ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume XII Issue VII July 2025

Economic Implication of IoT Devices Security in The Hospitality: A Comprehensive Evaluation

Muhammed Jaffer V, Muhammed Unais

Muhammed Abdurahiman Memorial Orphanage College, India

DOI: https://doi.org/10.51244/IJRSI.2025.120700001

Received: 05 July 2025; Accepted: 07 July 2025; Published: 26 July 2025

ABSTRACT

The introduction of IoT devices in the hospitality industry has greatly improved the satisfaction of guests and the efficiency of operations. It is important to identify the economic outcome by introducing such technology in the hospitality industry. The hospitality industry is known as a labour intensive and highly personalised industry. Identifying the use of IoT technology and how this will economically impact it can help to formulate a plan for introducing IoT technology further in the hospitality industry.

This research is designed to pinpoint the economic effect of IoT devices in the hospitality industry. The outcome of this research will have a global acceptance, as the era we live in moves toward a path that adopts technology in every step. Recognizing economic implications can help stakeholders in developing strategic plans for introducing IoT based environments in the hospitality industry.

Keywords: IoT devices, hospitality, Cybersecurity,

INTRODUCTION

The development in information communication technology has proven to be crucial in today's day-to-day life. IoT is a subset of Information and communication technology (ICT) (Bógdał-Brzezińska, 2020). IoT refers to a network of physical devices that have embedded technology such as sensor software and connectivity in order to collect and exchange data using the internet or a similar communication network (Madakam et al., 2015). These devices can be sensors, appliances, vehicles, and machinery that ease the day-to-day functions of human beings.

The introduction of Internet of Things (IoT) technologies has transformed the hospitality industry (Buhalis and Leung, 2018). The use of IoT can be seen widely in different areas of the hotel industry. Smart hotel rooms enabled with automated control for lighting, temperature, etc.; enhanced customer experience with the use of mobile applications for check-in and check-out, smart key systems via smartphone are some of the customer-oriented experiences that IoT provides (Car et al, 2019). The IoT also assists in energy management, maintenance and housekeeping, security and safety, and inventory and asset management (car et al, 2019).

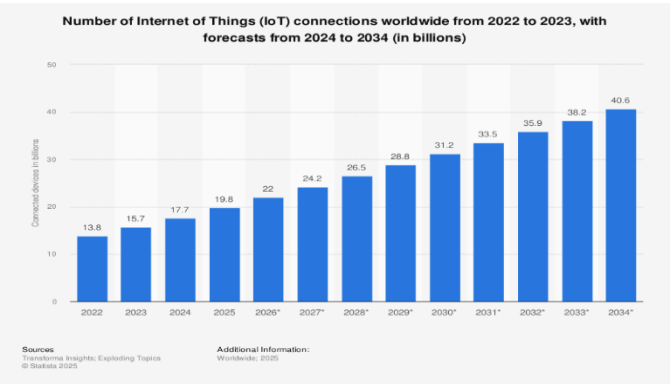

Figure 1

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume XII Issue VII July 2025

The number of IoT enabled devices are expected to reach 40.6 million by the year 2034 statista (2025). The use of IoT in hospitality sectors has many economic benefits. IoT helps to reduce operational costs by enabling automation and real-time monitoring. This feature helps in smart energy saving and water management in the hotels industry (Mercan et al., 2021). Providing personalized and efficient service delivery, IoT enhances customer experience, which leads to increased spending and higher customer satisfaction (Mercan et al, 2021). IoT collects data on guest preferences that assist the industry in formulate personalized services and tailored recommendations (Shani et al., 2023). The IoT driven analytics optimize pricing in peek seasons which enhances profitability further (Shani et al., 2023).

But moving toward such a digital environment has its own demerits as well. Since the IoT uses internet technology, the chances of a cyberattack against the establishment are high. These challenges pose significant concerns to overall network security, data integrity and guest privacy (Lee, 2020)). There are multiple security challenges that can be categorized under 4 domains (Taherdoost, 2023). Device security, data security, network security and application security are the domains identified. Any compromise to any of these domains can lead to loss of credibility of the organization.

