ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

An Analysis of IoT Device Security and Privacy Concerns

Ronak Italia

USA

ABSTRACT

The paper conducts with the widespread adoption of the Internet of Things (IoT) has revolutionised diverse sectors, including healthcare, smart cities, and manufacturing, enhancing connectivity, efficiency, and decision-making. However, this expansion has also exposed critical security and privacy vulnerabilities. This article delves into these challenges, exploring IoT device vulnerabilities, data protection, and secure communication. With an estimated 25% of IoT applications in smart homes, 20% in healthcare, and 18% in manufacturing, the increasing reliance on IoT underscores the urgency of addressing these issues. Trends such as integrating AI for real-time threat detection, developing encryption techniques, and standardising security protocols are shaping the future of IoT security. This study conducts a detailed review of existing literature to evaluate current solutions and presents a comprehensive framework that combines technical innovations like blockchain and privacy-preserving analytics with regulatory measures. By emphasising secure communication, enhanced authentication, and decentralised architectures, this research aims to provide actionable insights for mitigating risks and fostering a resilient IoT ecosystem. The findings underscore the need for a collaborative and holistic approach to safeguard IoT systems, offering a robust foundation for future research and practical applications.

***Corresponding author**

Ronak Italia, USA.

Received: February 03, 2022; **Accepted:** February 09, 2022, **Published:** February 28, 2022

Keywords: Internet of Things (IoT), IoT Security, Security Frameworks, Network Security, Conceptual Models

Introduction

The Internet of Things (IoT) offers significant benefits by turning everyday objects into smart, adaptive systems. However, these advancements also introduce security and privacy risks. In smart homes, devices like intelligent meters, cameras, and remote-controlled doors can be vulnerable to unauthorized access, potentially compromising personal security and causing harm [1]. As IoT systems grow, the vast data they generate can be exploited by attackers, raising concerns about privacy [2]. Highlight the increasing risks of data breaches, while stress the need for strong security measures. Also emphasize the importance of effective frameworks to address these emerging challenges. Further discuss the challenges and opportunities in securing IoT systems and ensuring privacy [3-5].

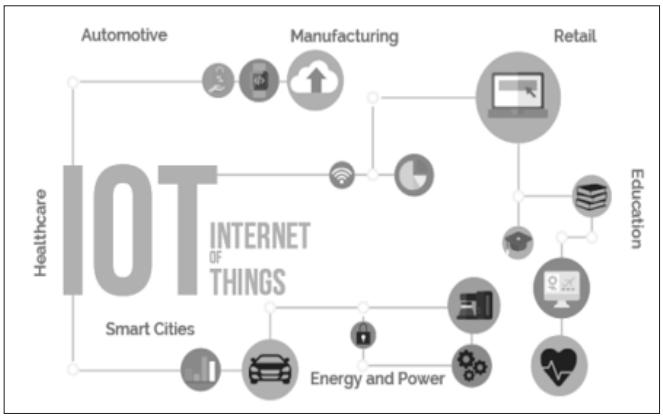


Image: Internet of Things

Similarly, connected vehicles that rely on sensors and wireless controls present a growing risk of cyber-attacks, where hackers could gain control over crucial vehicle systems like braking and steering [6]. In the medical field, IoT devices such as pacemakers and insulin pumps are vulnerable to remote exploitation, posing life-threatening risks [7]. Furthermore, in commercial settings, the security of IoT devices is of utmost importance, as cybercriminals could infiltrate organizations, steal sensitive data, and cause significant financial losses [8]. With IoT devices capable of collecting vast amounts of personal data, the potential for privacy violations is significant, especially as advanced technologies like facial and voice recognition continue to evolve. The aggregation of metadata from these devices could reveal private information, creating an urgent need for robust privacy protection mechanisms [9]. Lastly, the ongoing evolution of IoT technologies underscores the need for comprehensive security, privacy, and trust frameworks to ensure safe and secure deployments [10].

What is IoT and Regular Internet?

