

Review Article

Adopting Internet of Things and Big Data Analytics for HACCP Monitoring: A TOE Framework-Based Analysis of Critical Success Factors and Challenges

Fatimah Azzahra' Misebah¹, Sarina Abdul Halim-Lim^{1*}, Syed Abdul Rahman Al-Haddad², Salini Devi Rajendran³

¹Department of Food Technology, Faculty of Food Science and Technology, Universiti Putra Malaysia, 43000 UPM Serdang, Selangor, Malaysia; gs66241@student.upm.edu.my

²Department of Department of Computer and Communication System Engineering, Faculty of Engineering, Universiti Putra Malaysia, 43000 UPM Serdang, Selangor, Malaysia; sar@upm.edu.my

³Taylor's Culinary Institute, Faculty of Social Sciences and Leisure Management, Taylor University, Malaysia; Salini.Rajendran@taylors.edu.my

*Corresponding author: Sarina Abdul Halim-Lim, Department of Food Technology, Faculty of Food Science and Technology, Universiti Putra Malaysia, 43000 UPM Serdang, Selangor, Malaysia; gs66241@student.upm.edu.my; sarinalim@upm.edu.my

Abstract: The integration of the Internet of Things (IoT) and Big Data Analytics (BDA) into Hazard Analysis and Critical Control Points (HACCP) monitoring presents significant opportunities for enhancing food safety and regulatory compliance in Malaysian food manufacturing SMEs. This study adopts the Technology-Organisation-Environment (TOE) framework to develop a conceptual model that identifies key factors influencing the adoption of IoT and BDA in HACCP monitoring. Through a literature review, critical success factors (CSFs) and challenges are categorised across three dimensions: technological, organisational, and environmental. Technological factors include technology infrastructure (H1), integration complexity (H2) and data security (H3), while organisational factors encompass IT expertise (H4), cost and expected benefits (H5), top management support (H6), and organisational readiness (H7). Environmental factors such as government policies (H8), supporting industry (H9), and competitive pressure (H10) also play a pivotal role. However, challenges such as data overload (C1), complexity of integration (C2), lack of expertise (C3), cybersecurity threats (C4), high implementation costs (C5), resistance to change (C6), bureaucratic procedures (C7) and lack of ecosystem support (C8) hinder successful adoption. By addressing these factors systematically, organisations can better plan, implement, and manage digital transformation in food safety monitoring. The proposed model serves as a foundation for future empirical studies and strategic decision-making in the digitalisation of HACCP monitoring systems.

Keywords: Internet of things; Big data analytics; Critical success factor; Challenges

Received: 7th July 2025

Accepted: 10th January 2026

Available Online: 10th July 2026

Published: 14th October 2026

Citation: Misebah, F. A., Halim-Lim, S. A., Al-Haddad, S. A. R., *et al.* Adopting Internet of Thing and Big Data Analytics for HACCP Monitoring: A TOE Framework-Based Analysis of Critical Success Factors and Challenges. *Adv Agri Food Res J* 2026; 7(2): a0000646. <https://doi.org/10.36877/aafrj.a0000646>.

1. Introduction

Food safety management systems (FSMS) are critical components for ensuring the quality and safety of food products that are enforced by food manufacturers globally (Liu *et al.*, 2022). According to the Malaysian Food Act 1983 (Act 281), food safety management is implemented to protect the public against health hazards and frauds in the preparation, sale, and use of food. Thus, to fulfil this mandate, the Food Hygiene Regulations of 2009 require all food manufacturing premises to establish and maintain a food safety assurance programme. This may be based on any recognised food safety system such as Hazard Analysis and Critical Control Points (HACCP), Good Manufacturing Practice (GMP) or International Organisation for Standardisation (ISO) 22000.

HACCP is a systematic approach that focuses on identifying and mitigating possible food safety hazards throughout the food manufacturing process, from raw ingredients to final products (Suherman, 2021). Recently, with the emergence of new technologies in the industry and the consequences of the pandemic, the implementation of FSMS was proposed to be embedded with digital innovation (Zhou *et al.*, 2022). An effective way to reduce food safety risks is by incorporating a risk-based strategy with a multidisciplinary approach and focusing on contamination prevention throughout food production. Thus, the rapid advancement of digital technologies across industries has created opportunities for researchers to investigate and apply Internet of Things (IoT) and Big Data Analytics (BDA) solutions to improve the effectiveness of FSMS. The IoT is a network of physical objects, including cars, homes, and other objects, that have sensors, software, and network connections built in (Vermessan & Friess, 2013). The main role of IoT is to collect various types of data from various devices that aim to improve efficiency, ease, and automation in industries including healthcare, transportation, and manufacturing (Mao & Zhang *et al.*, 2023; Pratap & Pendyala, 2022). Meanwhile, BDA refers to the use of advanced techniques such as machine learning (ML), data mining, and real-time analytics to analyse large volumes of data. According to Marjani *et al.* (2017), these two emerging technologies, IoT and BDA, complement each other and should be developed together. In Malaysia, Abbaco Controls, a Malaysian automation

company, has implemented an IoT and BDA-based water management system in rice fields that has the potential to improve national food production.