Implementation of IoT can greatly benefit an organization. But acknowledging its technical integrity is important. Since the hospitality industry is a perfect competition market, any error that causes loss of their personal data will arise a negative emotion toward the establishment. Regular security updates and implementing a strong system to protect the valuable data will be sufficient to gain the trust of consumers. Although the rise of niche tourism models such as digital detox tourism will promote an environment that doesn't rely on such systems.

Aim and Objectives

Evaluating the security procedures and IoT device deployment in hotels as of right now.

- Determining typical weaknesses and methods of attack directed towards IoT devices within hotel networks.
- Assessing current security measures and procedures to reduce IoT-related hazards in lodging environments.
- Assessing financial consequences of various attacks on establishment.
- Using real-world case studies and real-world implementations to validate the suggested framework.

Significance of The Study

The hospitality industry has been increasing its reliance on digital technology such as IoT for operational efficiency and guest satisfaction. IoT enabled facilities such as smart room management, keyless entry, smart check-in and check-out, and personalized guest experiences are proven to be economical for the industry as well. Although, adopting such technologies can invite cyberthreats on the institution. The more the reliance on technology, the more the chance of cyber threats. These breaches can cause significant financial losses to the firm. These include direct costs such as ransom payments, legal penalties and indirect costs such as reputational damage. It is important to pinpoint these economic factors caused by various attacks.

LITERATURE REVIEW

IoT devices are becoming universal tools that can provide ease of work in a variety of areas. IoT presents a good opportunity for the tourism and hospitality industry as well (Car et al.,2019) it helps the industry to increase customer satisfaction and reduce operational costs (Car et al., 2019). The automation using IoT devices helps the establishments with smart energy consumption and water management (Mercan et al., 2021). Real time monitoring features help to carry out various complex activities effectively, such as room status updates and stock management (Mercan et al., 2021). IoT also assists in delivering personalized services,

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume XII Issue VII July 2025

which lead to higher guest satisfaction (Mercan et al., 2021). This helps the establishment be unique and acquire a large customer base. The data collected with the help of various IoTs can be effectively used for target marketing and to provide tailored services for various customers (Shani et al., 2023). Better marketing and personalized services delivery can help the establishment in developing a loyal customer base.

The security threats related to IoT are a matter of concern. The chances of security breaches via IoT devices can be attributed to inadequate security measures, unauthorized access, data interception, and device tampering (Lee, 2020). The integrity of IoT is being tested with various attacks. DDoS attacks, phishing, reply attacks, and insider attacks are the most occurring attacks faced by IoT environments (Iqbal and Auwul, 2022). The security breaches can be classified into four segments. Device security, network security, data security and application security (Taherdoost, 2023). Device security is concerned with the protection of physical devices from theft and tampering. It also comprises unauthorized access. Data protection contains safeguarding the data that are generated, transmitted and stored. The data should not be eavesdropped on or interfered. Network security is shielding the network infrastructure and protocols that enable communication between various IoT devices and other entities. Application security refers to the protection of software applications and services that run on IoT devices (Taherdoost, 2023).

The occurrence of any kind of security breach will cause financial and reputational damage for the establishment. Interference with the system may lead to system downtime and disruption in various services. These include smart room control, reservation and payments (Magalhães et al., 2016). Failing to address IoT security concerns may discourage customers from acquiring the product; thus, the organization may suffer financial losses. Breach can effectively damage the goodwill of the establishment, causing loss of customer truest and payments (Magalhães et al., 2016). Operational disruption due to cyberattacks can result in significant financial loss for the establishment. The disruption can cause guest inconvenience and potential revenue loss (Verma et al., 2021). A breach in data can result in a privacy breach of customers personal data. This will result in regulatory penalties (Verma et al., 2021).

