



UDK: 004.78:004.35
004.056.5
COBISS.SR-ID 148819465
DOI: 10.5281/zenodo.12593683
Review paper

SECURITY CHALLENGES OF INTERNET OF THINGS

Petar Čisar⁴; Sanja Maravić Čisar⁵

Abstract

The Internet of Things (IoT) is a concept of interconnecting physical devices, smart devices, and other devices with embedded electronic components, software, sensors, actuators, and network connectivity, enabling them to collect and exchange data. Devices must be always protected, from manufacturing to use in operational environments. This involves implementing a variety of measures such as secure booting, access control, firewall, device authentication, unauthorised access prevention systems, and regular software updates and corrections. Security in IoT solutions should not be viewed as one of the functional add-ons but as a crucial and indispensable part essential for the reliable operation of IoT devices. This paper focusses on the IoT environment and its unique security challenges, emphasising the need to implement strategies that enable overcoming these challenges.

Key words: Internet of Things, security, vulnerability, security recommendations, threat mitigation

Introduction

The Internet of Things (IoT) is a network of interconnected devices that spans various domains, such as automotive, residential, and urban infrastructure. IoT Analytics projects a global proliferation of connected devices that will reach 27 billion by 2025, driven by a compound annual growth rate (CAGR) of 22% [1], as shown in Figure 1.

This rapid expansion of IoT applications, from smart homes and autonomous vehicles to environmental monitoring and data analytics, highlights its transformative impact on daily life and business operations [2]. However, this growth also amplifies the need for robust security measures to counter evolving cyber threats. The evolving IoT landscape poses specific security challenges that require proactive mitigation strategies. Regulatory frameworks are adapting to address these risks, placing increasing pressure on organizations to

⁴ Petar Čisar, 1965, PhD, full professor, University of Criminalistic Investigation and Police Studies, Cara Dušana 196, 11080 Belgrade, Serbia, +381113107100, petar.cisar@kpu.edu.rs <https://orcid.org/0000-0002-8129-288X>

⁵ Sanja Maravić Čisar, 1970, PhD, college professor, Subotica Tech – College of Applied Sciences, Marka Oreškovića 16, 24000 Subotica, Serbia, +38124655201, sanjam@vts.su.ac.rs <https://orcid.org/0000-0001-8131-9141>



follow strict security standards. Furthermore, the complex nature of IoT ecosystems, characterised by diverse device types and complex development environments, demands specialised security solutions beyond traditional measures [3].

