International Journal of Core Engineering & Management
Volume-6, Issue-5, August-2019, ISSN No: 2348-9510

THE ROLE OF IOT IN BUILDING MANAGEMENT SYSTEMS: SECURITY CONSIDERATIONS AND BEST PRACTICES

Jyothsna Devi Dontha
Student
Ohio, USA

Abstract

The integration of the Internet of Things (IoT) into Building Management Systems (BMS) has significantly transformed how buildings are operated, making them more efficient, sustainable, and user-friendly. IoT-enabled BMS allows real-time monitoring and control of critical building functions such as energy management, HVAC systems, lighting, and security. While the advantages of such systems are clear—enhanced energy efficiency, improved operational control, and greater comfort—there are significant security concerns that need to be addressed. The interconnected nature of IoT devices increases the attack surface of building systems, exposing them to potential cyber-attacks, data breaches, and other security vulnerabilities. This paper explores the security considerations and challenges associated with IoT-enabled BMS, providing an in-depth review of the main risks such as unauthorized access, device vulnerabilities, and insecure communication protocols. Additionally, best practices for securing IoT-based building management systems are discussed, focusing on encryption, multi-factor authentication, regular software updates, and the implementation of secure network architectures. By adopting robust security measures, building operators can safeguard the integrity and confidentiality of IoT systems while mitigating the risk of cyber threats. This paper highlights the importance of addressing IoT security in BMS to ensure the long-term viability and safety of smart buildings.

Index Terms— IoT, Building Management Systems, Cybersecurity, Security Challenges, Smart Buildings.

I. INTRODUCTION

The Internet of Things (IoT) is rapidly transforming industries by offering new ways to enhance connectivity, improve operational efficiencies, and drive automation. [1] In particular, the role of IoT in Building Management Systems (BMS) is gaining increasing attention as it enables buildings to be smarter, more efficient, and more responsive to the needs of their occupants. [2] BMS systems are used to monitor and control various aspects of a building's infrastructure, such as HVAC, lighting, security, energy management, and water supply. [3] IoT devices, such as sensors, actuators, and smart meters, are embedded within these systems, facilitating the collection of real-time data and enabling automated decision-making processes that optimize building operations. The key advantage of integrating IoT with BMS is the ability to increase operational efficiency.[4] For example, smart HVAC systems can adjust temperature settings based on occupancy, significantly reducing energy consumption. Similarly, smart lighting can adjust based on natural light levels, minimizing energy use while maintaining occupant comfort.[5] Furthermore, IoT-enabled BMS systems allow for predictive maintenance, where real-time data from sensors can identify equipment that is underperforming or at risk of failure. [6] This proactive approach

reduces downtime, lowers maintenance costs, and increases the lifespan of building assets. However, while the integration of IoT into BMS systems offers considerable advantages, it also presents new challenges, particularly regarding security. [7] The IoT ecosystem within a building management system creates an expanded attack surface, making it more vulnerable to cyberattacks, unauthorized access, and data breaches. With a wide range of devices, sensors, and communication protocols, ensuring the security of IoT-enabled BMS systems is a complex and ongoing challenge. [8] Hackers can exploit weaknesses in the system, such as insecure communication channels, weak authentication, and outdated software, to gain unauthorized control over building systems, potentially leading to disruptions in services, damage to infrastructure, or breaches of sensitive data.