The interconnected use of different devices, which performs varieties of functions make IoT enabled hotel environment vulnerable to various attacks (Dhirani et, al., 2021). The recommended practices to mitigate cyberthreats include the use of encryption technology, digital signatures, message authentication codes, certificates, access control policies, audit logs, and privacy- preventing techniques (Abbasi and Gheisari, 2023). Continued monitoring and the use of vigorous protocols are also recommended to mitigate cyberthreats (Lu and Xu, 2018). Advanced solutions such as blockchain technology, hardware-based security mechanisms, AI-powered anomaly detection, and privacy prevention techniques can ensure the integrity of data and real-time threat prevention (Usman et, al., 2023). Various authentication techniques will be handy in blocking various attacks. One-time password, mutual authentication based on ECC (Elliptic Curve Cryptography), ID verification, certificate verification and blockchain-based authentication will improve the security posture of the establishment (Iqbal and Auwul, 2022). The rising AI-based security is proven to be worthy in detecting and preventing cyberthreats. AI assisted anomaly detection can act as a firewall against outside threats. (Afzal et, al., 2023).

One way to improve the security posture is to divide the network into smaller subsets (Sen and Dash, 2023). This method will effectively reduce the risk of total shutdown. The use of new age technology such as blockchain based prevention techniques (Srivastava et.al, 2023). It enables transparent and traceable transaction ledgers and can be applied in protecting privacy and security. AI techniques such as machine and deep learning can enhance the security posture of the organization (Casteo et, al., 2023). Machine learning algorithms can analyze large quantities of data and can identify any anomaly in the system. to ensure secure communication, encryption technology can be applied (Pramanik et, al. 2023). Implementing an access control mechanism can restrict unauthorized access into the system.

RESEARCH METHODOLOGY

the nature of this research demands a mixed approach in data collection. Thus, the research uses qualitative and quantitative technique for data collection. In depth interviews was conducted with different professionals

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume XII Issue VII July 2025

associated with hospitality industry for collecting qualitative data. These professionals include top level managers, IT professionals and security experts.

Primary data

A structured questionnaire was distributed among the professionals who are associated with cybersecurity and hospitality industry. The questionnaire was designed in a manner which capture a broad range of perspective of application and security of IoT devices in hospitality sector. questionnaire contained 18 questions which are relevant to the field. Expert's opinions were taken to create the questionnaire, so that it may contain all the necessary domains needed for successful completion of the research.

Interview

In order to grasp better understanding of the situation and for in-depth study, personal interview were conducted among various hotel staffs. The samples were taken from different hotels from Kerala, so that a generic idea of the problem can be received. The staffs were divided into 2 groups which contained front office staffs and technical staffs. Front office staffs were the people who had direct connection with the guests. Understanding the reaction of guests is vital for the study, so this interview session was fruitful. Technical staffs are the supporting staff who facilitate smooth operation of IoT devices. Various cyber-attacks, the methods employees to prevent such attacks were the valuable insight received from this group.

Sampling technique

Convenient sampling was the most suitable method for the study. The exploratory nature of the research also demands a convenient sampling. More over the sample population is a particular group employed in firms operates in hospitality industry.

Sampling numbers

The researchers were successfully able to extract responses from 109 personnel employed in the hospitality institutions across Kerala.

Data analysis method

Descriptive analysis: the researcher employed various techniques such as mean, standard deviation, variance etc to analyse the data. These descriptive analysis measures helped to synthesis the findings.

Correlation analysis: in order to establish relationship between 2 variables Karl Person correlation was used. The researchers identified 2 main variables from the study. IoT devices and labelling of IoT devices was identified as the most recurring variables.

Tools used for statical analysis

The researcher used IBM SPSS Statistics (Version No: 29.0.2.0(20)) for the statistical analysis.

RESULT OF THE STUDY

The researcher explored 18 different variables with the help of a questionnaire and discussion. The descriptive analysis based on two predetermined variables was carried out to assess the result. SPSS software was instrumental in carrying out this analysis.