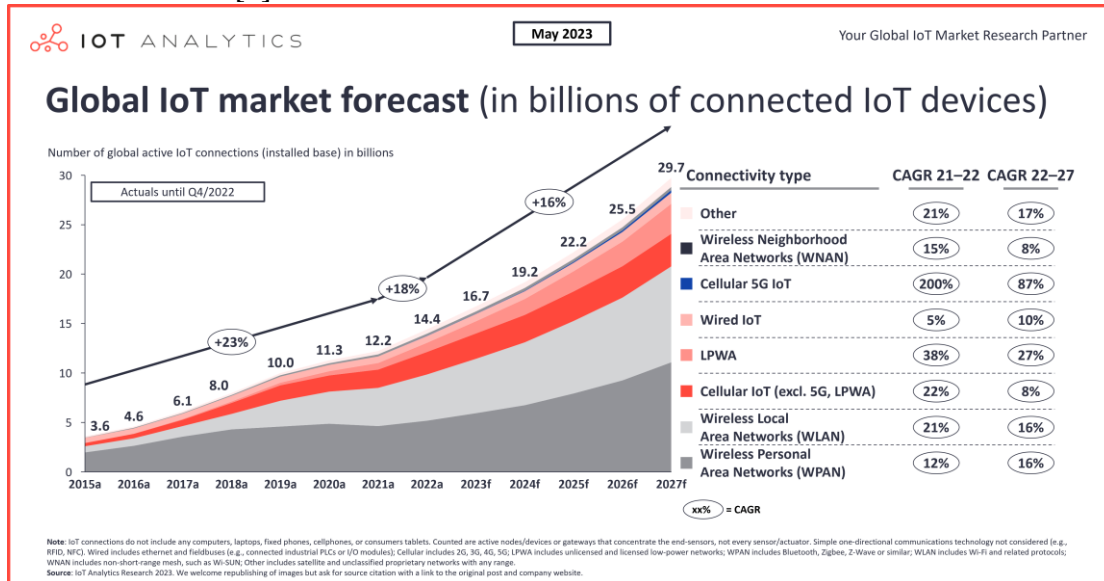


Figure 1: Global IoT market forecast [1]

Addressing these security challenges is essential to unlock the full potential of IoT while ensuring resilience against emerging threats. By implementing tailored security protocols and leveraging innovative technologies, stakeholders can effectively navigate the complexities of IoT security and mitigate associated risks.

The security landscape of the IoT includes the protection of connected devices and networks on which they depend against online threats and breaches. This involves a comprehensive approach to identifying, monitoring, and addressing potential security vulnerabilities across the IoT device spectrum. Basically, IoT security involves the practices adopted to ensure the security of IoT systems [4].

The extensive network of interconnected “things” within the IoT ecosystem possesses a wealth of user data, making it a prime target for cybercrime activities such as data theft and hacking. With the spread of connected devices, the area for potential security breaches is expanding, and cybercriminals are exposed to numerous opportunities for exploitation.

The consequences of IoT security breaches can be significant, impacting both digital and physical domains. Consider, for example, a smart car connected to the internet: cybercriminals could exploit vulnerabilities to manipulate critical safety features, posing significant risks to vehicle passengers [5]. Furthermore, as the Industrial Internet of Things (IIoT) becomes more widespread across various industries, cyberattacks can lead to cascading consequences with far-reaching impacts.

Similarly, in the sphere of healthcare, where the Internet of Medical Things (IoMT) is prevalent, compromised devices pose threats to patient privacy and safety, potentially compromising sensitive medical data or even endangering patient well-being [6]. Within smart homes, compromised IoT devices could allow unauthorised access, allowing intruders to monitor residents' activities and compromise their security and privacy [7].



In recent years, there have been notable cases in which cybercriminals have compromised IoT devices. In 2016, a botnet named Mirai enlisted hundreds of thousands of compromised connected devices. Botnets are networks of computers infected with malware that execute automated tasks on the Internet without the owners' consent. This attack led to temporary shutdowns of major services and websites like Spotify, Netflix, and PayPal [8].

The VPN Filter malware infected more than half a million routers in more than 50 countries in 2018. This malware could install additional malicious software on devices connected to infected routers, allowing cybercriminals to collect data, block network traffic, and steal passwords [9].

A cybersecurity expert demonstrated hacking a Tesla Model X in under two minutes by exploiting a Bluetooth vulnerability. Similar wireless key-dependent car models have also faced comparable attacks [10].

In 2021, Swiss hackers compromised approximately 150,000 live camera feeds manufactured by Verkada, a security camera company. These hacked feeds included cameras monitoring public sector buildings like schools, hospitals, prisons, as well as those in private corporate organizations [11].

Security Challenges of IoT

Key security challenges associated with IoT technologies include confidentiality, integrity, privacy, availability, authenticity, non-repudiation, and key management, as shown in Figure 2 [12].



Figure 2: Security challenges of IoT [12]

Confidentiality, Integrity, Availability, Authenticity, and Non-repudiation (often abbreviated as “CIA” or “CIAAN”) are fundamental security properties essential for safeguarding the reliability of information systems. They collectively underpin information security, ensuring safe handling of sensitive data [13].



