Security and Privacy in the Internet of Things: Threats, Requirements, and Countermeasures

Dr. Karthik Subramanian[1], Dr. Lavanya Venkatesh[2], Dr. Prakash Raman[3], Dr. Divya Anand[4]

ABSTRACT

The Internet of Things connects vast numbers of devices to networks, and the security and privacy of these devices and the data they carry are among the most pressing concerns of the field; this paper reviews the threats, requirements, and countermeasures. It describes the characteristics of the Internet of Things that make security difficult: the severe resource constraints of devices, which limit the cryptography they can perform; their physical accessibility and heterogeneity; their large numbers and long, poorly updatable lifetimes; and their often weak default configurations. It surveys the threats at each layer of the architecture, from physical tampering and node capture at the perception layer, through eavesdropping, interception, and denial of service at the network layer, to data breaches and weak authentication at the application layer. It sets out the security requirements, of confidentiality, integrity, availability, authentication, authorization, and privacy, and the countermeasures that address them, including lightweight cryptography, secure communication, device identity, secure boot and signed updates, access control, and intrusion detection, organised as defence in depth. It discusses the protection of privacy and the emerging approaches of hardware security and machine-learning-based detection. The study finds that securing the Internet of Things requires layered countermeasures adapted to the constraints of devices, and that it is limited by resource constraints, the difficulty of updates, and fragmentation. It notes that specific technologies and standards are representative of an evolving field. It concludes with the outlook. Certain figures are illustrative.

Page 45-55 © MANTECH PUBLICATIONS 2026. All Rights Reserved

KEYWORDS: *IoT Security, Privacy, Authentication, Lightweight Cryptography, Denial of Service, Secure Boot, Over-the-Air Updates, Defence in Depth, Intrusion Detection*

INTRODUCTION

The Internet of Things connects vast numbers of physical devices, sensors, appliances, industrial machines, and vehicles, to networks and to one another, and in doing so it extends the reach of computation into the physical world. This connection, however, exposes these devices, and the data they collect and the processes they control, to attack, and the security and privacy of the Internet of Things are therefore among the most pressing concerns of the field. Breaches have consequences that extend beyond the loss of data to the safety of physical systems and the integrity of infrastructure, and compromised devices have been assembled into large networks used to attack others. This paper reviews the threats to the Internet of Things, the security requirements it must meet, and the countermeasures that address them [1], [2].

Securing the Internet of Things is made difficult by several of its characteristics. Its devices are severely constrained in processing, memory, and energy, which limits the cryptographic and security functions they can perform; they are often physically accessible, exposing them to tampering and capture; they are heterogeneous, made by many manufacturers to many standards; they are deployed in vast numbers and for long periods, and are often difficult to update; and they are frequently configured with weak defaults, such as default passwords. These characteristics together create a large and varied attack surface that is hard to defend [1], [3].

Against this background, the security of the Internet of Things must be approached systematically, through an understanding of the threats at each layer, the requirements that must be met, and the countermeasures available, deployed in layers as defence in depth. The central purpose of this paper is to review these threats, requirements, and countermeasures, together with the protection of privacy and the emerging approaches to security. The paper draws on the established and current literature, notes that specific technologies and standards are representative of an evolving field, and notes that certain figures are illustrative.

LITERATURE REVIEW

Page 45-55 © MANTECH PUBLICATIONS 2026. All Rights Reserved

The security challenges and threats of the Internet of Things are described in the literature [1], [2], [4]. The literature emphasises that the constraints of devices, their physical accessibility, their heterogeneity, their scale, and their long and poorly updatable lifetimes make them difficult to secure, and it organises the threats by the layer of the architecture at which they arise. At the perception layer, where devices sense and act, the threats include physical tampering, the capture of nodes, the spoofing of sensors and tags, and side-channel attacks that extract secrets. At the network layer, the threats include the eavesdropping and interception of communication, replay and routing attacks, and denial of service, including the distributed denial of service mounted from large numbers of compromised devices. At the application and cloud layer, the threats include data breaches, weak authentication, insecure interfaces, and malware. The literature documents these threats and notes that the Internet of Things has been the target and the instrument of significant attacks [2], [5].