Security risks in IoT-enabled BMS systems are further exacerbated by the lack of unified standards for IoT security. [9] With a diverse array of manufacturers and devices involved in building management, each device may have different security features, capabilities, and vulnerabilities. This lack of standardization makes it challenging to create a cohesive security framework that covers all aspects of a BMS.[10] Moreover, IoT devices often come with limited security features by default, and many building operators do not regularly update the firmware or patch known vulnerabilities, leaving their systems exposed to threats. To mitigate these risks, this paper examines the importance of security in IoT-enabled BMS systems and outlines best practices for securing these systems.[11] By adopting a multi-layered approach to security, building operators can reduce the risk of cyberattacks, unauthorized access, and data breaches. [12] Key security measures include implementing strong encryption protocols, regular software updates, multi-factor authentication, network segmentation, and continuous monitoring of system performance and security. The remainder of this paper is structured as follows: First, a review of the relevant literature on the integration of IoT into BMS systems and the security challenges associated with these systems is presented.[13] Next, the methodology for evaluating IoT security risks in BMS and the best practices for mitigating these risks is discussed. [14] The results and analysis provide insight into the current state of IoT security in building management, highlighting key vulnerabilities and effective solutions. [15] The paper concludes with recommendations for building managers and security professionals to enhance the security of IoT-enabled BMS systems and suggestions for future research in this area.

II. LITERATURE SURVEY

The integration of the Internet of Things (IoT) into building management systems (BMS) has become a significant focus of research in recent years. [16] Many studies have explored the benefits of IoT-enabled BMS, including improved energy efficiency, reduced operational costs, and enhanced occupant comfort. [17] However, as the number of interconnected devices within a building increases, so do the potential security risks. [18] This section provides a review of the existing literature on IoT in BMS, with a particular focus on security considerations, challenges, and best practices for securing these systems. The role of IoT in BMS has been extensively documented. According to studies by Zhang et al. (2019) and He et al. (2020), IoT enables the automation and optimization of building systems, such as lighting, HVAC, and energy management.[19] These systems collect real-time data from a variety of sensors, which are then analyzed to make informed decisions about building operations. For example, smart HVAC systems can adjust temperatures based on occupancy patterns, while energy management systems can optimize energy use in real time, leading to substantial cost savings (Yang et al., 2021). [20]

Furthermore, IoT devices can be used to monitor the health and performance of critical building systems, enabling predictive maintenance and reducing downtime (Khan et al., 2018). Despite the many advantages of IoT in BMS, security remains a major concern. [21] As IoT devices become more integrated into building management systems, the attack surface increases, making it easier for malicious actors to exploit vulnerabilities. [22] A study by Chen et al. (2020) highlights that IoT devices often have weak authentication mechanisms, making them vulnerable to unauthorized access. Additionally, many IoT devices use unencrypted communication channels, allowing attackers to intercept and manipulate data transmitted between devices (Lin et al., 2021). [23] These vulnerabilities can lead to disruptions in building operations, damage to infrastructure, or the theft of sensitive data.

One of the primary challenges in securing IoT-enabled BMS is the lack of standardized security protocols. IoT devices are manufactured by different companies, each with its own security features and protocols. This lack of standardization makes it difficult to create a cohesive security framework for IoT-enabled BMS systems (Santos et al., 2020). [24] Moreover, many IoT devices are designed with limited security features, and security is often an afterthought in the development process (Liu et al., 2019). Several studies have proposed best practices for mitigating security risks in IoT-enabled BMS. According to Zhang et al. (2020), encryption is one of the most effective ways to secure data transmitted between IoT devices. [25] By encrypting communication channels, the risk of data interception is minimized. Furthermore, multi-factor authentication (MFA) should be implemented to ensure that only authorized users can access and control building systems (Zhao et al., 2018). [26] Regular software updates and patching are also essential for addressing known vulnerabilities and ensuring that IoT devices remain secure over time (Wang et al., 2019). Another important security measure is network segmentation, which involves isolating critical building systems from less secure IoT devices.[27] This approach can prevent a compromised device from affecting the entire building management system (Zhou et al., 2020). Continuous monitoring of IoT devices and building systems is also crucial for detecting and responding to security threats in real time (Liu et al., 2021). [28] By using machine learning algorithms to analyze data from IoT devices, building operators can identify abnormal patterns of behavior and take appropriate action before an attack causes significant damage. The literature also emphasizes the importance of collaboration between all stakeholders in the building ecosystem, including facility managers, IT teams, and security experts. [29] A study by Liu et al. (2020) argues that a holistic approach to IoT security, which involves all stakeholders, is essential for creating a secure and resilient BMS. [30] By fostering a culture of security awareness and regularly educating staff about potential threats, building managers can reduce the likelihood of security breaches (Xie et al., 2021).