1. **Confidentiality:** Protecting sensitive data from unauthorised disclosure is vital. This includes securing data at rest, in transit, and in use using encryption, access controls, and data masking.
2. **Integrity:** Ensuring that the data remain unaltered or tampered with is crucial. This involves protecting data from unauthorised modification, deletion, or addition using digital signatures, message authentication codes, and data hashing.
3. **Availability:** Ensuring information and systems are accessible to authorized users when needed is paramount. This includes defending against denial-of-service attacks and ensuring high system availability through techniques such as load balancing, redundancy, and disaster recovery planning.
4. **Authenticity:** Verifying that information and communication originate from a trusted source is essential. This involves protecting against impersonation and identity fraud using authentication, digital certificates, and biometric identification.
5. **Non-repudiation:** Preventing a party from denying its participation in a message or transaction is crucial. This includes protecting against message tampering and replay attacks using digital signatures, message authentication codes, and timestamps.

These five properties collectively form the foundation of information security and ensure the confidentiality, integrity, and availability of sensitive information [12].

Despite their undeniable advantages, IoT technologies have several weaknesses [14]:

1. **Remote exposure:** IoT devices, due to their connectivity supported by the internet, have a large attack surface, making them vulnerable to remote interactions by hackers. This accessibility, while valuable, also increases the risk of hacking campaigns such as phishing. IoT security, including cloud security, must address numerous entry points to protect assets.
2. **Lack of industry foresight:** Certain industries, such as automotive and healthcare, have expanded their use of IoT devices to improve productivity and cost-efficiency. However, this digital transformation has led to increased technological dependence, particularly on inherently vulnerable IoT devices. Many organizations in these industries were unprepared to invest sufficient resources in securing these devices, exposing them to heightened cybersecurity threats.
3. **Resource constraints:** Some IoT devices lack the computing power to integrate advanced security measures, such as firewalls or antivirus software. This limitation, exemplified by devices that use Bluetooth technology, contributes to an increased risk of data breach, particularly in sectors such as automotive.
4. **Weak default passwords:** IoT devices often come with weak default passwords, and consumers may not realise the importance of replacing them with stronger alternatives. Failure to change default passwords leaves devices susceptible to brute-force and other hacking attacks.
5. **Multiple connected devices:** Many households now have multiple interconnected IoT devices. While convenient, this interconnection means that a security misconfiguration in one device can affect the entire network, leading to widespread disruptions.
6. **Lack of encryption:** The majority of network traffic originating from IoT devices is unencrypted, heightening the risk of security threats and data breaches. Ensuring that all devices are properly secure and encrypted can mitigate these threats.

These weaknesses highlight the importance of addressing security concerns in IoT technologies to ensure their safe and effective integration into various industries and everyday life.



IoT Vulnerabilities

A vulnerability refers to a weakness within an IT system that attackers can exploit to carry out a successful attack. Vulnerabilities can arise from flaws, features, or user errors, and attackers often exploit one or more of these weaknesses to achieve their objectives [15].

The 2020 Unit 42 IoT Threat Report provides a comprehensive analysis of the current state of the IoT threat landscape. Conducted by Unit 42 threat intelligence and IoT security experts, the study examines security incidents that span 2018 and 2019 on 1.2 million IoT devices in the United States. The report focusses on several key areas [16]:

- An examination of the current IoT threat landscape, highlighting emerging trends and prevalent vulnerabilities.
- Identification of the IoT devices most vulnerable to compromise, along with an analysis of the underlying factors contributing to their susceptibility.
- Practical recommendations aimed at reducing IoT-related risks in the environment, offering actionable steps to improve security and mitigate potential threats.

During this research, several emerging trends have been identified that organisations should observe [16]:

- **Unencrypted IoT device traffic:** A surprising 98% of all IoT device traffic remains unencrypted, thus exposing personal and confidential data on the network. This vulnerability grants attackers the ability to intercept unencrypted network traffic, leading to the collection of sensitive information. Subsequently, attackers exploit these data to make a profit on the dark web.
- **Threats in healthcare organizations:** Approximately 51% of threats targeting healthcare organisations are directed towards imaging devices. These threats not only disrupt quality of care but also facilitate the exfiltration of patient data stored on these devices, posing significant privacy and security risks.
- **Integration of IoT and IT assets in healthcare VLANs:** Alarmingly, 72% of healthcare Virtual Local Area Networks (VLANs) merge IoT and IT assets. This integration enables malware to spread seamlessly from users' computers to vulnerable IoT devices on the same network, increasing the risk of cyberattacks and data breaches.