The security requirements and countermeasures are treated in the literature [4], [6], [7]. The requirements are the classical goals of information security, confidentiality, integrity, and availability, together with authentication of identity, authorization of actions, and the protection of privacy, applied to the particular setting of the Internet of Things. The countermeasures include cryptography, and in particular lightweight cryptography designed for constrained devices; the securing of communication by transport-layer and datagram transport-layer security; the establishment of device identity through keys, certificates, and secure hardware; the protection of devices through secure boot and the delivery of authenticated, signed updates; the control of access and the segmentation of networks; and the detection of intrusion, increasingly by methods based on machine learning. The literature stresses that no single countermeasure is sufficient and that security must be layered, as defence in depth, so that the failure of one layer does not compromise the whole [6], [7].

Privacy and the emerging approaches to security are treated in the literature [8], [9], [10]. The Internet of Things collects large quantities of data, much of it personal or revealing of behaviour, and the protection of privacy requires the minimisation of data, its anonymisation where possible, and adherence to principles of consent and purpose, informed by data-protection regulation; the processing of data at the edge, near its source, can assist privacy by keeping data local. The emerging approaches include the use of secure hardware, such as secure elements and trusted execution environments, to protect keys and computation; the use

Page 45-55 © MANTECH PUBLICATIONS 2026. All Rights Reserved

of distributed-ledger technologies for decentralised trust and identity; and the adoption of zero-trust architectures and of standards for the security of consumer and industrial devices. The literature presents these as directions in which the security of the Internet of Things is developing. These considerations frame the present review [8], [9], [10].

RESEARCH GAP

The threats, requirements, and countermeasures of Internet-of-Things security are treated in specialised literatures, but a concise, integrated account that presents the threats by layer, the security requirements, and the countermeasures organised as defence in depth, together with the protection of privacy, is useful for orientation. There is therefore value in a consolidated review that connects these elements and situates them within the security of the Internet of Things as a whole.

OBJECTIVES

The specific objectives of this study are:

- To describe the characteristics that make the Internet of Things difficult to secure.
- To survey the threats at the perception, network, and application layers.
- To set out the security requirements for the Internet of Things.
- To describe the countermeasures and their organisation as defence in depth.
- To discuss the protection of privacy and the emerging approaches.

METHODOLOGY

A review-based approach was adopted. The threats, requirements, and countermeasures of Internet-of-Things security were consolidated from the established and current literature [1]-[10], and the material was organised into a framework comprising the threats by layer, the layered countermeasures of defence in depth, and the secure lifecycle of a device. Where figures present the threats, the defence in depth, or the lifecycle, these are illustrative and schematic, and the technologies and standards named are representative examples of a rapidly evolving field rather than an exhaustive account.

Threats and Defence in Depth

The security threats at the layers of the architecture are represented in Figure 1, showing the threats to the perception, network, and application layers. The layered countermeasures of defence in depth are represented in Figure 2, showing the protection of the device, the

Page 45-55 © MANTECH PUBLICATIONS 2026. All Rights Reserved

communication, and the network and cloud as concentric layers. These representations organise the threats and countermeasures as set out in the literature [1], [6].

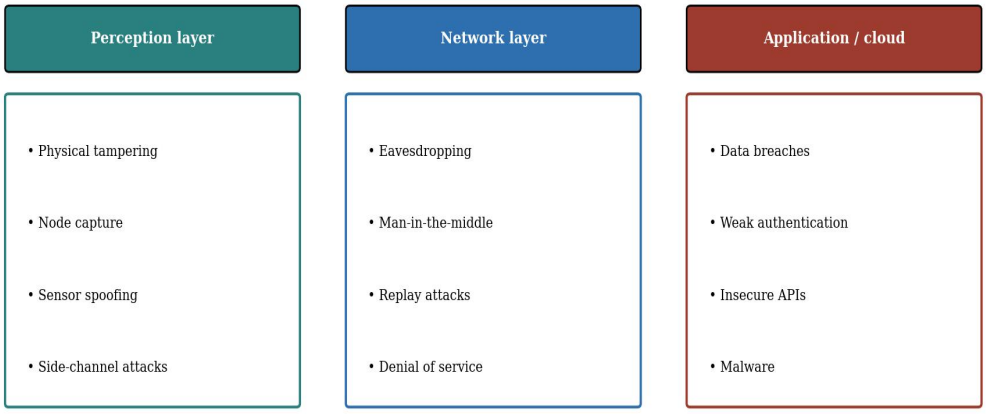


Figure 1: Security threats across the IoT architecture.