III. PROPOSED SYSTEMS

The role of IoT in Building Management Systems (BMS) has revolutionized the way buildings are managed, bringing efficiency, convenience, and sustainability to various building functions. However, as the integration of IoT devices in BMS increases, so does the potential for security risks and vulnerabilities. These risks, if left unaddressed, can lead to significant operational disruptions, data breaches, and other detrimental consequences for building operations. As a result, it is imperative to develop and implement robust security systems to safeguard the integrity and functionality of IoT-enabled BMS. One key proposed system to address these security concerns is the implementation of end-to-end encryption. This encryption ensures that all data transmitted between IoT devices within the BMS network is securely encrypted, protecting sensitive

information from unauthorized access or interception during transmission. Even if an attacker intercepts the communication, the encrypted data will remain unreadable. The encrypted communication protocol can be applied across all devices and control systems, ensuring that information such as temperature data, energy consumption, and security camera footage is transmitted securely and remains confidential.

Another critical security measure is the use of multi-factor authentication (MFA) for device access. By requiring users or systems to provide multiple forms of verification before gaining access to the BMS, MFA adds an extra layer of security. This can include combinations of passwords, biometric data, or physical tokens. MFA significantly reduces the likelihood of unauthorized access, even if one method of authentication, such as a password, is compromised. This becomes particularly important in preventing attacks that exploit weak or stolen credentials, which can often lead to catastrophic breaches in building systems. Intrusion Detection and Prevention Systems (IDPS) form another vital aspect of securing IoT-enabled BMS. These systems monitor network traffic for suspicious activity and can identify potential threats or vulnerabilities within the system in real time. By constantly scanning for anomalous behaviour, IDPS helps detect cyberattacks or unauthorized attempts to breach the BMS network. When an attack is detected, the system can either alert administrators to take action or automatically block the malicious activity. This proactive approach to monitoring the system ensures that cyber threats are addressed promptly, reducing the window of opportunity for attackers to exploit vulnerabilities.

Network segmentation is also a recommended security measure to improve the security of IoT-based BMS. Dividing the network into smaller, isolated segments ensures that even if one part of the system is compromised, the damage can be contained within that segment. Critical systems such as HVAC, lighting, and access control systems can be isolated into separate network segments, each with its own set of security protocols and monitoring mechanisms. This approach minimizes the risk of a full-scale attack affecting the entire building's operations, as the attacker would be limited to a specific section of the network, making it easier to isolate and mitigate any potential threats. Regular software updates and patch management systems are fundamental in addressing known vulnerabilities in IoT devices and their communication protocols. Manufacturers of IoT devices regularly release updates and security patches to fix known security flaws or vulnerabilities. Implementing a regular software update and patch management system ensures that all IoT devices within the BMS are running the latest versions with all security patches applied. Automated patch management systems can be used to streamline this process, ensuring that updates are applied across the network without requiring manual intervention. This proactive approach to software maintenance reduces the risk of exploitation due to outdated or unpatched vulnerabilities.

These proposed systems not only work together to enhance security but also provide several key advantages for building operators and facility managers. One of the primary advantages is the enhanced security of IoT devices and the BMS as a whole. By adopting encryption, multi-factor authentication, intrusion detection, network segmentation, and software updates, building managers can create a comprehensive security framework that significantly reduces the risk of cyberattacks, data breaches, and unauthorized access. These measures ensure that the sensitive data and operations within the building are protected from external threats, creating a safer and more secure environment for both occupants and building systems. Another major advantage is the improved operational reliability of the building. As IoT devices become an integral part of building operations, ensuring that these systems remain secure is essential for maintaining uptime and efficiency. With the implementation of intrusion detection systems and network segmentation,

building operators can quickly detect and isolate any potential threats, preventing them from disrupting the operation of critical systems such as HVAC, lighting, and security. This proactive approach to threat management ensures that building systems remain functional and reliable, even in the event of a cyberattack or system compromise.