As threats evolve, IoT devices are increasingly targeted using sophisticated techniques such as peer-to-peer command and control communications and worm-like features for self-propagation (Figure 3). With weak device and network security postures, attackers find ample opportunities to compromise IoT systems [16]:

- **Vulnerability of IoT devices:** A significant 57% of IoT devices are susceptible to medium- or high-severity attacks, making them attractive targets for attackers seeking low-hanging fruit.
- **Exploitation of device vulnerabilities:** Alarmingly, 41% of attacks exploit vulnerabilities in devices, as attackers scan through network-connected devices to exploit known weaknesses.
- **Role of IoT devices in cyberattacks:** Although IoT devices are easy targets due to their vulnerabilities, they are often used as stepping stones for lateral movement to attack other systems



on the network. Password-related attacks remain prevalent due to weak manufacturer-set passwords and poor password security practices.

- **Evolution of attack strategies:** There is a noticeable shift in attackers' motivations, moving away from running botnets for DDoS attacks via IoT devices. Instead, malware is spreading across networks via worm-like features, enabling attackers to execute various new attacks by running malicious code.

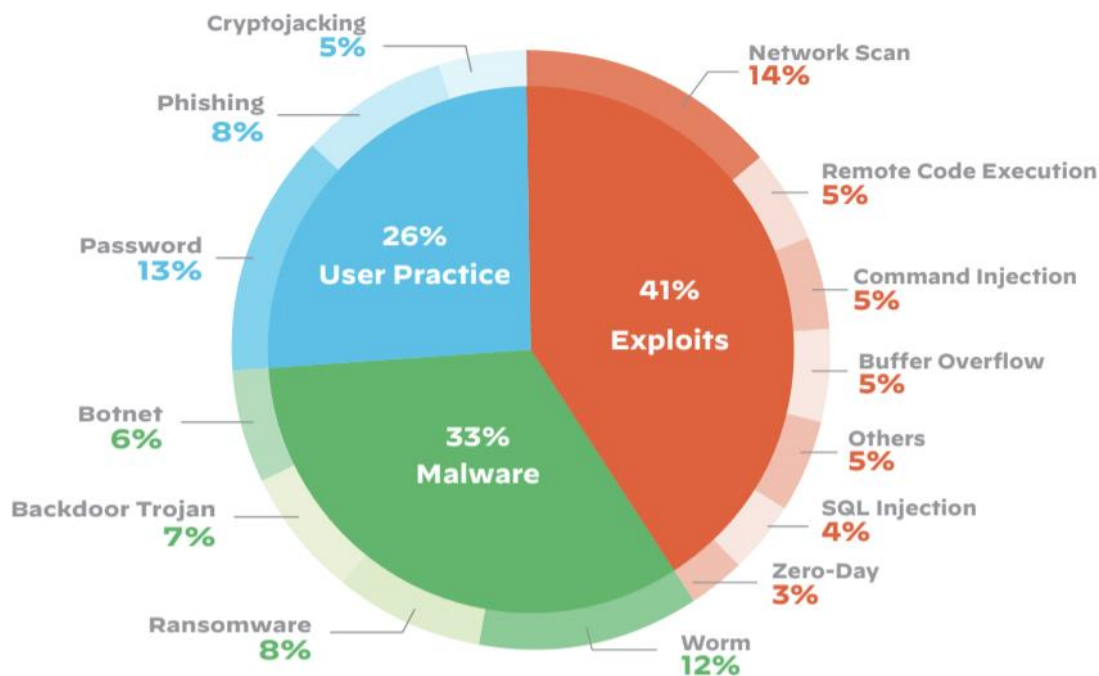


Figure 3: Top IoT threats [16]

Strategies for Securing IoT Devices

The Open Web Application Security Project, or OWASP, is an international non-profit organisation dedicated to security. The OWASP Internet of Things Top 10 is a project intended to help those who deal with creating network/Internet devices. The project analyses the ten main security flaws that are seen with IoT gadgets, and how to avoid them [17].