Thus, there is great potential for applying IoT and BDA within the HACCP system. In the context of HACCP, Critical Control Points (CCPs) must be monitored and controlled by establishing specific critical limits. Recently, there has been growing interest in using digital technologies to monitor CCPs, with several studies integrating IoT into HACCP monitoring. Real-time monitoring has become feasible, enabling the prompt identification and mitigation of potential food safety issues (Radu *et al.*, 2023; Fan *et al.*, 2022; Wang & Yue, 2017). Unfortunately, the implementation of IoT and BDA technologies in HACCP systems faces challenges due to their complexity and associated costs. Therefore, it is essential to identify and assess the challenges and critical success factors (CSFs) for the adoption of IoT and BDA within HACCP systems. Reviewing existing studies that focus on the CSFs and challenges of IoT and BDA will provide valuable guidance to managers seeking to implement these technologies in their organisations.

In this research, the Technology-Organisation-Environment (TOE) theoretical model was adopted to determine the CSFs. The TOE is a conceptual framework that helps organisations assess and analyse the various aspects that influence their ability to implement new technologies or strategies successfully (Siregar and Asvial, 2020). The original TOE framework was introduced by Tornatzky and Fleischer (1990), identifying three key elements that influence technology adoption: technology, organisation, and environment (Baker, 2012). The three elements technology, organisation, and environment will be used as categories to identify the key factors and challenges in implementing IoT and BDA in HACCP monitoring for SMEs. Technology elements refer to the internal and external characteristics of the technologies that are relevant to the organisation that can be evaluated by measuring the organisation's technology readiness, including adequacy of technology infrastructure, ease of system integration, and the robustness of data security measures. For the organisation, elements focus on the internal characteristics of the organisation that influence technology adoption and implementation that can be evaluated by examining internal capabilities such as top management support, overall organisational readiness and availability of resources of staff expertise. Meanwhile, the environmental elements involve external conditions that influence the organisation's decision in adopting new technologies that can be evaluated by analysing government policy requirements, supporting industry structure and competitive pressure. The specific factor for each element can vary depending on the technology and industry. Due to the limited empirical research that examines the TOE

elements within the context of IoT and BDA adoption, this study aims to review existing literature on IoT and BDA implementation using the TOE framework, with the intention of applying it to HACCP monitoring systems. Although previous studies have explored IoT and BDA adoption across various industries, research specifically addressing their integration into HACCP monitoring remains scarce. Furthermore, existing studies seldom combine the TOE framework with the specific challenges and critical success factors relevant to this setting. Additionally, prior literature lacks a comprehensive model that connects CSFs and challenges to guide SMEs in adopting IoT and BDA for food safety management.

2. Materials and Methods

Relevant research articles addressing IoT and BDA from theoretical, applied, and empirical perspectives were selected.

2.1. Stage 1: Planning the Review

In this stage, we identified research questions, developed a research strategy, and developed the review protocol that was used in addressing the objectives of this paper. The purpose of this review was to address the research question: What are the CSFs and challenges for integrating IoT with BDA in HACCP monitoring? The search strategy in this study was by performing a review based on a pre-defined search strategy to identify literature that was relevant to the research objective. The relevant academic databases Web of Science, IEEE Xplore and ScienceDirect were used in this study to determine the related articles. These databases were selected because they index high-quality, peer-reviewed publications and offer broad coverage across multidisciplinary fields including engineering, data analytics, food safety, and SME management. Their advanced search functions, citation tracking capabilities, and structured indexing contribute to the robustness and credibility of the literature review by ensuring comprehensive retrieval of relevant scholarly work and reducing selection bias. The keywords and Boolean operators (“IoT AND food safety,” “Big Data Analytics AND food safety”, “IoT AND TOE”, “Big data analytics AND TOE”) were used as a search strategy.

Despite their strength, reliance on these academic databases also presents limitations, for instance, some relevant materials such as industrial reports, government documents or practitioner insights may not be indexed in these platforms, potentially limiting practical perspective.

2.2. Stage 2: Screening

In this section, existing reviews, surveys, and technical research studies on the implementation of IoT and BDA technologies were examined to identify the CSFs based on the TOE framework. The TOE framework was selected for this research because it offers a comprehensive approach that integrates technological, organisational, and environmental dimensions. It is also widely adopted in prior studies, particularly due to its inclusion of the environmental context, which is often overlooked by models such as the Innovation Diffusion Theory (Amini & Bakri *et al.*, 2015). In this study, the three elements technology, organisation, and environment will serve as categories to identify key factors and challenges in implementing IoT and BDA in HACCP monitoring. These categories formed the foundation for developing hypotheses in subsequent sections. To determine suitable factors and challenges for adopting IoT and BDA in food safety management, Table 1 presents a compilation of relevant existing literature. Due to the limited integration of IoT and BDA in food manufacturing, this study will initially focus on factors related to IoT or BDA independently, or in any other relevant field, as part of a preliminary investigation. The challenges of adoption are discussed in detail in Section 3.1. To ensure the relevance and applicability of this chapter, the literature collections was limited to publications within the last 10 years. The literature selection includes papers relating to the CSFs of IoT and big data technology application in the TOE framework and the probable challenges. The literature collected is screened to validate the relevance and applicability of the literature content. Upon the literature screening, only fitting articles are used for this research. After screening, 13 articles were deemed relevant, and their full texts were reviewed to extract pertinent insights, which are presented in Tables 1 and 2.

2.3. Stage 3: Review and Reporting the Results

In this step, thematic analysis was conducted to identify patterns in the literature. This section synthesises the identified Critical Success Factors (CSFs) and challenges in implementing IoT and Big Data Analytics (BDA) categorised using the TOE framework. From the analysis, each CSF identified in the literature is labelled as H1-H10, corresponding to the specific technological, organisational, or environmental factor it represents. Likewise, each challenge is coded as C1-C8, reflecting the obstacles reported across studies.