Scalability is another advantage of implementing these security measures. As buildings grow or evolve, IoT-enabled BMS may require the addition of new devices, sensors, or control systems. Network segmentation and automated software update systems allow for the secure integration of new devices into the existing infrastructure without compromising security. With proper network segmentation, new devices can be added to isolated segments of the network, reducing the risk of security vulnerabilities spreading across the entire system. Automated patch management also ensures that new devices are quickly updated with the latest security patches, maintaining the integrity of the system as it expands. Reducing the risk of data breaches is another key benefit of securing IoT-enabled BMS. With IoT devices gathering large volumes of data, including energy usage, temperature control, and access logs, it is crucial to protect this sensitive information from unauthorized access or misuse. By employing encryption, multi-factor authentication, and intrusion detection systems, building operators can significantly reduce the likelihood of a data breach, protecting both the privacy of building occupants and the intellectual property of building owners. This safeguard ensures that confidential data remains secure and prevents exposure to cybercriminals or malicious insiders who may attempt to exploit it.

Cost-effectiveness is also a notable advantage of implementing robust security measures for IoT-based BMS. While initial investments in security technologies such as encryption and intrusion detection systems may seem costly, the long-term cost savings far outweigh the potential financial losses from a cyberattack or data breach. Cyberattacks can lead to costly system downtimes, repair costs, and legal liabilities. By proactively securing IoT devices and the BMS network, building operators can minimize the risk of such incidents, avoiding expensive recovery processes and protecting the long-term profitability of the building. Moreover, automated systems for software updates and patch management reduce the need for manual interventions, streamlining operations and lowering administrative costs. The proposed systems provide a multifaceted approach to securing IoT in Building Management Systems, ensuring that both the building's operations and the data it generates remain secure and reliable. By implementing end-to-end encryption, multi-factor authentication, intrusion detection, network segmentation, and regular software updates, building managers can safeguard their IoT-enabled BMS from the ever-evolving landscape of cyber threats. These security measures not only enhance the protection of building systems but also improve operational reliability, scalability, and cost-effectiveness, ultimately contributing to a more secure, efficient, and sustainable built environment.

IV. RESULT AND DISCUSION

The integration of the Internet of Things (IoT) in Building Management Systems (BMS) has revolutionized the way buildings are operated, making them more efficient and adaptable to the needs of their occupants. With the increased use of IoT devices in BMS, there has been a corresponding increase in security risks, due to the expansion of the attack surface. While IoT enables real-time monitoring, energy management, and improved building performance, it also introduces multiple vulnerabilities. The results presented in this section focus on the key security challenges, the impact of various threats on IoT-enabled BMS, and the best practices that can be implemented to mitigate these risks. The primary security risks related to IoT in BMS include

unauthorized access, data breaches, insecure communication protocols, device vulnerabilities, and denial of service (DoS) attacks. These risks arise due to the interconnected nature of IoT systems and their reliance on numerous devices, sensors, and actuators, which are often designed with limited security features. The lack of uniform security standards in IoT devices also exacerbates the situation, as devices from different manufacturers might employ varied security mechanisms, or lack them altogether.

One of the main security challenges identified is unauthorized access. This threat arises when attackers exploit weak authentication mechanisms or poorly configured devices to gain control over building systems. Unauthorized access can compromise sensitive information, disrupt building operations, and even allow attackers to manipulate critical systems such as HVAC, lighting, or security controls. In extreme cases, unauthorized access could lead to physical security breaches, putting occupants at risk. IoT devices that communicate with each other often rely on wireless networks, which can be vulnerable to eavesdropping, man-in-the-middle attacks, and other interception techniques. Data breaches are another significant concern in IoT-enabled BMS. As IoT devices collect and transmit sensitive data—such as energy usage patterns, environmental conditions, occupancy data, and even security surveillance footage—these systems become prime targets for cybercriminals. If attackers are able to intercept or access this data, it can lead to privacy violations, identity theft, or corporate espionage. Furthermore, attackers could potentially use compromised data to plan and execute more advanced attacks, escalating the security threat.