1. **Weak or hard-coded passwords:** IoT devices often feature web-based interfaces for configuration and management, along with authentication mechanisms like serial consoles and network services. Inappropriate configuration of these interfaces can grant unauthorised access, enabling them to compromise sensitive information and alter device configurations.

Mitigation: Manufacturers should implement robust authentication and password management controls to ensure secure and non-guessable passwords. In addition, users should be encouraged to replace default passwords with strong and unique ones during device setup.



2. **Insecure network services:** Vulnerabilities in network protocols, services, or configurations, including unencrypted communication protocols and outdated software, pose risks for IoT devices. Attackers exploit these weaknesses to steal data, launch attacks, or gain unauthorized access.
Mitigation: Employing secure network protocols like Transport Layer Security (TLS) and regular updates to network services can mitigate vulnerabilities. Periodic network vulnerability assessments and red team exercises are also recommended.
3. **Insecure ecosystem interfaces:** Insecure interfaces between components of the IoT ecosystem, such as cloud services and other devices, create vulnerabilities. Poorly secured interfaces enable attackers to access sensitive data, launch attacks, or manipulate devices.
Mitigation: Regular patching of APIs, strict access controls, secure communication channels, and encryption help mitigate this vulnerability.
4. **Lack of secure update mechanism:** IoT devices often lack secure update mechanisms, leaving them vulnerable to known exploits. Outdated firmware or software can be exploited by attackers, leading to compromised security and potential consequences like financial loss or data breaches.
Mitigation: Implementing features like digital signatures, anti-rollback mechanisms, secure delivery, and firmware validation addresses this vulnerability.
5. **Use of insecure or outdated components:** Many IoT devices use third-party components that may contain vulnerabilities. Exploitable vulnerabilities, such as outdated libraries, pose security risks.
Mitigation: Regularly updating software and components, along with monitoring for security vulnerabilities, helps mitigate risks.
6. **Insufficient privacy protection:** IoT devices often collect and store sensitive personal data without adequate privacy protection. Data collection without user consent, insecure storage, and unauthorized data sharing are common issues.
Mitigation: Implementing privacy-by-design principles, encryption, and obtaining user consent for data collection mitigate privacy risks.
7. **Insecure data transfer and storage:** IoT devices that transfer or store data without encryption are vulnerable to interception or manipulation. Weak data storage mechanisms and unencrypted communication channels pose security risks.
Mitigation: Using secure protocols like HTTPS, encrypting data, implementing access controls, and auditing data storage practices mitigate risks.
8. **Lack of device management:** Ineffective device management enables remote manipulation of IoT devices, potentially compromising entire networks.
Mitigation: Implementing strong authentication mechanisms, unique device credentials, and access controls limits unauthorized access.
9. **Insecure default settings:** Insecure default settings on IoT devices, including default usernames and passwords, leave devices vulnerable.
Mitigation: Changing default settings and disabling unnecessary services mitigates this vulnerability.
10. **Lack of physical hardening:** Physical security measures, such as disabled debug ports and the use of secure boot mechanisms, protect against hardware attacks and firmware tampering. Sensitive information should not be stored on removable memory cards.



Mitigation: Implementing physical security measures such as tamper detection and secure booting reduces the risk of unauthorised access.

As the popularity of IoT devices increases, addressing these vulnerabilities becomes crucial. Understanding and mitigating these risks, as described by the OWASP IoT Top 10 vulnerabilities, is essential for organisations and individuals to ensure the security of their IoT ecosystems and protect data and privacy.