Internet of Things (IoT) and the regular Internet are both networks that enable communication between devices, but they serve different purposes and have distinct characteristics. Here's a comparison (refer table 1):

Table 1: Comparison of IoT and Regular Internet

Feature	Regular Internet	Internet of Things (IoT)
Purpose	Human-to-human and human-to-machine munication	Machine-to-machine (M2M) ommunication
Devices	Computers, artphones, tablets, etc.	Everyday objects embedded with sensors & actuators (e.g., smart home devices, wearables)
Communication	Primarily human users interacting with devices	Devices autonomously ommunicating with each other or central systems
Data Flow	Content delivery (websites, apps)	Continuous data collection, analysis, and action
User Interaction	Requires user nvolvement (e.g., browsing, messaging)	Minimal human involvement; devices work autonomously
Applications	Social media, email, web browsing, cloud computing, etc.	Smart homes, wearables, healthcare devices, smart cities
Automation	No direct automation; humans control the devices	Devices can automate actions based on data (e.g., smart thermostats adjusting temperature)
Real-Time Action	Primarily passive interaction (e.g., watching videos, browsing)	Real-time decisions based on sensor data (e.g., smart devices reacting to movement)
Security Focus	Focused on protecting data, users, and networks	Focused on securing devices, data transmission, and privacy
Examples	Browsing the web, streaming videos, sending emails	Smart thermostats, connected vehicles, health monitors, smart cities

Technologies of IoT

The technologies of IoT have evolved significantly in recent years, driven by the need for smarter, more efficient systems. Below is an overview of the latest trends and technologies shaping the IoT landscape:

Edge Computing

Edge computing processes data locally on IoT devices or nearby nodes, reducing the need to send sensitive data to centralized cloud servers and enhancing privacy [11]. However, it also introduces security challenges for local networks and devices [12]. Connected vehicles, medical IoT devices, and commercial systems are increasingly vulnerable to cyber-attacks, with risks ranging from control of critical systems to data theft. The vast amount of personal data collected by IoT devices also raises privacy concerns, especially as technologies like facial and voice recognition evolve, highlighting the need for strong privacy protections.

5G Technology

The deployment of 5G technology brings higher bandwidth, lower latency, and supports a massive number of IoT devices. This enables real-time data transmission, critical for applications like autonomous vehicles and smart cities. However, 5G also presents new security risks due to increased connectivity and new attack surfaces. Note that while 5G can enhance IoT efficiency, securing the network and devices across such a vast ecosystem is essential to prevent vulnerabilities [13].

AI and Machine Learning (AI/ML)

AI/ML techniques are being used to improve IoT security through real-time threat detection and anomaly monitoring. Explain that AI can help identify potential security breaches by analysing large datasets [14]. However, AI systems themselves pose privacy concerns, as they may inadvertently expose sensitive data or introduce bias. Ensuring the privacy and fairness of AI-driven IoT systems is crucial for user trust and data protection.

Table 2: More IoT Technology

Technology	Key Benefits
Blockchain Technology	- Ensures data integrity and security - Transparent, verifiable transactions - Builds trust among devices
Low Power Wide Area Networks (LPWAN)	- Low energy for long battery life - Long-range communication - Ideal for remote IoT apps
Smart Sensors	- Real-time data collection - Enables smart automation - Supports diverse IoT applications
Cloud Computing	- Scalable, cost-effective - Remote access to data - Supports big data analytics
Cybersecurity Innovations	- Protects against cyber threats - Real-time attack detection - Ensures data confidentiality and integrity
AR/VR	- Immersive experiences - Enhances remote diagnostics - Improves training and education
Wearable IoT Devices	- Continuous health monitoring - Personalized healthcare - Enables remote patient monitoring