Variable 1: The result shows a mean score of 3.85and frequency distribution of 66%. This indicates that the majority have some idea about the use and importance of IoT devices.

Variable 2: For the question regarding the security of IoT devices, the majority of guests were lacking knowledge of IoT related security. which means they did not get any information.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume XII Issue VII July 2025

Descriptive Statistics						
Sl No	Variables	N	Mean		Std. Deviation	Variance
		Statistic	Statistic	Std. Error	Statistic	Statistic
1	Awareness of IOT Devices	109	3.853	0.1157	1.20819	1.46
2	Information about security of IOT Devices	109	3.294	0.1053	1.09969	1.209
3	Strange Activity of IOT Devices	109	2.505	0.0871	0.90905	0.826
4	Connection of Personal Devices to Hotel IOT	109	4.092	0.1206	1.25861	1.584
5	Suspicious activity due to Connection of personal device	109	1.642	0.1162	1.21353	1.473
6	Option of Disability or Data limiting	109	2.459	0.1534	1.60169	2.565
7	Disclosure of Best practices during data sharing	109	3.321	0.1009	1.05304	1.109
8	Accessibility of IOT Devices	109	3.239	0.1158	1.20876	1.461
9	Data Protection Confidence Level	109	2.495	0.1072	1.11906	1.252
10	Labelling of Instructions on IOT Devices	109	3.165	0.114	1.19035	1.417
11	Problems of IOT Devices	109	2.789	0.1188	1.24032	1.538
12	Seamlessly Stream Content Position	109	3.138	0.1448	1.5121	2.286
13	Utility of IOT Devices Provided	109	3.514	0.0756	0.78898	0.622
14	Disclaiming of data collection by IOT Devices	109	2.22	0.1363	1.42308	2.025
15	Expectations about Data Privacy of IOT	109	2.303	0.1794	1.87332	3.509
16	Security Policies for rebooking	109	3.642	0.0997	1.04104	1.084
17	Usage of available IOT Devices	109	3.101	0.1397	1.45898	2.129
18	Adoption of smart IOT by considering security and privacy	109	4.211	0.0885	0.92369	0.853

Variable 3: The majority of the guests did not find any suspicious activities that are worth noticing. The mean value of 2.504 and standard deviation of 0.91 back this conclusion.

Variable 4: The majority of the participants are confident in the IoT security of their respective establishments. Guests of the hotels always connect their personal devices with the hotels IoT device/network. The mean value of 4.1 and frequency of 75.02% indicate this result.

Variables 5: While connecting to the IoT/Network, 57.8% did not notice any kind of suspicious activities.

Variable 6: The rate at which disabling or limiting data at hotel premises is surprisingly low. Most of the respondents never or rarely disable or limit the data. It can also be interpreted as the option to disable or limit data connection of in-room IoT devices being highly inconsistent.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume XII Issue VII July 2025

Variable 7: The respondents lack clarity about the security practices in IoT devices to prevent cyberthreats. More than half of the respondents are uncertain about best practices to mitigate cyberthreats.

Variable 8: On the basis of analysis, 40.4% of respondents are uncertain about the accessibility of IoT devices in hotels. The mean value of 3.24 shows uncertainty in the visitors.

Variable 9: The respondents lack confidence about the protection and security of personal data collected via IoT devices. They have uncertainty regarding the privacy of sensitive data.

Variable 10: The responses indicate that some of the IoT devices have clear labels. Many have failed to notice labeling with instructions for accessing IoT devices.

Variable 11: Many of the visitors have experienced certain problems related to IoT devices.

Variable 12: 26.6% of respondents have tried to cast/stream content from their personal devices connected to IoT devices in their hotel room.

Variable 13: The majority of the respondents are neutral or satisfied (45% and 40.4%, respectively) about the utilities provided by using IoT devices.

Variable 14: 50.5% of the participants did not find any notice or disclaimer regarding data collection and storage while accessing IoT services. 20.2% sometimes notice, and 11% and 10% of the respondents replied with often and always notice.

