-things. Accessed 8 Jan 2017
13. Thiesse F, Michahelles F (2006) An overview of EPC technology. Sens Rev 26(2):101–105
14. Minerva R, Biru A, Rotondi D (2015) Towards a definition of the internet of things (IoT). Technical report, IEEE, Internet of Things
15. SPU (2005) The internet of things executive summary. Technical report, The ITU Strategy & Policy Unit, (SPU)
16. Krčo S, Pokrić B, Carrez F (2014) Designing IoT architecture(s): A european perspective. In: 2014 IEEE World Forum on Internet of Things (WF-IoT). IEEE, Seoul. pp 79–84
17. Ray PP (2018) A survey on Internet of Things architectures. J King Saud Univ Comput Inform Sci 30(3):291–319
18. Bradley J, Loucks J, Macaulay J, Noronha A (2013) Internet of everything (IoE) value index. Technical report, Cisco
19. IEEE (2015) Standards, Internet of Things, IEEE P2413. http://standards.ieee.org/develop/project/2413.html. Accessed 8 Jan 2017
20. Bandyopadhyay D, Sen J (2011) Internet of things: Applications and challenges in technology and standardization. Wirel Pers Commun 58(1):49–69
21. Han C, Jornet JM, Fadel E, Akyildiz IF (2013) A cross-layer communication module for the internet of things. Comput Netw 57(3):622–633
22. Khan R, Khan S, Zaheer R, Khan S (2012) Future internet: The internet of things architecture, possible applications and key challenges. In: 2012 10th International Conference on Frontiers of Information Technology. IEEE, Islamabad. pp 257–260
23. Rao BBP, Saluia P, Sharma N, Mittal A, Sharma SV (2012) Cloud computing for internet of things & sensing based applications. In: 2012 Sixth International Conference on Sensing Technology (ICST). IEEE, Kolkata. pp 374–380
24. Khan Z, Kiani SL, Soomro K (2014) A framework for cloud-based context-aware information services for citizens in smart cities. J Cloud Comput 3(1):14
25. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015) Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Commun Surv Tutor 17(4):2347–2376
26. Charif B, Awad AI (2014) Business and government organizations' adoption of cloud computing. In: Corchado E, Lozano JA, Quintián H,

Yin H (eds). Intelligent Data Engineering and Automated Learning – IDEAL 2014. Springer, Cham. pp 492–501

27. Citron R, Maxwell K, Woods E (2017) Smart city services market. Technical report, Navigant Research
28. Ahmed E, Yaqoob I, Gani A, Imran M, Guizani M (2016) Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. IEEE Wirel Commun 23(5):10–16
29. Schaffers H, Komninos N, Pallot M, Trousse B, Nilsson M, Oliveira A (2011) Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation. Springer, Berlin
30. Taherkordi A, Eliassen F (2016) Scalable modeling of cloud-based IoT services for smart cities. In: 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops). IEEE, Sydney. pp 1–6
31. Ali B, Awad AI (2018) Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors 18(3):1–17
32. Granjal J, Monteiro E, SáSilva J (2015) Security for the internet of things: A survey of existing protocols and open research issues. IEEE Commun Surv Tutor 17(3):1294–1312
33. Kumar S, Vealey T, Srivastava H (2016) Security in internet of things: Challenges, solutions and future directions. In: 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa. pp 5772–5781
34. Liu X, Zhao M, Li S, Zhang F, Trappe W (2017) A security framework for the internet of things in the future internet architecture. Future Internet 9(3)
35. Trappe W, Howard R, Moore RS (2015) Low-energy security: Limits and opportunities in the internet of things. IEEE Secur Priv 13(1):14–21
36. Hassan AM, Awad AI (2018) Urban transition in the era of the internet of things: Social implications and privacy challenges. IEEE Access 6:36428–36440
37. Mohan R, Danda J, Hota C (2016) Attack Identification Framework for IoT Devices. Springer, New Delhi
38. Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D (2014) Security of the internet of things: perspectives and challenges. Wirel Netw 20(8):2481–2501
39. Forsström S, Butun I, Eldefrawy M, Jennehag U, Gidlund M (2018) Challenges of securing the industrial internet of things value chain. In: 2018 Workshop on Metrology for Industry 4.0 and IoT. IEEE, Brescia. pp 218–223