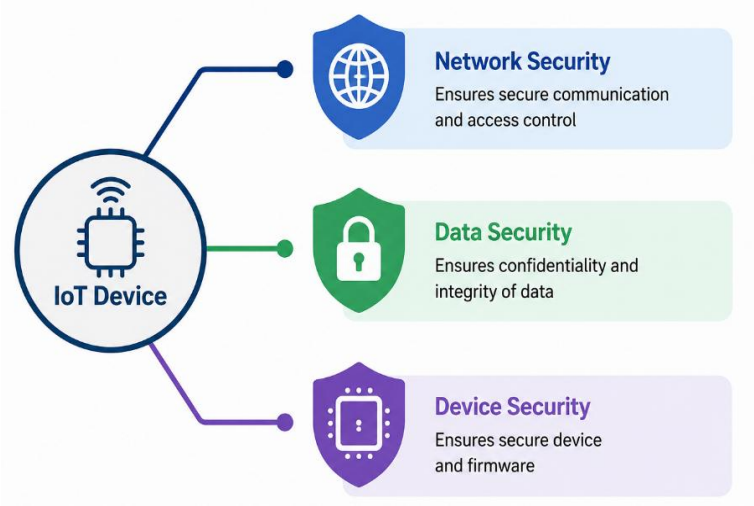
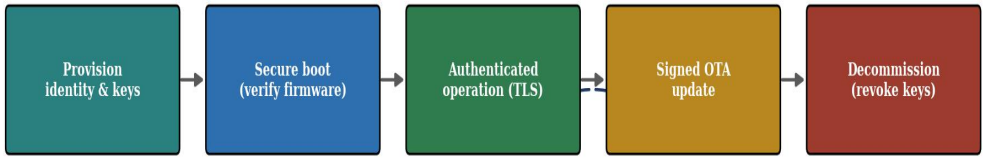


Figure 2: Defence in depth for IoT security.

Secure Lifecycle

The secure lifecycle of a device is represented in Figure 3, showing the provisioning of identity and keys, secure boot, authenticated operation, signed over-the-air updates, and decommissioning. This representation conveys the securing of a device throughout its life, from manufacture to retirement [7].



Page 45-55 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Figure 3: Secure device lifecycle

RESULTS AND FINDINGS

Threats

Table 1 sets out the threats by layer and their countermeasures, and Figure 1 depicts them. The findings show that the threats differ by layer, physical tampering and capture at the perception layer, eavesdropping, interception, and denial of service at the network layer, and data breaches and weak authentication at the application layer, and that each requires appropriate countermeasures. The finding is that the varied threats reflect the varied exposure of the layers, the physical exposure of devices, the exposure of communication, and the exposure of data and interfaces, so that security must address every layer, and that the assembling of compromised devices into networks for attack makes the security of even individual devices a matter of wider concern [1], [2], [5].

Table 1: Threats by layer and countermeasures.

Layer	Example threats	Countermeasure
Perception	Tampering, node capture, spoofing	Secure element, tamper resistance
Network	Eavesdropping, MITM, replay, DoS	TLS/DTLS, authentication, filtering
Application / cloud	Data breach, weak auth, insecure APIs	Access control, strong auth, hardening

Requirements

Table 2 sets out the security requirements, and Figure 2 depicts the layered protection that addresses them. The findings show that the requirements are the classical goals of confidentiality, integrity, and availability, together with authentication, authorization, and privacy, applied to the Internet of Things. The finding is that these requirements must all be met for a system to be secure, and that they interact, since, for example, availability may be threatened by denial of service even where confidentiality and integrity are protected, so that security is not a single property but a set of properties that must be assured together, and the countermeasures are chosen to address them collectively [4], [6].