3. Results

3.1. CSFs for IoT and BDA adoptions

From the review, previous research has identified ten influence elements within the TOE framework on the implementation of the IoT and BDA technology as shown in Table 1. Within technological factors, three elements were found to influence the adoption. First, technology infrastructure (H1) required strong infrastructure for the technology adoption (Ali Eltabey, 2023; Dave *et al.*, 2025; Ichsan & Dachyar, 2019; Siregar & Asvial, 2020). Then, technology integration (H2) and data security (H3) become another important element because the integration within old and new technology will result in different security and privacy systems that need to be considered, ensuring efficient adoption of IoT and BDA (Siregar & Asvial, 2020).

Meanwhile, under the organisation factor, four elements determined under this factor were IT expertise (H4), cost and benefit (H5), top management support (H6) and organisational readiness (H7). The availability of skilled personnel and adequate financial resources within an organisation plays a pivotal role in facilitating the adoption of IoT and BDA technologies (Dave *et al.*, 2025). Strong top management support, particularly through the recruitment of competent technical personnel responsible for system selection, installation, and maintenance, is essential for optimising processes and enhancing the overall efficiency of IoT and BDA adoption. Meanwhile, determination of organisational readiness in terms of budget resources and skilled workers is essential before adoption of technology can be decided (Dave *et al.*, 2025; Salman *et al.*, 2022; Urus *et al.*, 2024).

Then, environmental dimensions were identified with three key elements, that is, government policy (H8), supporting industries (H9), and competitive pressure (H10). These external factors will shape the broader ecosystem in which organisations operate. The organisation needs to consider government policies that establish the regulatory and strategic framework, which can either facilitate or hinder the adoption of IoT and BDA within the organisation (Ichsan & Dachyar, 2019). The presence of supporting industries such as technology vendors, service providers, and infrastructure partners will enable implementation by offering essential technical and operational support. Meanwhile, competitive pressure encourages organisations to adopt innovative technologies to maintain or enhance their market position (Dave *et al.*, 2025).

Table 1. Critical Success Factors (CSFs) in IoT and BDA implementation

Category	Factor	References	Key Findings
Technological	Technology Infrastructure (H1)	Siregar & Asvial (2020); Ichsan & Dachyar (2019); Dave <i>et al.</i> (2025); Ali Eltabey, (2023)	Strong infrastructure is key for technological adoption
	Technology Integration (H2)	Siregar & Asvial (2020)	Effective integration enhances system efficiency
	Data Security (H3)	Siregar & Asvial (2020); Salman <i>et al.</i> (2022); Dave <i>et al.</i> (2025)	Data security measures prevent system vulnerabilities
Organisational	IT Expertise (H4)	Siregar & Asvial (2020); Dave <i>et al.</i> (2025); Shah <i>et al.</i> (2019)	A skilled workforce is critical for IoT and BDA success
	Cost and Benefit (H5)	Siregar & Asvial (2020); Dave <i>et al.</i> (2025); Salman <i>et al.</i> (2022)	Sufficient budget is required to ensure successful of adoption
	Top Management Support (H6)	Siregar & Asvial (2020); Ichsan & Dachyar (2019); Dave <i>et al.</i> (2025); Shah <i>et al.</i> (2019); Salman <i>et al.</i> (2022)	Leadership commitment drives IoT and BDA adoption
Environmental	Organisational Readiness (H7)	Salman <i>et al.</i> (2022); Dave <i>et al.</i> (2025); Urus <i>et al.</i> (2024)	Readiness in terms of resources and skills is essential
	Government Policy (H8)	Siregar & Asvial (2020); Shah <i>et al.</i> (2019); Salman <i>et al.</i> (2022)	Supportive policies facilitate adoption
	Supporting Industry (H9)	Siregar & Asvial (2020); Shah <i>et al.</i> (2019)	Collaboration with tech providers accelerates adoption
	Competitive Pressure (H10)	Ichsan & Dachyar (2019); Siregar & Asvial (2020); Dave <i>et al.</i> (2025)	Market competition encourages innovation in IoT adoption

3.2.Challenges in IoT and BDA adoptions

Across the TOE categories, several key challenges identified hinder the integration of IoT and BDA, as shown in Table 2. Technologically, food manufacturing faces data overload (C1) where excessive data volume complicates processing (Donaghy *et al.*, 2021). Meanwhile, integration complexity due to diverse IoT and BDA components (C2) and cybersecurity (C3) threats jeopardises the adoption of IoT and BDA (Misra *et al.*, 2020; Urus *et al.*, 2024). Meanwhile, the organisational challenges include a lack of expertise and trained personnel to manage IoT and BDA systems (C4) have been identified (Selamat *et al.*, 2019;

Urus *et al.*, 2024). Moreover, high implementation costs (C5) are due to the cost of the sensor and data analytics system that limit adoption (Misra *et al.*, 2020). Resistance to change (C6), as top management that responsible in decision making within organisation refuses to adapt to digitalisation changes (Selamat *et al.*, 2019). From an environmental perspective, bureaucratic procedures (C7) slow down adoption of this technology (Donaghy *et al.*, 2021). While a lack of ecosystem support (C8), including insufficient external assistance and industry collaboration, further constrains successful implementation (Urus *et al.*, 2024).