40. Rubio-Loyola J, Sala D, Ali AI (2008) Accurate real-time monitoring of bottlenecks and performance of packet trace collection. In: 2008 33rd IEEE Conference on Local Computer Networks (LCN). IEEE, Montreal. pp 884–891
41. Rubio-Loyola J, Sala D, Ali AI (2008) Maximizing packet loss monitoring accuracy for reliable trace collections. In: 2008 16th IEEE Workshop on Local and Metropolitan Area Networks. IEEE, Chij-Napoca. pp 61–66
42. Ghorbani AA, Lu W, Tavallaee M (2010) Network Intrusion Detection and Prevention, Advances in Information Security, vol. 47. Springer, US
43. Anwar S, Mohamad Zain J, Zolkipli MF, Inayat Z, Khan S, Anthony B, Chang V (2017) From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions. Algorithms 10(2):1–24
44. Denning DE (1987) An intrusion-detection model. IEEE Trans Softw Eng SE-13(2):222–232
45. Stefan A (2000) Intrusion detection systems: A survey and taxonomy. Technical report, Chalmers University of Technology Göteborg, Sweden
46. Ganapathy S, Kulothungan K, Muthurajkumar S, Vijayalakshmi M, Yogesh P, Kannan A (2013) Intelligent feature selection and classification techniques for intrusion detection in networks: a survey. EURASIP J Wirel Commun Netw 2013(1):1–16
47. Mitchell R, Chen I-R (2014) A survey of intrusion detection in wireless network applications. Comput Commun 42:1–23
48. Butun I, Morgera SD, Sankar R (2014) A survey of intrusion detection systems in wireless sensor networks. IEEE Commun Surv Tutor 16(1):266–282
49. Creech G, Hu J (2014) A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns. IEEE Trans Comput 63(4):807–819
50. Kumar S, Gautam, Om H (2016) Computational neural network regression model for host based intrusion detection system. Perspect Sci 8:93–95
51. Snort The Open Source Network Intrusion Detection System. https://www.snort.org. Accessed 1 Nov 2016
52. Macia-Perez F, Mora-Gimeno FJ, Marcos-Jorquera D, Gil-Martinez-Abarca JA, Ramos-Morillo H, Lorenzo-Fonseca I (2011) Network intrusion detection system embedded on a smart sensor. IEEE Trans Ind Electron 58(3):722–732
53. Pontarelli S, Bianchi G, Teofili S (2013) Traffic-aware design of a high-speed fpga network intrusion detection system. IEEE Trans Comput 62(11):2322–2334
54. Mori Y, Kuroda M, Makino N (2016) Nonlinear Principal Component Analysis and Its Applications, JSS Research Series in Statistics. Springer, Singapore
55. Jolliffe IT (2002) Principal Component Analysis, Springer Series in Statistics, vol. 2. Springer, New York
56. Elrawy MF, Awad AI, Hamed HFA (2016) Flow-based features for a robust intrusion detection system targeting mobile traffic. In: 2016 23rd International Conference on Telecommunications (ICT). IEEE, Thessaloniki. pp 1–6
57. Nwanze N, i. Kim S, Summerville DH (2009) Payload modeling for network intrusion detection systems. In: MILCOM 2009 - 2009 IEEE Military Communications Conference. IEEE, Boston. pp 1–7
58. Chabathula KJ, Jaidhar CD, Kumara MAA (2015) Comparative study of principal component analysis based intrusion detection approach using machine learning algorithms. In: 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN). IEEE, Chennai. pp 1–6
59. Bul'ajoul W, James A, Pannu M (2015) Improving network intrusion detection system performance through quality of service configuration and parallel technology. J Comput Syst Sci 81(6):981–999
60. Meng W, Li W, Kwok L-F (2014) Efm: Enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism. Comput Secur 43:189–204
61. Abduvaliyev A, Pathan ASK, Zhou J, Roman R, Wong WC (2013) On the vital areas of intrusion detection systems in wireless sensor networks. IEEE Commun Surv Tutor 15(3):1223–1237
62. Bhuyan MH, Bhattacharyya DK, Kalita JK (2014) Network anomaly detection: Methods, systems and tools. IEEE Commun Surv Tutor 16(1):303–336
63. Hong J, Liu C, Govindarasu M (2014) Integrated anomaly detection for cyber security of the substations. IEEE Trans Smart Grid 5(4):1643–1653
64. Mishra P, Pilli ES, Varadharajan V, Tupakula U (2017) Intrusion detection techniques in cloud environment: A survey. J Netw Comput Appl 77:18–47