Page 45-55 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Table 2: Security requirements for the IoT

Requirement	Meaning
Confidentiality	Data are disclosed only to authorised parties
Integrity	Data are not altered without detection
Availability	Services remain accessible when needed
Authentication	The identity of devices and users is verified
Authorization / privacy	Actions are permitted; personal data are protected

Countermeasures

Table 3 sets out the countermeasures, and Figures 2 and 3 depict defence in depth and the secure lifecycle. The findings show that the countermeasures include lightweight cryptography for constrained devices, secure communication, device identity, secure boot and signed updates, access control and segmentation, and intrusion detection, and that they are deployed in layers throughout the life of a device. The finding is that securing the Internet of Things requires the combination of these countermeasures as defence in depth, adapted to the constraints of devices, so that the compromise of one layer does not compromise the whole, and that the securing of a device over its lifetime, through provisioning, secure boot, authenticated operation, and signed updates, is as important as the protection of the network in which it operates [6], [7].

Table 3: Countermeasures for IoT security.

Countermeasure	Purpose
Lightweight cryptography	Confidentiality and integrity on constrained devices
TLS / DTLS	Secure communication over the network
Device identity (keys, certificates)	Authentication and trust
Secure boot and signed OTA updates	Integrity of firmware over the lifetime

Page 45-55 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Countermeasure	Purpose
Access control; intrusion detection	Limit and detect unauthorised activity

DISCUSSION

The principal point of this review is that securing the Internet of Things requires layered countermeasures, adapted to the constraints of its devices and addressing the threats at every layer, and that no single measure suffices. The threats are varied, arising from the physical exposure of devices, the exposure of communication, and the exposure of data and interfaces, and the requirements, of confidentiality, integrity, availability, authentication, authorization, and privacy, must all be met. The countermeasures, deployed as defence in depth, are the means by which these requirements are assured against these threats, so that the failure of one layer does not compromise the system [1], [6].

The constraints of the Internet of Things shape its security in a way that distinguishes it from conventional computing. The limited processing, memory, and energy of devices restrict the cryptography they can perform, motivating lightweight cryptography and the use of secure hardware; their physical accessibility motivates tamper resistance and the protection of keys; and their scale and long, poorly updatable lifetimes motivate secure provisioning and the delivery of authenticated updates over the air. The securing of a device over its whole lifetime, from the provisioning of identity through secure operation to decommissioning, is therefore a central concern, and the difficulty of updating fielded devices is one of the field's most serious weaknesses. Security must be designed in from the start, not added later [3], [7].

The protection of privacy and the emerging approaches to security are increasingly important. The Internet of Things collects large quantities of personal and behavioural data, and its privacy depends on the minimisation, anonymisation, and careful handling of that data, assisted by processing at the edge; and the emerging approaches, including secure hardware, machine-learning-based intrusion detection, distributed trust, and zero-trust architectures, together with standards for device security, are strengthening the field. These developments respond to the recognised weaknesses of the Internet of Things and to the growing consequences of its insecurity. Presented together, the threats, the defence in depth, and the secure lifecycle convey the security of the Internet of Things as a connected whole. Specific

Page 45-55 © MANTECH PUBLICATIONS 2026. All Rights Reserved

technologies and standards are representative of an evolving field, and certain figures are illustrative and convey structure rather than exact configurations.

LIMITATIONS

This study is a review of a rapidly evolving field and presents the threats, requirements, and countermeasures of Internet-of-Things security in summary form; the technologies and standards named are representative examples rather than an exhaustive or final account, and the field will continue to change. The review addresses the subject at a high level and does not provide detailed technical, cryptographic, or threat analysis or measured data. The threats, defence in depth, and lifecycle shown in the figures are illustrative and schematic rather than exact configurations. Readers requiring authoritative and current detail are referred to the primary literature and to the relevant security standards and guidance.

FUTURE SCOPE

Further study building on this account can proceed in several directions:

- Development of lightweight cryptography and secure hardware for constrained devices.
- Advancement of machine-learning-based intrusion detection for IoT networks.
- Improvement of secure provisioning, device identity, and over-the-air updates.
- Study of privacy-preserving data handling and edge processing.
- Investigation of zero-trust architectures and decentralised trust for the IoT.
- Adoption and evaluation of security standards for consumer and industrial devices.