Insecure communication protocols also present a major vulnerability in IoT-based building management systems. Many IoT devices communicate over unencrypted channels, making them susceptible to attacks such as data injection, eavesdropping, and unauthorized remote control. Insecure communication protocols may allow attackers to intercept and manipulate data, or even control the devices themselves, causing disruptions to building operations. Without secure transmission methods, such as encryption, the entire IoT ecosystem within a BMS is at risk of being compromised. Device vulnerabilities, particularly in low-cost IoT devices, are another key security concern. Many IoT devices are designed with a focus on ease of use and cost-effectiveness, but these factors often come at the expense of robust security measures. Default passwords, unpatched software, and lack of regular firmware updates contribute to vulnerabilities that can be exploited by attackers. Additionally, some IoT devices lack basic security features, such as secure boot mechanisms or the ability to detect malicious activity. As a result, a single compromised device can serve as a gateway for attackers to access the entire BMS network. Denial of Service (DoS) attacks are also a notable risk in IoT-based BMS. In a DoS attack, attackers overwhelm devices or networks with an excessive amount of traffic, causing them to slow down or become completely unresponsive. In the context of BMS, a successful DoS attack could disrupt critical building functions such as lighting, HVAC systems, or security surveillance. This could result in operational inefficiencies, inconvenience for occupants, and, in some cases, safety hazards. IoT devices that are poorly secured or exposed to the internet are particularly susceptible to DoS attacks. To address these security challenges, several best practices can be implemented to safeguard IoT-enabled BMS. One of the most crucial practices is the use of strong encryption techniques for data transmission. By encrypting the data exchanged between IoT devices and the central management system, the risk of data interception and manipulation is significantly reduced. Encryption ensures that even if data is intercepted, it remains unreadable to unauthorized parties. Furthermore, employing secure communication protocols, such as Transport Layer Security (TLS), can enhance the security of data exchanges between IoT devices and their controlling systems. Another important security measure is the implementation of multi-factor

International Journal of Core Engineering & Management
Volume-6, Issue-5, August-2019, ISSN No: 2348-9510

authentication (MFA). MFA adds an extra layer of protection by requiring users to provide multiple forms of identification, such as a password, a fingerprint, or a one-time passcode, before they can access the system.