Table 2. Challenges in IoT and BDA implementation

Category	Challenges	References	Key Findings
Technological	Data Overload (C1)	Donaghy <i>et al.</i> (2021)	Excessive data volume complicates processing
	Complexity of Integration (C2)	Rikalovic <i>et al.</i> (2021)	SMEs struggle with integrating various IoT components
	Cybersecurity Threats (C3)	Selamat <i>et al.</i> (2019); Misra <i>et al.</i> (2020); Tao <i>et al.</i> (2021); Urus <i>et al.</i> , (2024)	Cyber threats pose risks to data
Organisational	Lack of Expertise (C4)	Selamat <i>et al.</i> (2019); Urus <i>et al.</i> , (2024)	Lack of trained professionals for IoT and BDA implementation
	High Implementation Costs (C5)	Selamat <i>et al.</i> (2019); Misra <i>et al.</i> (2020)	Cost-effective of sensors and data analytics impacted the adoption of IoT and BDA
	Resistance to Changes (C6)	Selamat <i>et al.</i> (2019)	Top management sceptical with digital transformation
Environmental	Bureaucratic Procedures (C7)	Donaghy <i>et al.</i> (2021)	Regulatory complexities slow down IoT adoption
	Lack of Ecosystem Support (C8)	Urus <i>et al.</i> (2024)	Limited external support hinders implementation

4. Discussion

4.1. CSF for IoT and BDA Adoptions in HACCP Monitoring

4.1.1. Technological factors

The TOE framework aids in evaluating the technological components involved in the implementation of IoT and BDA systems. This aspect plays a critical role in influencing the adoption of IoT and BDA among SMEs (Maroufkhani *et al.*, 2023). From the previous result, technology infrastructure (H1) becomes an important element in the technological factor, which includes IoT sensor technologies and data transmission protocols. Sensor integration refers to the incorporation of various sensors for monitoring critical control points (CCP) in the HACCP system such as temperature, humidity, and pH levels in food processing environments (Radogna *et al.*, 2022). Meanwhile, the data transmission factor involves selecting appropriate protocols and technologies for efficient and reliable transmission of data from IoT devices to central systems (Landaluce *et al.*, 2020). This element is essential for adopting IoT and BDA within HACCP monitoring, as selecting the appropriate technological components enables real-time monitoring and timely alerts to relevant authorities whenever deviations are detected. Additionally, technology support entails providing organisations with the necessary resources and expertise to set up, manage, and address challenges related to the technology infrastructure during IoT and BDA implementation (Shah *et al.*, 2019).

Technology integration (H2) focuses on ensuring seamless connectivity with existing HACCP monitoring systems and IT infrastructure to prevent duplication of efforts and enhance interoperability. IoT system has made it much easier to monitor and control the CCP system from a distance. When companies use IoT systems that follow common standards, everything becomes more open and easier to connect. This helps different devices and systems work well together. It also makes the system safer, more reliable, and easier to maintain. Developers can add new features more easily, and the system can connect with other company tools without difficulty. Overall, using open and standard IoT systems makes monitoring and controlling processes simpler, safer, and more flexible (Biscotti *et al.*, 2020).

Data security (H3) is a critical aspect of adopting IoT and BDA in the HACCP monitoring system. Implementing end-to-end encryption ensures that data is securely encrypted from the point of generation (IoT device) to its destination (BDA platform or storage). Strong encryption algorithms and effective key management practices are essential to protect data from unauthorised access or interception. Encrypting data both in transit and at rest further safeguards it against interception during transmission and unauthorised access

when stored in databases or cloud repositories. Secure protocols such as Transport Layer Security (TLS) and Advanced Encryption Standard (AES) are widely used to protect data in transit and at rest, respectively. Role-Based Access Control (RBAC) allows organisations to define and enforce detailed access policies based on users' roles and privileges, ensuring that only authorised individuals or systems can access sensitive data and perform specific actions within IoT and BDA environments. Multi-Factor Authentication (MFA) adds an extra layer of security by requiring users to provide multiple forms of verification (e.g., passwords, biometrics, One-Time Passwords (OTPs)) to access IoT devices, BDA platforms, or data repositories. This reduces the risk of unauthorised access due to compromised credentials or identity theft. Additionally, digital signatures and cryptographic hashing techniques can be used to verify the authenticity and integrity of data by generating unique identifiers (signatures or hashes) based on the data's content. Any unauthorised modification or tampering alters the signature or hash, alerting stakeholders to potential security breaches. Data Loss Prevention (DLP) solutions also play a crucial role by monitoring and controlling data movement within IoT and BDA environments, preventing unauthorised data exfiltration or leakage. DLP enforces policies and detects anomalous activities, safeguarding sensitive data from accidental or malicious exposure. Establishing robust data governance frameworks and compliance programs ensures that organisations adhere to industry regulations and internal policies governing data security and privacy. Regular audits, risk assessments, and compliance monitoring help identify and mitigate data security risks proactively while ensuring CCP monitoring data is safely stored. By addressing these data security factors comprehensively, organisations can reduce risks, protect sensitive information, and ensure the confidentiality, integrity, and availability of data within IoT and BDA ecosystems. Proactive security measures not only defend against cyber threats but also build trust among users and stakeholders, promoting the responsible and ethical use of data-driven technologies.

4.1.2. Organisational factors

In the organisational context, technology support from IT experts (H4) entails providing organisations with the necessary resources and expertise to set up, manage, and address challenges related to the technology infrastructure during IoT and BDA implementation. The availability of expertise in operating IoT and BDA within the organisation is crucial to ensure the system is operating efficiently in monitoring of CCP.