Pursuing these directions would strengthen the security and privacy of the Internet of Things.

CONCLUSION

This paper has reviewed the security and privacy of the Internet of Things. It describes the characteristics, constraint, physical accessibility, heterogeneity, scale, and poor updatability, that make it difficult to secure; the threats at the perception, network, and application layers, from tampering and capture through eavesdropping and denial of service to data breaches; the security requirements of confidentiality, integrity, availability, authentication, authorization, and privacy; and the countermeasures, lightweight cryptography, secure communication, device identity, secure boot and signed updates, access control, and intrusion detection, deployed as defence in depth and throughout the lifetime of a device. The central conclusion is that securing the Internet of Things requires layered countermeasures adapted to the

Page 45-55 © MANTECH PUBLICATIONS 2026. All Rights Reserved

constraints of devices, that security must be designed in from the start, and that it is limited by resource constraints, the difficulty of updates, and fragmentation, which the emerging approaches and standards seek to address. Specific technologies and standards are representative of an evolving field, and certain figures presented are illustrative.

REFERENCES

1. J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 2015.
2. M. Antonakakis *et al.*, "Understanding the Mirai botnet," in *Proc. USENIX Security Symp.*, 2017, pp. 1093–1110.
3. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *Proc. IEEE ISCC*, 2015, pp. 180–187.
4. K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Netw.*, vol. 32, pp. 17–31, 2015.
5. C. Kolias *et al.*, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.
6. S. Sicari *et al.*, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, 2015.
7. N. Asokan *et al.*, "ASSURED: Architecture for secure software update of realistic embedded devices," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 11, pp. 2290–2300, 2018.
8. C. Perera *et al.*, "Big data privacy in the Internet of Things era," *IT Prof.*, vol. 17, no. 3, pp. 32–39, 2015.
9. Dorri *et al.*, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE PerCom Workshops*, 2017, pp. 618–623.
10. ETSI, *EN 303 645: Cyber Security for Consumer Internet of Things: Baseline Requirements*. Sophia Antipolis, France: ETSI, 2020.
11. Al-Fuqaha *et al.*, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 2015.
12. E. Bertino and N. Islam, "Botnets and Internet of Things security," *Computer*, vol. 50, no. 2, pp. 76–79, 2017.
13. D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: A top-down survey," *Comput. Netw.*, vol. 141, pp. 199–221, 2018.

Page 45-55 © MANTECH PUBLICATIONS 2026. All Rights Reserved

14. M. A. Al-Garadi *et al.*, "A survey of machine and deep learning methods for Internet of Things security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 2020.
15. National Institute of Standards and Technology, *NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers*. Gaithersburg, MD, USA: NIST, 2020.
16. Bogdanov *et al.*, "PRESENT: An ultra-lightweight block cipher," in *Proc. CHES*, 2007, pp. 450–466.
17. Z. Shelby, K. Hartke, and C. Bormann, *The Constrained Application Protocol (CoAP), RFC 7252*. IETF, 2014.
18. R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, 2013.

***Author for Correspondence**
Dr. Karthik Subramanian
E-mail: karthik.subramanian2@gmail.com

[1]Professor, Department of Computer Science and Engineering, College of Engineering, Guindy, Anna University, Chennai
[2]Associate Professor, Department of Information Science and Technology, College of Engineering, Guindy, Anna University, Chennai
[3]Associate Professor, Department of Electronics and Communication Engineering, College of Engineering, Guindy, Anna University, Chennai
[4]Assistant Professor, Department of Computer Applications, Anna University, Chennai

Received Date: May 05, 2026
Accepted Date: May 20, 2026
Published Date: June 30, 2026

Citation: Dr. Karthik Subramanian, Dr. Lavanya Venkatesh, Dr. Prakash Raman, Dr. Divya Anand. Security and Privacy in the Internet of Things: Threats, Requirements, and Countermeasures. International Journal of Programming Languages and Internet of Things. 2026; 2(1): 45-55p.