IoT Application Across Industries

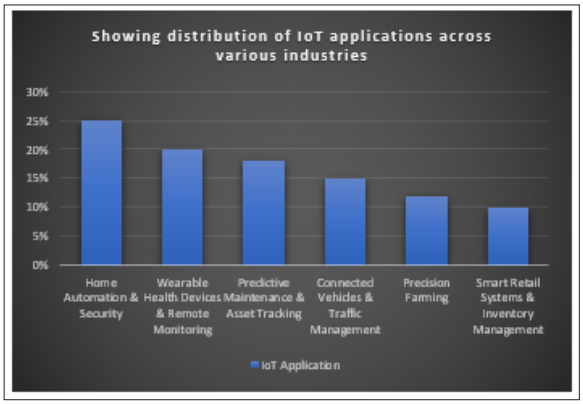
The Internet of Things (IoT) is transforming industries by enabling devices to collect, share, and analyse data, improving efficiency and capabilities. In smart homes, IoT enhances convenience and energy efficiency by controlling appliances, lighting, heating, and

security systems [15]. In healthcare, IoT devices like wearables and remote monitoring improve patient care and reduce costs [16]. IoT also optimizes manufacturing and supply chain management through predictive maintenance and real-time tracking [17]. In transportation, IoT supports connected vehicles, traffic management, and autonomous driving [18]. Agriculture benefits from precision farming using IoT sensors to monitor soil, crop health, and irrigation. However, the widespread use of IoT raises security and privacy concerns, requiring robust data protection measures and secure communication protocols [19,20].

Table 3: Estimated Distribution of IoT Applications Across Various Industries

Industry	IoT Application	Estimated Market Share (%)
Smart Homes	Home Automation & Security	25%
Healthcare	Wearable Health Devices & Remote Monitoring	20%
Manufacturing	Predictive Maintenance & Asset Tracking	18%
Transportation	Connected Vehicles & Traffic Management	15%
Agriculture	Precision Farming	12%
Retail & Commerce	Smart Retail Systems & Inventory Management	10%

Graph 1: Showing Distribution of IoT Applications Across Various Industries



IoT applications are transforming various industries, with smart homes (25%) leading the way through automation, energy management, and security systems like smart thermostats and cameras. In healthcare (20%), IoT is revolutionizing care with wearables, telemedicine, and remote monitoring, fuelled by the shift toward personalized health management. Manufacturing (18%) leverages IoT for predictive maintenance, asset tracking, and supply chain optimization, driving operational efficiency. The transportation sector (15%) applies IoT in connected vehicles, traffic management, and logistics, particularly with the rise of autonomous vehicles. In agriculture (12%), IoT enhances precision farming, irrigation, and crop health monitoring, supporting sustainable food production. Lastly, retail and commerce (10%) benefits from IoT through smart inventory management, optimized supply chains, and improved customer experiences.

Trends in IOT

The Internet of Things (IoT) has rapidly evolved, with growing applications across industries, but it faces significant security challenges. One of the major trends in IoT security is the increasing focus on securing communication between devices. Emphasize the need for enhanced encryption and authentication mechanisms to prevent unauthorized access to sensitive data [21]. As IoT systems expand, there is a growing demand for solutions to address device vulnerabilities, particularly with the rise in connected devices in sectors like healthcare, manufacturing, and smart homes [22]. Furthermore, the trend is shifting toward integrating AI and machine learning to detect and respond to security threats in real-time, as IoT systems become more autonomous and decentralized [23]. Privacy protection remains a central concern as IoT devices generate massive amounts of personal data, with efforts focused on using advanced encryption techniques and user consent protocols to mitigate privacy risks [24]. Finally, there is a significant push toward standardization in IoT security protocols to ensure interoperability and reduce risks across different devices and platforms [25,26]. These trends indicate that as IoT adoption grows, addressing security and privacy through more robust, intelligent, and standardized solutions is crucial for its long-term success.