65. Han J, Kamber M, Pei J (eds) (2012) Data mining: concepts and techniques. Morgan Kaufmann, Boston
66. Duque S, bin Omar MN (2015) Using data mining algorithms for developing a model for intrusion detection system (IDS). Procedia Comput Sci 61:46–51
67. Feng W, Zhang Q, Hu G, Huang JX (2014) Mining network data for intrusion detection through combining SVMs with ant colony networks. Futur Gener Comput Syst 37:127–140
68. Alseiari FAA, Aung Z (2015) Real-time anomaly-based distributed intrusion detection systems for advanced metering infrastructure utilizing stream data mining. In: 2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE). IEEE, Offenburg. pp 148–153
69. Tsai JJP, Yu PS (eds) (2009) Machine Learning in Cyber Trust: Security, Privacy, and Reliability. First edn. Springer US, Springer-Verlag US. pp 1–362
70. Nishani L, Biba M (2016) Machine learning for intrusion detection in MANET: a state-of-the-art survey. J Intell Inf Syst 46(2):391–407
71. Namdev N, Agrawal S, Silkari S (2015) Recent advancement in machine learning based internet traffic classification. Procedia Comput Sci 60:784–791
72. Tsai C-F, Hsu Y-F, Lin C-Y, Lin W-Y (2009) Intrusion detection by machine learning: A review. Expert Syst Appl 36(10):11994–12000
73. Weller-Fahy DJ, Borghetti BJ, Sodemann AA (2015) A survey of distance and similarity measures used within network intrusion anomaly detection. IEEE Commun Surv Tutor 17(1):70–91
74. Amin SO, Siddiqui MS, Hong CS, Lee S (2009) RIDES: Robust intrusion detection system for ip-based ubiquitous sensor networks. Sensors 9(5):3447

75. Muzammil MJ, Qazi S, Ali T (2013) Comparative analysis of classification algorithms performance for statistical based intrusion detection system. In: 2013 3rd IEEE International Conference on Computer, Control and Communication (IC4), Karachi. pp 1–6
76. Mabu S, Chen C, Lu N, Shimada K, Hirasawa K (2011) An intrusion-detection model based on fuzzy class-association-rule mining using genetic network programming, Vol. 41
77. Xu C, Chen S, Su J, Yiu SM, Hui LCK (2016) A survey on regular expression matching for deep packet inspection: Applications, algorithms, and hardware platforms. IEEE Commun Surv Tutor 18(4):2991–3029
78. Davis JJ, Clark AJ (2011) Data preprocessing for anomaly based network intrusion detection: A review. Comput Secur 30(6–7):353–375
79. Vancea F, Vancea C (2015) Some results on intrusion and anomaly detection using signal processing and NEAR system. In: 2015 38th International Conference on Telecommunications and Signal Processing (TSP). IEEE, Prague. pp 113–116
80. Ko C, Ruschitzka M, Levitt K (1997) Execution monitoring of security-critical programs in distributed systems: a specification-based approach. In: 1997 IEEE Symposium on Security and Privacy, Oakland. pp 175–187
81. Berthier R, Sanders WH (2011) Specification-based intrusion detection for advanced metering infrastructures. In: 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing. IEEE, Pasadena. pp 184–193
82. Surendar M, Umamakeswari A (2016) InDReS: An intrusion detection and response system for internet of things with 6LoWPAN. In: 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai. pp 1903–1908
83. Le A, Loo J, Chai KK, Aiash M (2016) A specification-based IDS for detecting attacks on RPL-based network topology. Information 7(2):1–19
84. Bostani H, Sheikhan M (2017) Hybrid of anomaly-based and specification-based IDS for internet of things using unsupervised OPF based on MapReduce approach. Comput Commun 98:52–71
85. Gupta GP, Kulariya M (2016) A framework for fast and efficient cyber security network intrusion detection using apache spark. Procedia Comput Sci 93:824–831
86. Farissi IE, Saber M, Chadli S, Emharraf M, Belkasmi MG (2016) The analysis performance of an intrusion detection systems based on neural network. In: 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt). IEEE, Tangier. pp 145–151
87. Liu C, Yang J, Chen R, Zhang Y, Zeng J (2011) Research on immunity-based intrusion detection technology for the internet of things. In: 2011 Seventh International Conference on Natural Computation, vol. 1. IEEE, Shanghai. pp 212–216