Additionally, costs and benefits (H5) are another crucial element in the decision to implement IoT and BDA systems within CCP monitoring in the HACCP system. The upfront

costs can be substantial, including expenses for hardware installation, software development, data storage infrastructure, and hiring skilled personnel. Additionally, there are ongoing costs related to maintenance, upgrades, and security. However, these technologies offer significant benefits by enabling organisations to gather and analyse vast amounts of data in real-time, which leads to improved decision-making, operational efficiency, and cost savings. The benefits may include better predictive maintenance, enhanced customer experience, optimised supply chain management, and new revenue streams through data monetisation.

Top management support (H6) is essential for the successful adoption of IoT and BDA within an organisation. Executives must understand the strategic importance of these technologies and be willing to allocate the necessary financial and human resources for implementation. Leadership from top management can also help align the adoption of IoT and BDA with the organisation's overall goals, providing direction and overcoming resistance to change. Their endorsement ensures that these initiatives receive the attention and prioritisation needed for success (Siregar & Asvial, 2020; Ichsan & Dachyar, 2019; Dave *et al.*, 2025; Shah *et al.*, 2019; Salman *et al.*, 2022).

Assessing organisational readiness (H7) is essential for adopting IoT and BDA. This involves examining whether existing systems, networks, and data storage infrastructure can support these technologies. Successful implementation also depends on having a workforce with skills in data analytics, cybersecurity, and IoT device management. Organisations may need to provide training or hire specialists to fill these skill gaps. For instance, quality personnel responsible for CCP monitoring will require training in calibrating IoT sensors and managing data in BDA systems, while IT staff must be equipped to maintain the overall system. Additionally, organisational culture strongly influences the success of technology adoption. Cultivating a culture that encourages innovation, experimentation, and data-driven decision-making is crucial, along with implementing effective change management strategies to address employee concerns and support the transition.

4.1.3. Environmental factors

In the environmental factors, government policies (H8) play a crucial element in ensuring compliance with regulatory requirements and standards related to food safety and data privacy in environments where HACCP monitoring is conducted. Governments may also provide incentives, subsidies, or funding programs to encourage the adoption of IoT and BDA technologies. These initiatives could include research grants, tax credits for technology

investments, or subsidies for infrastructure development, particularly in sectors like smart cities or healthcare.

In addition, a supportive industry (H9) ecosystem is vital. The availability of reliable technology providers offering IoT platforms, analytics software, and related services is essential for successful adoption. A strong ecosystem of vendors and solution providers gives organisations various options to meet their specific needs and preferences (Siregar & Asvial, 2020; Shah *et al.*, 2019). Operational factors, such as the conditions in food processing environments like temperature fluctuations and exposure to contaminants, must also be evaluated, as these can impact the performance of IoT devices. Standards like MQTT (Message Queuing Telemetry Transport) for IoT communication or JavaScript Object Notation (JSON) for data interchange help ensure integration and interoperability across diverse systems and devices.

Moreover, competitive pressures (H10) push organisations to adopt IoT and BDA to maintain a competitive edge. Companies that fail to embrace these technologies risk falling behind competitors who use data-driven insights to improve efficiency, enhance customer experience, and drive innovation. As customer expectations evolve, businesses must leverage IoT and BDA to deliver personalised, seamless, and connected experiences across various channels. Customer-centric organisations that use data to anticipate needs, personalise offerings, and provide superior service gain a clear competitive advantage. Organisations must effectively navigate these external factors to capitalise on the opportunities these transformation technologies offer and maintain competitiveness in an increasingly data-driven market.

4.2. Challenges in IoT and BDA Adoptions in HACCP Monitoring

However, adoption of IoT and BDA in HACCP monitoring is not without challenges. A few challenges have been determined by previous researchers. From a technological standpoint, the implementation of IoT and BDA in HACCP monitoring encounters three main challenges. Firstly, data overload (C1) becomes the main challenge, where the large volume of data generated, structured and unstructured from CCP monitoring activity becomes difficult to process and manage effectively. There is also the complexity of integration (C2), as connecting and synchronising diverse IoT and BDA components often exceeds the technical capacity of an organisation. In addition, cybersecurity threats (C3) remain a major concern, with vulnerabilities in IoT devices and data systems posing significant risks to sensitive operational and safety data.

From an organisational perspective, lack of expertise (C4) becomes another obstacle need to overcome, as they often do not have personnel trained particularly in IoT device management, data analytics, or cybersecurity. There are also high implementation costs (C5) that discourage adoption, as the affordability of sensors, data storage, and analytics tools directly affects willingness to invest in IoT and BDA systems. There is also needed in modifying food manufacturing infrastructure to support the deployment of IoT and BDA may necessitate expertise in data science, which can pose challenges for organisations. Furthermore, resistance to change (C6) persists, with top management in some organisations remaining sceptical or hesitant toward digital transformation, thereby slowing down adoption efforts. Leadership and commitment from top management are crucial for driving digital transformation within the organisation.

Within the environmental category, organisations encounter bureaucratic procedures (C7), where stringent or complex regulations create delays in implementing new IoT and BDA systems. Regulatory uncertainty surrounding IoT, data privacy, and food safety further complicates the adoption of these technologies among HACCP-certified organisations. Compliance with industry-specific standards when implementing IoT and BDA also poses a significant challenge that needs to be overcome.