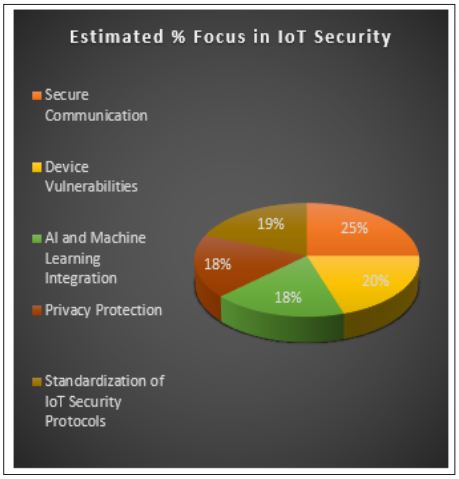
Table 4: Trends in IoT

Trends	Description
Secure Communication	Focus on enhancing encryption and authentication mechanisms to secure communication between IoT devices and prevent unauthorized access.
Device Vulnerabilities	Addressing vulnerabilities in connected devices, especially in sectors like healthcare, manufacturing, and smart homes.
AI and Machine Learning Integration	Using AI and machine learning for real-time threat detection and response to enhance security in IoT systems.
Privacy Protection	Implementing advanced encryption techniques, user consent protocols, and data anonymization to protect user privacy in IoT systems.
Standardization of IoT Security Protocols	Developing and enforcing standardized IoT security protocols to ensure interoperability and reduce security risks across devices and platforms.

Table 5: Trends in IoT Security with Percentage Estimations Based on the Literature Provided

Trend	Estimated % Focus in IoT Security
Secure Communication	25%
Device Vulnerabilities	20%
AI and Machine Learning Integration	18%
Privacy Protection	18%
Standardization of IoT Security Protocols	19%

Graph 2: Trends in IoT Security with Percentage Estimations Based on the Literature Provided



In the realm of IoT security, the highest emphasis (25%) is placed on secure communication, ensuring that data exchanged between IoT devices is properly encrypted and protected to prevent unauthorized access, highlighting its critical importance. Following closely, device vulnerabilities account for 20% of the focus, as significant research and attention are dedicated to addressing security weaknesses in IoT devices, which are prime targets for cyberattacks. AI and machine learning integration contributes 18% to IoT security trends, with real-time threat detection capabilities rapidly evolving, though it remains a developing area. Similarly, privacy protection also receives 18% of the focus, reflecting the growing concern about safeguarding personal data generated by IoT devices. Finally, standardization is crucial to IoT's long-term success, with 19% of efforts directed at developing standardized security protocols to ensure interoperability across devices, although it is regarded more as an overarching framework than a specific technical solution.

IOT Security and Privacy Concern

IOT security and privacy concern is given below:

IoT Security Concerns

IoT security concerns primarily focus on protecting devices, networks, and data from unauthorized access, cyber-attacks, and vulnerabilities due to their interconnected nature.

IoT Device Vulnerabilities: IoT devices are often vulnerable to cyber-attacks due to their reliance on wireless communication. Effective encryption, authentication, and anomaly detection are necessary to secure sensitive data and prevent unauthorized access [27].

Blockchain for IoT Security: Blockchain technology offers a solution to secure communication and ensure the integrity of data exchanged across IoT networks. This decentralized approach can help mitigate security risks in IoT environments [28].

Cryptographic Solutions: Cryptography, such as homomorphic encryption, is essential for ensuring the authentication and integrity of data within IoT networks, protecting sensitive information even during processing [29].

Table 6: Comparison Between IoT Securities

Security Solution	Features	Benefits	Challenges
IoT Device Vulnerabilities	- Wireless ommunication reliance - Need for encryption, authentication, and anomaly detection - Vulnerable to cyber-attacks	- Secures sensitive data - Prevents unauthorized access - Improves overall device security	- High attack surface - Limited resources on IoT devices - Difficulty in implementing robust security
Blockchain for IoT Security	- Decentralized ledger - Tamper-proof data storage - Peer-to-peer network structure	- Data integrity - Secure and transparent ommunication - Increased trust between devices	- High energy consumption for consensus algorithms - Scalability concerns - Complex mplementation
Cryptographic Solutions	- Homomorphic encryption - Data encryption during ommunication and processing - Authentication mechanisms	- Protects data even during processing - Ensures data integrity - Prevents unauthorized access	- Computational overhead - Complex mplementation in low-power devices - Key management

IoT Privacy Concerns

IoT privacy concerns revolve around the collection, storage, and sharing of vast amounts of personal data, raising issues of user consent, data protection, and unauthorized access.