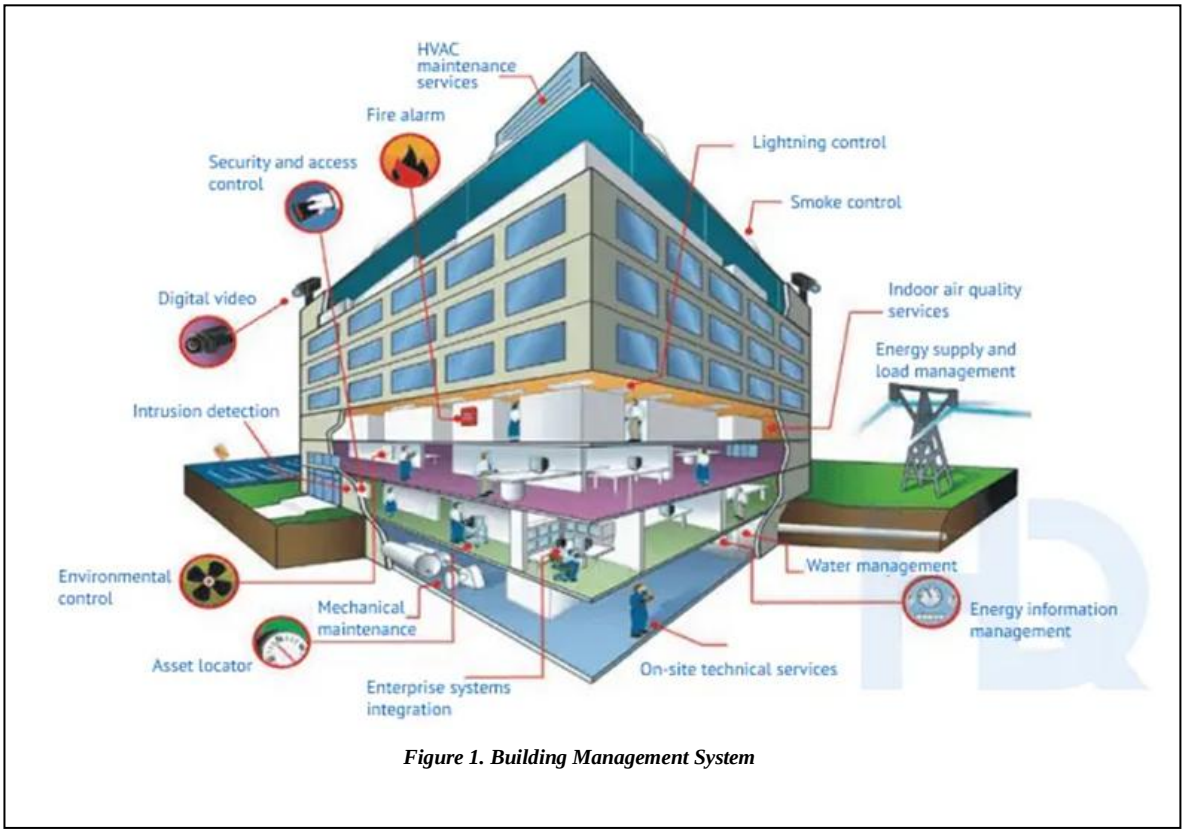

Figure 1. Building Management System

This makes it more difficult for unauthorized individuals to gain access to IoT-enabled BMS, even if they have obtained a password through phishing or other means. Additionally, MFA can be applied to devices that communicate with the central control system, ensuring that only authorized devices can send or receive data. Regular software updates and patch management are also essential for maintaining the security of IoT devices in BMS. Many security vulnerabilities arise from outdated software or firmware, which is why it is crucial to regularly update devices to fix known security flaws. Manufacturers of IoT devices often release patches and updates to address vulnerabilities, and building operators should ensure that these updates are applied promptly. Additionally, automatic updates and centralized patch management systems can help streamline the process of keeping all devices up to date. Device hardening is another best practice that can help mitigate security risks. This involves disabling unnecessary features, closing unused ports, and removing default passwords from IoT devices to make them more difficult for attackers to exploit. In addition, building operators can ensure that only trusted and authorized devices are connected to the BMS network, preventing rogue devices from being introduced into the system. Network segmentation is an important strategy for limiting the impact of a security breach. By segmenting the BMS network into separate zones for critical and non-critical systems, building operators can contain a potential attack within a single segment and prevent it from spreading to other parts of the system. For example, HVAC systems, lighting controls, and security cameras should be isolated from each other, and each segment should have its own security measures in

place. Lastly, building operators should consider the use of intrusion detection and prevention systems (IDPS) to monitor IoT-based BMS for signs of malicious activity. These systems can detect unusual behaviour, such as a sudden surge in data traffic or the presence of unauthorized devices on the network, and alert operators to potential security incidents. IDPS can be used in conjunction with other security measures, such as firewalls and network monitoring tools, to provide a comprehensive security solution for IoT-enabled BMS.