Additionally, a lack of ecosystem support (C8), including limited guidance from government agencies, technology providers, and industry partners, further restricts HACCP certified organisation from effectively implementing IoT and BDA solutions in some regions could impede adoption when the end users usually have no experience in handling this technology that other service providers need.

The challenge mentioned before may vary depending on the country and size of the business, including both large companies and Small and Medium Enterprises (SMEs). Large companies may have more advantages in adopting IoT and BDA compared to SMEs that have limited resources. SMEs may face limitations of adoption IoT and BDA when needed of additional infrastructure for adopting IoT and BDA. There is a high cost of implementation where IoT devices, sensors and data analytic platform can be expensive for SMEs to implement. Regarding the security aspect, SMEs are also facing cyber-attacks due to outdated database management, insecure hardware and software, which became main challenges that need to be tackled by SMEs. Additionally, regulatory uncertainty surrounding IoT, data privacy, and food safety further complicates the adoption of these technologies among SMEs. Together, these challenges highlight the multifaceted barriers SMEs must address to fully leverage IoT and BDA in their operations.

4.3. Proposed Conceptual Model

Based on the findings of this study, the research adopts the theoretical TOE framework in the proposed conceptual model (Figure 1). By considering the detailed critical success factors and challenges identified in the previous section, organisations can more effectively plan, implement, and manage the adoption of IoT and BDA in HACCP monitoring, thereby enhancing food safety and regulatory compliance.

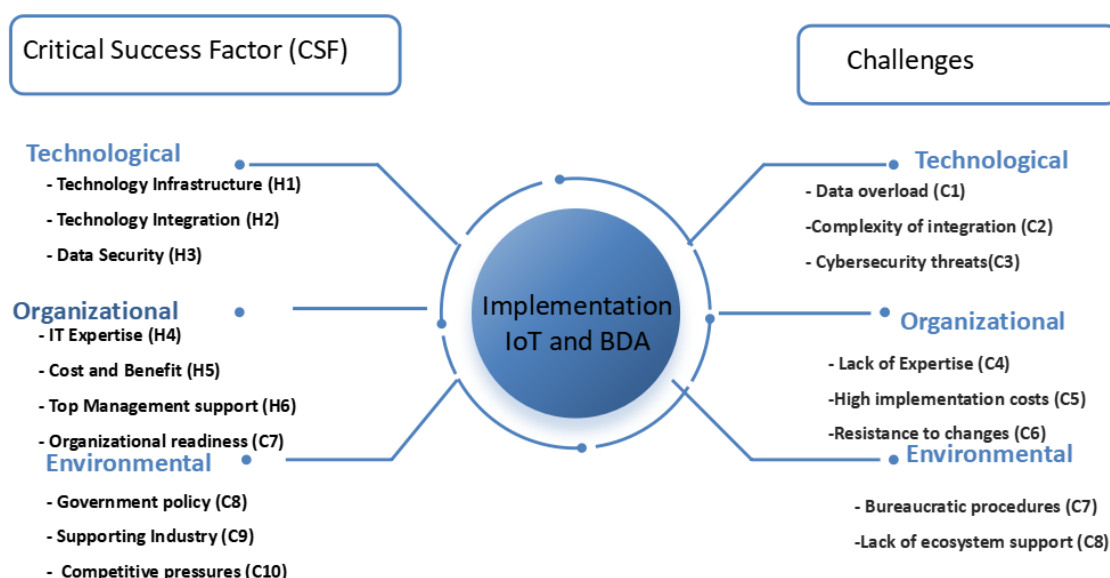


Figure 1. Proposed conceptual model

The model (Figure 1) illustrates how the CSFs and challenges interact to influence the successful implementation of IoT and BDA in HACCP monitoring. On the left side, the CSFs represent the enablers that support adoption, while the right side shows the barriers that may hinder progress. In practice, these two sides operate simultaneously. Under the technological dimension, strong technology infrastructure, effective system integration, and robust data security (H1–H3) enable food manufacturing to implement IoT and BDA smoothly. However, these must counterbalance challenges such as data overload, integration complexity, and cybersecurity threats (C1–C3). For example, even if an SME has good infrastructure, the lack of proper integration or secure systems can slow down implementation.

In the organisational dimension, factors such as IT expertise, cost and benefit, top management support, and readiness (H4–H7) act as internal strengths that drive adoption of IoT and BDA in HACCP monitoring. But these must overcome internal barriers such as lack of expertise, high costs of implementation, and resistance to change (C4–C6). For instance,

having supportive top management (H6) can help reduce resistance to digital transformation (C6), while investing in staff training supports readiness (H7) and mitigates expertise gaps (C4).

Meanwhile, the environmental dimension involves external influences, including government policy, supporting industry, and competitive pressure (H8–H10). These external drivers often motivate SMEs to adopt new technologies. However, challenges such as bureaucratic procedures and limited ecosystem support (C7–C8) can slow down adoption despite these pressures. For example, strong government incentives (H8) can encourage adoption, but complex regulatory procedures (C7) may delay IoT and BDA system approvals.

Overall, the model shows that successful IoT and BDA implementation requires balancing the enablers with the challenges across all three dimensions. CSFs push SMEs toward adoption, while the challenges highlight the obstacles that must be managed carefully in real-world implementation.