Privacy Risks with Data Collection: IoT devices continuously collect vast amounts of personal data. Strong privacy protocols and trust models are necessary to ensure user data is protected and that interactions remain secure [30].

Data Sovereignty and Control: With data stored in the cloud, users must retain control over their personal data, ensuring compliance with privacy regulations and protecting against unauthorized access [31].

Differential Privacy for Data Protection: Differential privacy methods can help collect and analyse data without compromising individual privacy, allowing for secure data sharing while maintaining anonymity [32].

Remedies of the Problem

Here are some remedies for IoT security and privacy concerns based on the provided references:

Enhanced Authentication Mechanisms: Implementing stronger authentication methods, such as multi-factor authentication (MFA), biometric authentication, and token-based systems, can prevent unauthorized access to IoT devices and networks [33].

Encryption and Secure Communication: Employing end-to-end encryption for data transmitted between IoT devices ensures that sensitive information is protected from unauthorized interception or tampering. Additionally, using secure communication protocols (e.g., TLS, SSL) can enhance security [34].

Regular Software Updates and Patch Management: Continuous monitoring and timely updates to IoT devices' firmware and software are critical to fixing security vulnerabilities. Automating

this process can reduce the risk of attacks due to outdated systems [35].

Data Minimization and Anonymization: Minimizing the amount of personal data collected by IoT devices, along with implementing anonymization and pseudonymization techniques, can reduce the potential for privacy breaches. Chatzikokolakis et al [36].

Distributed and Decentralized IoT Networks: Moving towards decentralized models, such as blockchain-based IoT systems, can reduce the risk of single-point failures and mitigate privacy risks by enhancing control over data and reducing reliance on central authorities [37].

Access Control and Monitoring: Implementing strict access control policies and real-time monitoring can help identify potential vulnerabilities and unauthorized activities. Role-based access control (RBAC) and context-aware security can enhance the protection of sensitive data [38].

Privacy-Preserving Data Analytics: Using privacy-preserving technologies like homomorphic encryption and secure multi-party computation in IoT data analytics ensures that personal data is processed securely without exposing it to potential leaks [39].

IoT Device Lifecycle Management: IoT devices should be securely decommissioned and wiped of sensitive information at the end of their lifecycle to prevent data theft and ensure that unused devices do not become security risks [40].

Collaboration Between Stakeholders: Manufacturers, users, and regulators need to collaborate on developing industry standards and best practices for IoT security and privacy, as well as ensuring that IoT products meet established security requirements before being marketed [41]

Edge Computing and Localized Data Processing: Moving data processing to the edge of networks, close to where the data is generated, can reduce the risks associated with sending sensitive information over networks. Localized data processing minimizes exposure and enhances privacy [42].

```
// Main Flow
function main():
    if !auth() return "Auth Failed"
    data = anonymize(collect())
    data = encrypt(data)
    if !checkAccess() return "Access Denied"
    data = processData(data)
    sendData(data)
    analyzePrivately(data)
    monitor()
    if endOfLife() wipeDevice()
    return "Done"

// Authentication & Access
function auth(): return validToken()
function checkAccess(): return hasPermission()

// Data Handling
function anonymize(data): return removeID(data)
function encrypt(data): return encryptData(data)

// Processing & Communication
function processData(data): return (local() ? processLocally(data) : sendToCloud(data))
function sendData(data): return secureSend(data)

// Privacy & Monitoring
function analyzePrivately(data): return encryptedAnalyze(data)
function monitor(): if suspicious() alert()
function wipeDevice(): wipeData()
```