Variable 15: The respondent's dissatisfaction regarding data privacy practices can be seen from the responses. Due to the inconsistency of the experience, variability in opinion can also be found from responses.

Variable 16: The majority of the respondents are likely or very likely influenced by a comprehensive hotel IoT security policy while re-booking.

Variable 17: The analysis clearly indicates that 49.6% have concerns about their privacy while using IoT devices in hotels. This is the main reason for not accessing these services.

Variable 18: With a 4.21 mean and less standard deviation shows a strong positive opinion regarding the adoption of IoT enabled amenities for assuring guest security and privacy in hotels.

DISCUSION AND ANALYSIS

Data integrity and privacy are important aspects for providing a better experience for the customers. It is important to formulate clear policies by the hotels to secure the privacy of the users. IoT devices pose serious threats due to their nature of connectivity in the internet or shared networks. The chances of getting attacked are likely high in weak security devices. This will result in the loss of valuable data and the loss of customer trust. Such events will lead to a damaging reputation and financial losses.

The study throws some valuable insight into current problems. It confirms that guests have no knowledge of how their data is handled and how these data are used in the future. Many have failed to recognize the mechanism on how to operate the device due to a lack of manuals. Proper labeling of devices is essential in order to create an impact on consumers. And the acknowledgement from the management regarding how the data is secured can boost the confidence of guests. The internet provided by the institution is the most used facility. High-speed internet is a basic facility that establishments have to provide. Although the majority of the visitors have concerns regarding Wi-Fi security. On technical side, there should be proper mechanism in order to avoid security breaches. This includes authentication, continues monitoring, and robust response protocols. It is important to train all the human resources to handle any kind of threats that may occur.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume XII Issue VII July 2025

Security Framework

Implementation of cutting-edged technology and artificial intelligence-enabled security frameworks can improve data security and protection in hotel IoT environments. These technologies can be implemented in various scenarios.

Anomaly detection: implementation of machine learning algorithms to detect suspicious activities can effectively prevent breaches in the network.

Predictive maintenance: an AI supervised system can predict when IoT devices are likely to fail or require maintenance. This will reduce downtime and potential security vulnerabilities.

Automated threat response: Developing an AI based threat management system can act swiftly against any kind of attack.

Intelligent access control: For secure access, facial recognition systems and biometric systems can be deployed, enhancing the physical security of the IoT infrastructure.

CONCLUSION

The integration of IoT devices in the hotel industry is essential to provide a better customer experience for the client. The hospitality industry is characterized by a perfect competition market. In order to be unique, the integration of IoTs is necessary. Moreover, it can help the establishments in providing tailored services and better marketing to target markets. Automation in various fields such as energy management, water management, and inventory management can help management is save cost.

Although the security threats posed by the IoT devices have to be acknowledged. Various attacks can occur in order to acquire precious data of the customers. Safeguarding these data is solely the responsibility of hotels. The study has identified the need for implementing robust security approaches since the guests are suspicious about how the data is handled. The hotels should clarify how safe these data are and be transparent about how these data will be used in the future. The majority of the guests have identified the need for the implementation of IoT enabled devices. This concludes that the guests understand its importance. Clarifying security matters can help them to boost confidence, which causes brand loyalty. Any kind of attack can have a negative effect on the reputation of the establishment. This includes financial loss as well. Legal penalties will be heavy as the organization fails to meet basic security measurements. On top of that the establishment may face reduced bookings since the guests lost their trust. Continues improvement in IoT practices is necessary. Ongoing research and collaboration among industry stakeholders, cybersecurity experts, and regulatory bodies are essential to develop and maintain robust security standards that keep pace with technological advancements.