5. Conclusions

A conceptual framework of TOE in the adoption of IoT and BDA in HACCP monitoring has been proposed, which is to be equipped with variables and indicators that affect the adoption of this digital technology. Identified CSF from this paper includes technological factors, comprising technology infrastructure (H1), integration complexity (H2) and data security (H3), while organisational factors encompass IT expertise (H4), cost and expected benefits (H5), top management support (H6), and organisational readiness (H7). Environmental factors such as government policies (H8), supporting industry (H9), and competitive pressure (H10) also play a pivotal role. However, challenges such as data overload (C1), complexity of integration (C2), lack of expertise (C3), cybersecurity threats (C4), high implementation costs (C5), resistance to change (C6), bureaucratic procedures (C7) and lack of ecosystem support (C8) hinder successful adoption. By addressing these factors systematically, organisations can better plan, implement, and manage digital transformation in food safety monitoring. The proposed model serves as a foundation for future empirical studies and strategic decision-making in the digitalisation of HACCP monitoring systems.

5.1. Future study

The proposed model serves as a foundation for future empirical studies and strategic decision-making in the digitalisation of HACCP monitoring systems. Therefore, our further work will focus on an empirical study by the adoption of Analytical Hierarchy Process and

the Decision Making Trial and Evaluation Laboratory (AHP- DEMATEL) method, which will be used to rank and relate between CSF and challenges in the implementation of IoT and BDA in HACCP monitoring. The AHP-DEMATEL method is applied when multiple criteria and alternatives need to be considered to achieve an objective, and a deep understanding of the interrelationships between factors is required. Integrating AHP and DEMATEL provides a comprehensive evaluation framework. AHP quantifies the weights of CSFs and challenges, while DEMATEL visualises and measures their interconnections. This is especially relevant for complex, multi-dimensional contexts like technology adoption, where factors may not only differ in importance but also influence each other in cascading ways. By applying the AHP-DEMATEL method, the study can prioritise CSFs and challenges while simultaneously identifying the key drivers and interdependent relationships among TOE factors, supporting more informed decision-making and strategy formulation. An empirical study by survey will be designed to validate the relative importance and causal relationships of TOE-CSFs and challenges identified in the literature and expert analysis. Managers, technical officers, and decision-makers in Malaysian food manufacturing SMEs who are involved in food safety management or technology adoption. Combining weights from AHP with causal insights from DEMATEL will provide a holistic understanding of priorities and interdependencies. The expected outcome will achieve actionable recommendations for SMEs to focus on the most influential CSFs and challenges that need to be overcome under each TOE dimension for successful IoT and BDA implementation in HACCP monitoring.

Supplementary Materials: All materials included in the manuscript

Author Contributions: Conceptualisation, F.A.M. and S.A.H.L.; methodology, F.A.M.; software, S.A.H.L.; validation, S.A.H.L.; formal analysis, F.A.M.; investigation, F.A.M.; resources, S.A.H.L.; data curation, S.A.H.L. and S.A.R; writing original draft preparation, F.A.M.; writing review and editing, S.A.H.L., S.A.R and S.A.D.

Funding: This research was funded by the Fundamental Research Grant Scheme, Ministry of Higher Education (MOHE) through Universiti Putra Malaysia, grant number (FRGS/1/2022/SS02/UPM/02/1).

Acknowledgements: Not Available

Conflicts of Interest: The authors declare no conflict of interest.

References

- Ali Eltabey, R. (2023). Utilizing digital technologies to ensure food safety. *International Journal of Artificial Intelligence and Emerging Technology*, 6(2), 42–65. <https://doi.org/10.21608/ijalet.2024.275187.1007>
- Amini, M., Bakri, A. (2015). Cloud computing adoption by SMEs in Malaysia: A multi-perspective framework based on DOI theory and TOE framework. *Journal of Information Technology & Information Systems Research (JITISR)*, 9(2), 121–135. <https://ssrn.com/abstract=2841175>
- Baker, J. (2012). The technology–organization–environment framework. In Y. K. Dwivedi, M. Wade, & S. L. Schneberger (Eds.), *Information Systems Theory: Explaining and Predicting Our Digital Society* (pp. 231–245). Springer. https://doi.org/10.1007/978-1-4419-6108-2_12