88. Kasinathan P, Pastrone C, Spirito MA, Vinkovits M (2013) Denial-of-service detection in 6LoWPAN based internet of things. In: 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, Lyon. pp 600–607
89. Suricata The Next Generation Intrusion Detection System. https://oisf.net/. Accessed 5 Dec 2017
90. Kasinathan P, Costamagna G, Khaleel H, Pastrone C, Spirito MA (2013) DEMO: An IDS framework for internet of things empowered by 6LoWPAN. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer; Communications Security, CCS '13, Berlin. pp 1337–1340
91. Jun C, Chi C (2014) Design of complex event-processing IDS in internet of things. In: 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation. IEEE, Zhangjiajie. pp 226–229
92. Krimmling J, Peter S (2014) Integration and evaluation of intrusion detection for CoAP in smart city applications. In: 2014 IEEE Conference on Communications and Network Security. IEEE, San Francisco. pp 73–78
93. Butun I, Ra I-H, Sankar R (2015) An intrusion detection system based on multi-level clustering for hierarchical wireless sensor networks. Sensors 15(11):28960–28978
94. Alzubaidi M, Anbar M, Al-Saleem S, Al-Sarawi S, Alieyan K (2017) Review on mechanisms for detecting sinkhole attacks on RPLs. In: 2017 8th International Conference on Information Technology (ICIT). IEEE, Amman. pp 369–374
95. Garcia-Font V, Garrigues C, Rifà-Pous H (2017) Attack classification schema for smart city WSNs. Sensors 17(4):1–24
96. Fu Y, Yan Z, Cao J, Ousmane K, Cao X (2017) An automata based intrusion detection method for internet of things. Mob Inf Syst 2017:13
97. Deng L, Li D, Yao X, Cox D, Wang H (2018) Mobile network intrusion detection for IoT system based on transfer learning algorithm. Clust Comput 21:1–16
98. KDD Cup 1999 Data. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. Accessed 6 Oct 2018
99. Amouri A, Alaparthy VT, Morgera SD (2018) Cross layer-based intrusion detection based on network behavior for IoT. In: 2018 IEEE 19th Wireless and Microwave Technology Conference (WAMICON). IEEE, Sand Key. pp 1–4
100. Liu L, Xu B, Zhang X, Wu X (2018) An intrusion detection method for internet of things based on suppressed fuzzy clustering. EURASIP J Wirel Commun Netw 2018(1):113
101. Abhishek NV, Lim TJ, Sikdar B, Tandon A (2018) An intrusion detection system for detecting compromised gateways in clustered IoT networks. In: 2018 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR). IEEE, Austin. pp 1–6
102. Oh D, Kim D, Ro WW (2014) A malicious pattern detection engine for embedded security systems in the internet of things. Sensors 14(12):24188–24211
103. Summerville DH, Zach KM, Chen Y (2015) Ultra-lightweight deep packet anomaly detection for internet of things devices. In: 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC). IEEE, Nanjing. pp 1–8
104. Arrington B, Barnett L, Rufus R, Esterline A (2016) Behavioral modeling intrusion detection system (BMIDS) using internet of things (IoT) behavior-based anomaly detection via immunity-inspired algorithms. In: 2016 25th International Conference on Computer Communication and Networks (ICCCN), Waikoloa. pp 1–6
105. Gupta A, Pandey OJ, Shukla M, Dadhich A, Mathur S, Ingle A (2013) Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks. In: 2013 IEEE International Conference on Computational Intelligence and Computing Research. IEEE, Enathi. pp 1–7
106. Raza S, Wallgren L, Voigt T (2013) SVELTE: Real-time intrusion detection in the internet of things. Ad Hoc Netw 11(8):2661–2674
107. Khan ZA, Herrmann P (2017) A trust based distributed intrusion detection mechanism for internet of things. In: 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA). IEEE, Taipei. pp 1169–1176
108. Okoh E, Awad AI (2015) Biometrics applications in e-health security: A preliminary survey. In: Yin X, Ho K, Zeng D, Aickelin U, Zhou R, Wang H (eds). Health Information Science. Springer, Cham. pp 92–103
109. Noura M, Atiquzzaman M, Gaedke M (2018) Interoperability in internet of things: Taxonomies and open challenges. Mobile Networks and Applications 23:1–14