Conclusions

The Internet of Things enables electronic devices in our environment to actively engage by exchanging information within the network. This capability enables the recognition of events and changes in their surroundings, empowering autonomous actions and reactions with minimal human intervention. The advantages of IoT are vast, transforming our work and lifestyles by conserving time and resources, and creating new avenues for growth, innovation, and knowledge exchange among entities.

However, despite the significant potential benefits, various obstacles and challenges need to be addressed to realize the full potential of the IoT. These challenges include security, privacy, standards, interoperability, legal and regulatory issues, as well as considerations related to emerging economies. The IoT encompasses a complex array of technological, social, and political factors that involve various stakeholders.

Connected devices have revolutionised consumer experiences, but they also offer attractive targets for hackers. The Internet of Things and cybercriminal activity share two important characteristics: they are largely invisible and ubiquitous in our environment. As IoT continues to be implemented and utilised, there is a pressing need to address its security challenges effectively while maximising its benefits and minimizing associated risks.

References

- [1] S. Sinha, "State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally," Available: <https://iot-analytics.com/number-connected-iot-devices/>.
- [2] B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus and Ž. Bojović, Internet of Things, Beograd: Fakultet organizacionih nauka, 2017.
- [3] Kaspersky, "IoT security challenges and potential responses". Available: <https://iotac.eu/iot-security-challenges-and-potential-responses/>.
- [4] E. von Hollen, "The Growing IoT Landscape in Business". Available: <https://www.maintech.com/blog/iot-security-fundamental-practices>.
- [5] A. Giannaros, A. Karras, L. Theodorakopoulos, C. Karras, P. Kranias, N. Schizas, G. Kalogeratos and D. Tsolis, "Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions," Cybersecurity and Privacy, pp. 493-543, 2023.
- [6] R. Hireche, H. Mansouri and A.-S. K. Pathan, "Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis," Cybersecurity and Privacy, pp. 640-661, 2022.
- [7] B. Hammi, S. Zeadally, R. Khatoun and N. Jamel, "Survey on Smart Homes: Vulnerabilities, Risks, and Countermeasures," Computers and Security, vol. 117, 2022.



- [8] E. Bursztein, “Inside the infamous Mirai IoT Botnet: A Retrospective Analysis” Available: <https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis>.
- [9] A. Greenberg, “Stealthy, Destructive Malware Infects Half a Million Routers”. Available: <https://www.wired.com/story/vpnfilter-router-malware-outbreak/>.
- [10] V. Tangermann, “New hack steals a Tesla in minutes via bluetooth”. Available: <https://futurism.com/the-byte/hack-steals-tesla-minutes-bluetooth>.
- [11] K. Randolph and M. Hunt, “Security Incident Report,” Verkada, 2021.
- [12] Y. Khan, M. Bin Mohd Su’ud, M. M. Alam, S. F. Ahmad, N. A. Salim and N. Khan, “Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications,” Electronics, vol. 12, no. 1, 2023.
- [13] A. Kolbach, Confidentiality, Integrity, Availability, Authenticity, and Non-repudiation, 2023.
- [14] K. Yasar, S. Shea and I. Wigmore, “What is IoT security (internet of things security)?,” Available: <https://www.techtarget.com/iotagenda/definition/IoT-security-Internet-of-Things-security>.
- [15] “Understanding vulnerabilities” 2015.
Available: <https://www.ncsc.gov.uk/information/understanding-vulnerabilities>.
- [16] Palo Alto Networks, “2020 Unit 42 IoT Threat Report,” Palo Alto Networks, Santa Clara, 2020.
- [17] OWASP, “The OWASP IoT top 10 vulnerabilities and how to mitigate them”. [Online]. Available: <https://www.sisainfosec.com/blogs/the-owasp-iot-top-10-vulnerabilities-and-how-to-mitigate-them/>.