Figure 1: Secure Data Processing and Management Flow

Explanation

- **Main Function:** Integrates all IoT security measures, ensuring secure data collection, authentication, encryption, and continuous monitoring.
- **Authentication:** Verifies user credentials (biometric, token, or MFA) before granting access.
- **Data Minimization & Anonymization:** Reduces and anonymizes data to protect sensitive information.
- **Software Updates & Patch Management:** Regular updates ensure devices run the latest security patches.
- **Encryption & Secure Communication:** Encrypts data (TLS/SSL) during transmission for security.
- **Edge Computing:** Processes data locally or in the cloud, depending on needs.
- **Privacy-Preserving Analytics:** Uses techniques like homomorphic encryption for secure data analysis.
- **Blockchain:** Ensures transaction integrity and data consistency via blockchain.
- **Lifecycle Management:** Properly decommissions devices and wipes data at end of life.
- **Access Control & Monitoring:** Enforces RBAC and monitors for unauthorized access.

Table 7: Iot Problem and Its Solution

Problem	Solution
Lack of Standardization	Develop and enforce common security standards and protocols across IoT devices to ensure consistency and compatibility.
Data Privacy Concerns	Implement robust data encryption, anonymization techniques, and user consent management to safeguard personal information.
Device Vulnerabilities	Regularly update IoT devices with security patches, and implement secure boot processes and intrusion detection systems.
Insecure Communication	Use strong encryption (e.g., TLS/SSL) for communication between IoT devices and servers to protect data integrity.
Unauthorized Access	Implement strong authentication and access controls, such as multi-factor authentication (MFA) for IoT devices.

Future of IoT Device Security and Privacy Concern

The future of IoT security and privacy faces significant challenges as IoT technologies expand across sectors like healthcare and smart cities. Emphasize that the growing number of connected devices increases the attack surface, making effective security more difficult [43]. In healthcare, where IoT devices collect sensitive personal data, stress the need for secure communication and compliance with privacy regulations like HIPAA [44]. Highlights the importance of securing medical devices to prevent unauthorized access and data breaches [45]. As IoT adoption grows, standardization in security protocols is crucial for ensuring interoperability and compatibility. Data privacy remains a major concern, as IoT devices generate large amounts of personal data. Data protection techniques like anonymization and user consent management will be vital in addressing privacy concerns. Ultimately, securing IoT will require collaboration across industries to create robust solutions that safeguard both security and privacy.

Conclusion

In conclusion, while the Internet of Things (IoT) presents immense opportunities for innovation and convenience across various industries, it also introduces significant security and privacy challenges. The sheer volume of interconnected devices and the sensitive nature of the data they collect make IoT systems highly

vulnerable to cyber-attacks and privacy breaches. Key concerns include inadequate device security, lack of standardized protocols, data privacy violations, and the potential for unauthorized access to critical systems. Addressing these challenges requires the implementation of robust security measures, such as encryption, secure communication protocols, and regular software updates, along with privacy-focused strategies like data anonymization and user consent management [46-54].

As IoT continues to evolve, future advancements must prioritize creating secure, standardized, and privacy-respecting ecosystems. The involvement of industry stakeholders, including device manufacturers, policymakers, and end-users, is crucial to establishing comprehensive frameworks that mitigate risks. By advancing technologies like artificial intelligence for real-time threat detection and enhancing legal frameworks for data protection, the future of IoT can be safer and more secure, ensuring that its benefits outweigh the potential risks.