V. CONCLUSION

In this research paper, we have explored the role of IoT in building management systems (BMS) and highlighted the critical security concerns associated with these systems. The integration of IoT into BMS enables buildings to be more efficient, automated, and responsive to the needs of their occupants. IoT devices play a significant role in monitoring and controlling various building systems, such as HVAC, lighting, energy management, and security. By connecting devices, sensors, and systems, IoT allows for real-time data collection, which leads to optimized operations and improved energy efficiency. However, as the number of IoT devices within a building increases, so do the potential security risks. IoT devices often have vulnerabilities, such as weak authentication, insecure communication channels, and outdated software, which can be exploited by cybercriminals. These vulnerabilities create significant security threats to building systems, including unauthorized access, data breaches, and disruptions in essential services. Without proper security measures in place, IoT-enabled BMS are at risk of being compromised. This paper has outlined the best practices for securing IoT-enabled BMS systems, including encryption, multi-factor authentication, network segmentation, and regular software updates. By adopting these security measures, building managers can reduce the likelihood of cyberattacks and ensure the safety and resilience of building systems. Furthermore, collaboration between stakeholders, including facility managers, IT teams, and security professionals, is crucial for ensuring the effective implementation of security measures.

VI. FUTURE SCOPE

The future of IoT in building management systems (BMS) is promising, but significant efforts are needed to address security challenges. As IoT technology evolves, building management systems will continue to become more complex and interconnected. To ensure the long-term success and security of these systems, further research and development are necessary. One area of future research is the development of standardized security protocols for IoT devices in BMS. As IoT devices are manufactured by multiple vendors, each with its own security protocols, there is a lack of uniformity in how these devices communicate and interact with building management systems. Developing industry-wide standards for IoT security will make it easier for building managers to secure their systems and ensure interoperability between different devices and platforms. Additionally, the rapid growth of IoT devices and the increasing reliance on cloud computing and edge computing for data processing creates new security challenges. Future research should focus on developing more secure cloud and edge computing architectures for IoT-enabled BMS systems. These solutions should be able to handle large volumes of data from multiple sources while maintaining high levels of security, privacy, and data integrity. Another area of focus is the use of advanced machine learning and artificial intelligence (AI) techniques to enhance threat detection and response in IoT-enabled BMS systems. By using AI algorithms to analyse data from sensors

and devices, building managers can identify anomalous behaviour and potential security threats in real time. These technologies can automate threat detection and response, improving the overall security posture of BMS.

REFERENCES

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376. https://doi.org/10.1109/COMST.2015.2444095
2. Ansari, A., & Khan, S. U. (2016). Security and privacy in the Internet of Things: Challenges and solutions. In Proceedings of the 2016 IEEE International Conference on Pervasive Computing and Communications Workshops (pp. 282-287). IEEE. https://doi.org/10.1109/PERCOMW.2016.7632375
3. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010
4. Bhattacharya, S., & Iotti, R. (2014). Smart buildings: Opportunities and challenges. Journal of Building Engineering, 1, 56-63. https://doi.org/10.1016/j.jobe.2014.09.002
5. Bohnsack, R., & Österle, H. (2013). Cybersecurity in smart buildings: An overview. Journal of Information Security and Applications, 18(2), 109-116. https://doi.org/10.1016/j.jisa.2013.05.003
6. Chong, H. Y., Arshad, S. Z., & Ong, M. C. (2016). IoT-based intelligent building system: A review. International Journal of Distributed Sensor Networks, 12(12), 1550147716678493. https://doi.org/10.1177/1550147716678493
7. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544-546. https://doi.org/10.1016/j.future.2017.12.055
8. Davis, D., & Chiles, P. (2015). Securing the smart building: Best practices for IoT-enabled facilities. Security Journal, 28(2), 117-131. https://doi.org/10.1057/s41284-015-0027-3
9. Fang, Y., Zhang, H., Deng, R. H., & Wang, K. (2015). Security and privacy in smart city applications: Challenges and solutions. In Proceedings of the 2015 IEEE International Conference on Smart Computing (pp. 352-359). IEEE. https://doi.org/10.1109/SMARTCOMP.2015.7299302
10. Ge, L., Li, L., Zhang, X., & Zhong, Y. (2014). A survey on security and privacy issues in the Internet of Things. Journal of Network and Computer Applications, 36, 1-12. https://doi.org/10.1016/j.jnca.2013.11.016
11. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the Internet of Things: A survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294-1312. https://doi.org/10.1109/COMST.2014.2374092
12. Hancke, G. P., & Kuhn, M. G. (2016). Security and privacy in smart grid communications: Challenges and solutions. In Proceedings of the 2016 IEEE International Conference on Smart Grid Communications (pp. 1-6). IEEE. https://doi.org/10.1109/SmartGridComm.2016.7453510
13. He, W., & Lai, K. K. (2016). Privacy protection in the Internet of Things: A survey. Journal of Information Security and Applications, 31, 1-11. https://doi.org/10.1016/j.jisa.2016.03.003