REFERENCES

1. Abbasi, M., & Gheisari, M. (2023). Security in the Internet of Things application layer: Requirements, threats, and solutions. IEEE Access, 10, 97197-97216.
2. Afzal, M. U., Abdellatif, A. A., Zubair, M., Mehmood, M. Q., & Massoud, Y. (2023). Comprehensive survey on AI-based technologies for enhancing IoT privacy and security: Trends, challenges, and solutions. IEEE Access, 11(1), 1-25. https://doi.org/10.1109/ACCESS.2023.2228053
3. Bógdał-Brzezińska, A. (2020). Information and Communication Technology (ICT) as a source of development of states and regions in the age of globalization. Journal of Geography, Politics and Society, 10(1), 15–22.
4. Buhalis, D., & Leung, R. (2018). Smart hospitality—Interconnectivity and interoperability towards an ecosystem. International Journal of Hospitality Management *Volume 71*, pp 41-50.
5. Car, T., Pilepić, L., & Šimunić, S, M. (2019). Internet of things (IoT) in tourism and hospitality: opportunities and challenges, Tourism in Southern and Eastern Europe, Vol. 5, pp. 163-175

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume XII Issue VII July 2025

6. Castro, O, E, L., Deng, X., & Park, J, H. (2023). Comprehensive Survey on AI-Based Technologies for Enhancing IoT Privacy and Security: Trends, Challenges, and Solutions. Human-centric Computing and Information Sciences (2023) 13:39.
7. Iqbal, M. W., & Auwul, M. R. (2022). Internet of things (IoT) security and privacy concerns: An overview. Journal of Sensors, 2022, 5724168. https://doi.org/10.1155/2022/5724168
8. Dhirani, L, L., Armstrong, E., & Newe, T. (2021). Industrial IoT cyber threats and standards landscape: Evaluation and roadmap. Sensors, vol. 21, no. 11, pp 3901.
9. Lee. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management," Future Internet, vol. 12, no. 9, pp 157.
10. Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(5), pp 164–173. https://doi.org/10.4236/jcc.2015.35021
11. Magalhães, S. T., Magalhães, M. J., & Revett, K. (2016). Internet of Things for the hotel industry: A review. EAI Endorsed Transactions on Energy Web and Information Technologies, 14(2), e152285. https://doi.org/10.4108/eai.14-2-2017.152285
12. Mercan, S., Cain, L., Alonso, M., & Cobanoglu, C. (2021). Improving the service industry with hyper-connectivity: IoT in hospitality, International Journal of Contemporary Hospitality Management, Vol. 33 No. 1, Pp 243-262.
13. Pramanik, S., Pandey, D., Joardar, S., Niranjanmurthy, M., Pandey, B, K., & Kaur, J. (2023). n overview of IoT privacy and security in smart cities. *AIP Conf. Proc.* 2495, 020057.
14. Sen, R, K., & Dash, A. (2023). Unveiling the Shadows: Exploring the Security Challenges of the Internet of Things (IoT). International Journal of Scientific Research and Management (IJSRM).
15. Shani, S., Mohammed, M., Alhassan, S., & Awini, G. (2023). Internet of Things (IoTs) in the Hospitality Sector: Challenges and Opportunities, Advances in Information Communication Technology and Computing, Pp 67-81.
16. Srivastava, S., Ahmed, T., & Saxena, A. (2023). An Approach to Secure IoT Applications of Smart City Using Blockchain Technology. International Journal of Engineering Sciences and Emerging Technologies 11(2), pp 71-78.
17. Taherdoost, H. (2023). Security and internet of things: Benefits, challenges, and future perspectives. Electronics, 12(8), 1901. https://doi.org/10.3390/electronics12081901
18. Usman, M., Asim, M., Imran, M., & Vasilakos, A. V. (2023). IoT security challenges and emerging solutions: A comprehensive review. IEEE Access, 11(1).
19. Verma, A., Shukla, V. K., & Sharma, R. (2021). Convergence of IoT in tourism industry: A pragmatic analysis. Journal of Physics: Conference Series, 1714(1), 012037. https://doi.org/10.1088/1742-6596/1714/1/012037
20. Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2103-2115.