References

1. RH Weber, R Weber (2010) Internet of Things- New security and privacy challenges. Computer Law & Security Review 26: 23-30.
2. D Miorandi, S Sicari, FD Pellegrini, I Chlamtac (2012) Internet of Things: Vision, applications and research challenges. Ad Hoc Networks 10: 1497-1516.
3. J Zhou, VCM Leung (2015) Security and privacy in the Internet of Things: A survey, Proc. IEEE Int. Conf. Commun. (ICC) 1-6.
4. R Roman, J Zhou, J Lopez (2013) On the security and privacy of cyber-physical systems, Proc. 7th Int. Conf. Security Privacy Commun. 1Networks (SecureComm) 1-8.
5. M Conti, A Dehghantanha, K Franke, S Watson (2018) Internet of Things security and forensics: Challenges and opportunities, Future Generation Computer Systems 78: 544-546.
6. MA Babar, MA Niazi (2015) A systematic review on security and privacy of the Internet of Things. Int J Comput Appl 112: 1-8.
7. Y Liu, M Xu, M Liu (2017) A survey of IoT security and privacy, Proc. IEEE Int. Conf. Internet Things (iThings) 14-20.
8. L Zheng, S Jajodia (2016) Security and privacy in the Internet of Things, Computer Science Review 20: 1-10.
9. MI Shafique, M Guizani (2020) Security and privacy issues in IoT, Proc. 2020 IEEE 20th Int Conf Commun Technol (ICCT 2343-2348.
10. S Sicari, A Rizzardi, LA Grieco (2015) Security, privacy and trust in Internet of Things: The road ahead, Computer Networks 76: 1-21.
11. P Mell, T Grance (2011) The NIST definition of cloud computing, National Institute of Standards and Technology https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf.
12. W Yang, S Chen (2019) Security and Privacy in the Internet of Things (IoT): Technologies and Challenges, Springer.
13. S Sicari, A Rizzardi, LA Grieco (2016) Security, Privacy and Trust in the Internet of Things, Springer Series in Computer Science, Springer.
14. L Atzori, A Iera, G Morabito (2017) The Internet of Things: A Survey, in Springer Handbook of Internet of Things. Springer 345-358.
15. X Liu, Y Zhang (2019) Secure IoT Applications: The Privacy and Security Challenges, Elsevier.
16. C Cai, X Wang (2021) Security and Privacy in the Internet of Things, Wiley-IEEE Press.
17. Cisco (2016) Internet of Things (IoT) Security: Protecting the Expanding Surface of Vulnerability, Cisco Systems.
18. Gartner (2020) Hype Cycle for Emerging Technologies, Gartner Research.
19. IBM (2019) Securing the Internet of Things, IBM Security.
20. ENISA (2018) Security and Privacy in the Internet of Things, European Union Agency for Cybersecurity.
21. Kelechi G Eze, Cajetan M Akujuobi (2022) Design and Evaluation of a Distributed Security Framework for the Internet of Things, Journal of Signal and Information Processing 13.
22. PR Beznosov, BY Zhao (2014) Security and privacy issues in the Internet of Things, Proc. IEEE Globecom Workshops 1-6.
23. KA Azad, DM Shahin (2017) Securing the Internet of Things: Challenges, issues and solutions, International Journal of Computer Science and Network Security 17: 95-102.
24. MG Santis, FL David (2016) Security and privacy challenges in IoT systems, Proc. IEEE World Congress on Computer Science and Information Engineering 421-426.
25. G Chatzikokolakis, PGK Mahajan, PA Markopoulou (2019) On the privacy of IoT networks, IEEE Trans. Network and Service Management 16: 651-663.
26. M Barbeau, RK Gupta, KS Sandhu (2016) Privacy and security challenges in the Internet of Things, IEEE Internet of Things Journal 3: 1-12.
27. F Zhang, R Zhang, Y Li (2020) A survey of IoT security: Challenges, solutions, and future Directions. IEEE Access 8: 58515-58538.
28. Z Yan, J Li, MZY Zou (2018) A survey of security and privacy issues in IoT, Wireless Communications and Mobile Computing 1-13.
29. D Nguyen, H Mahemmed (2015) Security challenges in the Internet of Things: A survey, International Journal of Computer Applications 114: 1-9.
30. T Yu (2020) A survey of IoT security: Challenges, solutions and future directions, IEEE Internet of Things Journal 7: 1-14.
31. GAJ Smith (2018) Ensuring IoT security: Best practices for privacy protection, Journal of Network and Computer Applications 39: 24-37.
32. SR Mohsen (2021) IoT security: Challenges and solutions, Journal of Computer and Communications 9: 109-119.
33. MD Nguyen (2016) Security issues in the Internet of Things: A survey, International Journal of Computer Science and Information Security 14: 91-100.
34. HK Salama (2015) Challenges and solutions in the security of IoT devices, International Journal of Smart Home 9: 13-24.
35. NY Zhou (2018) Recent advances in IoT security: A survey, IEEE Transactions on Industrial Informatics 12: 745-757.
36. TK Li (2017) Security and privacy in the Internet of Things: A state of the art, IEEE Transactions on Information Forensics and Security 12: 1267-1280.
37. S Khan, MA Khan (2020) Challenges in IoT security and privacy: A comprehensive survey. IEEE Access 8: 155289-155312.
38. X Zeng, X Zhang (2020) IoT security and privacy in healthcare: A survey. IEEE Access 8:153943-153957.
39. DB Xiaoyang (2021) Security and privacy challenges in smart healthcare IoT. IEEE Internet of Things Journal 8: 1905-1918.
40. JM Rao (2017) Security concerns and challenges for the Internet of Things (IoT): A survey. International Journal of Computer Science 35: 315-322.
41. YF Zhang, DZ Liu (2016) Privacy protection in the Internet