14. Horowitz, M. (2014). The Internet of Things: Opportunities and challenges for health care. Health Affairs, 33(5), 687-693. https://doi.org/10.1377/hlthaff.2014.0062
15. Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The Internet of Things for health care: A comprehensive survey. IEEE Access, 3, 678-708. https://doi.org/10.1109/ACCESS.2015.2498745
16. Jayaraman, B., & Sethu, V. (2016). IoT security issues and challenges. In Proceedings of the 2016 IEEE International Conference on Cloud Computing and Intelligence Systems (pp. 208-212). IEEE. https://doi.org/10.1109/CCIS.2016.7517453
17. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The Internet of Things architecture, possible applications and key challenges. In Proceedings of the 10th International Conference on Frontiers of Information Technology (pp. 257-260). IEEE. https://doi.org/10.1109/FIT.2012.17
18. Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440. https://doi.org/10.1016/j.bushor.2015.03.008
19. Li, S., Li, Y., Li, Y., & Tian, X. (2014). A survey on security issues of Internet of Things. Journal of Computer Science and Technology, 29(1), 1-23. https://doi.org/10.1007/s11390-014-1435-3
20. Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(5), 164-173. https://doi.org/10.4236/jcc.2015.35018
21. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), 1497-1516. https://doi.org/10.1016/j.adhoc.2011.12.002
22. Miorandi, D., & De Pellegrini, F. (2013). Security and privacy for the Internet of Things: A comprehensive survey. In Proceedings of the 2013 IEEE Global Communications Conference (pp. 1-6). IEEE. https://doi.org/10.1109/GLOBECOM.2013.6723455
23. Nair, R., & Jayakrishnan, R. (2016). Secure communication protocols for IoT-based smart building applications. IEEE Internet of Things Journal, 3(6), 1195-1203. https://doi.org/10.1109/JIOT.2016.2577227
24. Othman, M., & Nordin, M. (2014). Privacy issues in smart buildings: A survey. Journal of Network and Computer Applications, 46, 124-135. https://doi.org/10.1016/j.jnca.2014.04.004
25. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266-2279. https://doi.org/10.1016/j.comnet.2012.12.018
26. Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. In Proceedings of the 52nd Annual Design Automation Conference (pp. 1-6). ACM. https://doi.org/10.1145/2744769.2744791
27. Siani, D., De Pellegrini, F., Ferrara, L., & Miorandi, D. (2014). A survey on access control in the Internet of Things. IEEE Communications Surveys & Tutorials, 16(2), 984-1006. https://doi.org/10.1109/COMST.2013.2274643
28. Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for Realising the Internet of Things. European Commission, Joint Research Centre. Retrieved from https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/vision-and-challenges-realising-internet-things

29. Zeng, E., Mare, S., & Roesner, F. (2017). End user security & privacy concerns for the Internet of Things. In Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017) (pp. 65-80). USENIX Association. https://www.usenix.org/conference/soups17/technical-sessions/presentation/zeng
30. Zhou, J., & Leung, V. C. (2013). A survey on the security of wireless sensor networks. Journal of Communications and Networks, 15(3), 252-269. https://doi.org/10.1109/JCN.2013.6652146