- Biscotti, A., Giannelli, C., Keyi, C. F. N., *et al.* (2020). Internet of things and blockchain technologies for food safety systems. In *2020 IEEE International Conference on Smart Computing (SMARTCOMP)* (pp. 440–445). IEEE. <https://doi.org/10.1109/SMARTCOMP50058.2020.00091>
- Dave, H., Ahmad, S., Panghal, A., *et al.* (2025). Mapping the critical factors of IoT implementation in the food industry. *Sustainable Food Technology*, 3(1), 263–276. <https://doi.org/10.1039/d4fb00274a>
- Donaghy, J. A., Danyluk, M. D., Ross, T., *et al.* (2021). Big data impacting dynamic food safety risk management in the food chain. *Frontiers in Microbiology*, 952. <https://doi.org/10.3389/fmicb.2021.668196>
- Fan, M., Liu, S., Xu, L., *et al.* (2022). Credible pigeon permissioned blockchain traceability platform integrated with IoT based on HACCP. *Scientific Reports*, 12(1), 22363. <https://doi.org/10.1038/s41598-022-27065-2>
- Ichsan, M., Dachyar, M. (2019). Readiness for implementing industry 4.0 in food and beverage manufacturer in Indonesia. In *IOP Conference Series: Materials Science and Engineering*, 598(1), 012129. IOP Publishing. <https://iopscience.iop.org/article/10.1088/1757-899X/598/1/012129>
- Landaluce, H., Arjona, L., Perallos, A., *et al.* (2020). A review of IoT sensing applications and challenges using RFID and wireless sensor networks. *Sensors*, 20(9), 2495. <https://doi.org/10.3390/s20092495>
- Liu, N., Bouzembrak, Y., Van den Bulk, L. M., *et al.*, (2022). Automated food safety early warning system in the dairy supply chain using machine learning. *Food Control*, 136, 108872. <https://doi.org/10.1016/j.foodcont.2022.108872>
- Mao, Z., Zhang, Q. (2023). Application Process Design of Digital Quality Monitoring and Traceability System for Fresh Agricultural Products. *Digitalization and Management Innovation* (pp. 34–42). IOS Press. <https://ebooks.iospress.nl/doi/10.3233/FAIA230005>
- Marjani, M., Nasaruddin, F., Gani, A., *et al.* (2017). Big IoT data analytics: Architecture, opportunities, and open research challenges. *IEEE Access*, 5, 5247–5261. <https://doi.org/10.1109/ACCESS.2017.2689040>
- Maroufkhani, P., Iranmanesh, M., Ghobakhloo, M. (2023). Determinants of big data analytics adoption in small and medium-sized enterprises (SMEs). *Industrial Management & Data Systems*, 123(1), 278–301. <https://doi.org/10.1108/IMDS-11-2021-0695>
- Misra, N. N., Dixit, Y., Al-Mallahi, A., *et al.*, (2020). IoT, big data, and artificial intelligence in agriculture and food industry. *IEEE Internet of Things Journal*, 9(9), 6305–6324. <https://doi.org/10.1109/JIOT.2020.2998584>
- Pratap, E. V., Pendyala, S. (2022). Supply chain management using IoT-A comprehensive review. *Journal of Positive School Psychology*, 412–418. <https://journalppw.com/index.php/jpsp/article/view/6921/4519>
- Radogna, A. V., Latino, M. E., Menegoli, M., *et al.* (2022). A Monitoring Framework with Integrated Sensing Technologies for Enhanced Food Safety and Traceability. *Sensors*, 22, 6509. <https://doi.org/10.3390/s22176509>
- Radu, E., Dima, A., Dobrota, E., *et al.* (2023). Global trends and research hotspots on HACCP and modern quality management systems in the food industry. *Heliyon*, 9(7). <https://doi.org/10.1016/j.heliyon.2023.e18232>
- Rikalovic, A., Suzic, N., Bajic, B., *et al.* (2021). Industry 4.0 implementation challenges and opportunities: A technological perspective. *IEEE Systems Journal*, 16(2), 2797–2810. <https://doi.org/10.1109/JSYST.2021.3101673>
- Salman, M. S., Sani, M. K. J. A., Sahid, N. Z., *et al.*, (2022). Assessing the big data analytics readiness based on technology-organization-environment (TOE) framework of Malaysian libraries. Descriptive

- Analysis. *International Journal of Academic Research in Progressive Education and Development*, 11(2), 1465–1484. <http://dx.doi.org/10.6007/IJARPED/v11-i2/13903>
- Selamat, S. A. M., Prakoonwit, S., Sahandi, R., *et al.* (2019). Big Data and IoT Opportunities for Small and Medium-Sized Enterprises (SMEs). In *Handbook of Research on Big Data and the IoT*, pp 77–88. IGI Global. <http://dx.doi.org/10.4018/978-1-5225-7432-3.ch005>
- Shah, S. A., Seker, D. Z., Hameed, S., *et al.* (2019). The rising role of big data analytics and IoT in disaster management: recent advances, taxonomy and prospects. *IEEE Access*, 7, 54595–54614. <https://doi.org/10.1109/ACCESS.2019.2913340>
- Siregar, K. L., Asvial, M. (2020). Analysis of IoT implementation using the dematel method and TOES framework. In *2020 3rd International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT)* (pp. 19–23). IEEE. <https://doi.org/10.1109/MECnIT48290.2020.9166602>
- Suherman, S., Janitra, A. A., Budhiary, K. N. S., *et al.* (2021). Review on hazard analysis and critical control point (HACCP) in the dairy product: Cheese. In *IOP Conference Series: Materials Science and Engineering*, 1053(1), 012081. IOP Publishing. <http://dx.doi.org/10.1088/1757-899X/1053/1/012081>
- Tao, Q., Ding, H., Wang, H., *et al.* (2021). Application research: Big data in food industry. *Foods*, 10(9), 2203. <https://doi.org/10.3390/foods10092203>
- Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington, MA: Lexington Books.
- Urus, S. T., Rahmat, F., Othman, I. W., *et al.* (2024). Application of the technology-organization-environment framework on big data analytics deployment in manufacturing and service. *Asia-Pacific Management Accounting Journal*, 19(2), 57–92. <https://www.doi.org/10.24191/APMAJ.V19i2-04>
- Vermesan, O., Friess, P. (Eds.). (2013). *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. River Publishers.
- Wang, J., Yue, H. (2017). Food safety pre-warning system based on data mining for a sustainable food supply chain. *Food Control*, 73, 223–229. <https://doi.org/10.1016/j.foodcont.2016.09.048>
- Zhou, Q., Zhang, H., Wang, S. (2022). Artificial intelligence, big data, and blockchain in food safety. *International Journal of Food Engineering*, 18(1), 1–14. <https://doi.org/10.1515/ijfe-2021-0299>