of Things. IEEE Transactions on Knowledge and Data Engineering 28: 711-725.

42. A Al-Fuqaha, SS Gupta, M Mohammadi, MA Ayyash, ASGaddour, et al. (2015) Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, IEEE Communications Surveys & Tutorials 17: 2347-2376.
43. ZA Bakar, MB Abolhasan, TM Shirmohammadi (2020) Security and Privacy Issues in IoT Devices: A Survey. IEEE Access 8: 90869-90897.
44. MU Siddiqui, WA Shah, IA Syed (2020) A survey on the security and privacy challenges of Internet of Things (IoT), Proc. 2020 IEEE Int. Conf. Internet of Things (iThings) 126-131.
45. SC Mohsen (2021) Security and Privacy Challenges in the Internet of Things: A Survey, Computers, Materials & Continua 67: 2587-2604.
46. Internet of Things (IoT)- security, privacy, applications & trends | by Arin Dey Medium https://medium.com/@arindey/internet-of-things-iot-security-privacy-applications-trends-3708953c6200.
47. Al-Fuqaha A, Gupta SS, Mohammadi M, Ayyash MA, Gaddour AS, et al. (2015) Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials 17: 2347-2376.
48. Zhou Z, Leung VC (2015) Recent Advances in IoT Technology and Its Applications. IEEE International Conference on Communications (ICC), London, UK 4687-4692.
49. Sicari S, Rizzardi A, Grieco LA (2016) Security, Privacy and Trust in the Internet of Things, Springer Series in Computer Science, Springer 73-91.
50. SV Gupta (2015) Internet of Things (IoT): A Survey on Enabling Technologies, Protocols, and Applications, IEEE Communications Surveys & Tutorials 17: 2347-2376.
51. KG Eze, CM Akujuobi (2022) Trends in IoT Security: A Comprehensive Survey on Emerging Threats, Solutions, and Future Directions, Journal of Signal and Information Processing 13: 1-12.
52. CA Bakar, MB Abolhasan, TM Shirmohammadi (2020) Security and Privacy Issues in IoT Devices: A Survey. IEEE Access 8: 90869-90897.
53. C Li, H Li, L Yang, Z Yan (2019) Secure Data Processing and Management for IoT: Challenges and Solutions. IEEE Internet of Things Journal 6: 452-463.
54. DM Azad, MS Shahin, MZ Khan (2020) Internet of Things (IoT): Problems, Challenges, and Solutions. IEEE Access 8: 169-186.