

A CONCEPTUAL BUSINESS MODEL FOR SAFESPHERE: ADVANCING SMART HOME SECURITY SYSTEMS

ARINA BATRISYIA SOBHAN BINTI MOHD RAZALI¹, NUR JANNAH NAI'MAH BINTI ZAINAL^{2*}, NURIZZATI INSYIRAH BINTI MOHD NAZIM³, NADHIRAH BINTI MUHAMMED NAJMUDDIN⁴, ABDUL RAHMAN AHMAD DAHLAN⁵

^{1,2,3,5}Department of Information System, ⁴Department of Computer Science, Kulliyah of Information and Communication Technology, International Islamic University Malaysia, Gombak, Malaysia

*Corresponding author: njnnaimah@gmail.com

ABSTRACT: The goal of this paper is to present a conceptual SafeSphere Smart Home Security System business model embedded within a digital platform aligned with the United Nations Sustainable Development Goals (SDG). Although smart home technologies are expanding, adoption remains limited due to ecosystem fragmentation and multiple device communication protocols that complicate integration for users. To address this, the SafeSphere model proposes a smart home gateway that acts as a unified hub to manage diverse protocols, enhancing device interoperability and simplifying user experience. The value proposition centres on safety, convenience and compatibility through features such as AI-powered intrusion detection, PDPA-compliant local data storage and centralized control of cameras and locks via a single mobile application. Guided by the principle of Rahmatan lil 'Alamin, SafeSphere aims to promote universal well-being by offering accessible security solutions for all communities. The business model includes affordable and scalable packages for B40 and M40 households to encourage wider adoption and reduce digital inequality. The gateway approach also provides a standardized communication layer that benefits both users and hardware providers. The purpose of this paper is to develop an initial business model and platform that address the key challenges, pains and desired gains of four main customer segments: homeowners, small businesses operators, schools institutions and hardware providers. The initiative aligned with SDG 9 (Industry, Innovation and Infrastructure), SDG 11 (Sustainable Cities and Communities) and SDG 16 (Peace, Justice and Strong Institutions), by promoting secure digital innovation and strengthening digital trust. The paper adopts the Design Thinking (DT) methodology to understand user pain points and generate innovative solutions. Business modelling tools such as the Business Model Canvas (BMC), Value Proposition Design Canvas (VPC) and Environmental Map (EM) are used to conceptualize and evaluate the proposed business model.

KEY WORDS: Smart home security, Internet of Things (IoT), Data sovereignty, Business Model Canvas (BMC), B40 and M40

1. INTRODUCTION

In the age of digital transformation, where cities aim to become “smart” and every device communicates through data, the twenty-first century is witnessing a blend between technology and daily life that is reshaping how people live, work and

protect their homes. The Fourth Industrial Revolution (4IR) has introduced technologies such as the IoT and AI that have revolutionized how individuals interact with their environments. In Malaysia, the increasing crime index from 50,813 cases in 2022 to 52,444 in 2023, with 41,991 property crimes reported has been one of the key factors driving the adoption of smart home technologies (Department of Statistics Malaysia, 2024). As Ab-Rahman and Razaly (2012, as cited in Mokhtar & Ismail, 2018) stated “home surveillance systems can be used to keep up with the increasing rate of crime” (p. 9).

Globally, the smart home security market was estimated at approximately USD 33.94 billion in 2024 and is projected to reach around USD 82.07 billion by 2030, growing at about 15.2% (Grand View Research, 2025). However, while these technologies promise convenience, they also expose vulnerabilities particularly in terms of data privacy and interoperability. The growing adoption of smart devices has led to diverse and uncoordinated ecosystems, forcing users to manage multiple applications and hubs that often fail to integrate seamlessly (Kam et al., 2023).

In Malaysia, security and interoperability remain fundamental challenges. The market is still dominated by imported smart home solutions that are costly and poorly adapted to local needs. These challenges highlight the need for a unified smart home platform that prioritizes safety and data sovereignty. The national agenda supports this direction under the 13th Malaysia Plan (2026-2030) that emphasises digital infrastructure, data governance and ICT-enabled growth (Ministry of Economy, 2025). Moreover, the recently tabled Malaysia Budget 2026 reinforced the government’s commitment by allocating resources to digital infrastructure, sovereign AI cloud services and 5G expansion (AmInvestment Bank Berhad, 2025). These figures highlight not only the urgent need for property protection but also the need for a centralized smart security hub that can unify multiple devices and protocols under one reliable platform.

To address this gap, the SafeSphere Smart Home Security Ecosystem is conceptualized as a next-generation hub that bridges compatibility across diverse smart home devices. SafeSphere serves as a central gateway capable of handling protocols such as ZigBee, Wi-Fi and Bluetooth allowing cameras, sensors, alarms and smart locks to operate through a single platform. This approach reduces complexity for users by replacing multiple apps with a single interface. Built with AI-driven motion recognition, IoT connectivity and locally hosted cloud services, SafeSphere ensures both technological efficiency and compliance with Malaysia’s Personal Data Protection Act (PDPA). In the spirit of *rahmatan lil’ alamin*, SafeSphere is designed not only as a commercial venture but as a contributor to safer, more inclusive communities, ensuring that B40 and M40 households also have equitable access to smart security technology. SafeSphere promotes trust and digital responsibility, reflecting the ethical vision of serving humanity and safeguarding communities in a sustainable way.

The MyMukim2Cloud initiative illustrates how integrated platforms can improve service delivery by consolidating data, improving security and streamlining processes across multiple stakeholders through a Whole-of-Government (WoG) approach (Saleh et al., 2013). This demonstrates that Malaysia benefits greatly from centralized systems built on shared databases, coordinated infrastructure and interoperability which are the principles that similarly guide the development of SafeSphere.

The key customer segments include homeowners, small businesses, schools and hardware providers. For homeowners, the central job-to-do involves protecting family members and property through real-time monitoring but face challenges such as complex installation, high costs and privacy concerns. Furthermore, small business owners need reliable monitoring and access control for safety. Lastly, hardware providers aim to expand their market reach by integrating compatible smart devices through SafeSphere's ecosystem that can reduce distribution costs and enhance brand credibility.

Current solutions in the marketplace such as Eufy and Hive offer remote access, smart doorbells and motion sensors but rely heavily on international cloud servers, which raises concerns regarding the Personal Data Protection Act (PDPA) compliance and limits consumer control over their own data. Furthermore, they exhibit limitations in terms of affordability, local data hosting and system interoperability, thereby creating a gap in the Malaysian market (Kam et al., 2023). SafeSphere aims to address these gaps by providing a unified gateway architecture that improves reliable smart living.

Ultimately, SafeSphere is introduced as a practical response to current security and integration challenges, offering a reliable system that supports safer and more connected living environments across Malaysia. This platform reflects Malaysia's aspiration for a secure and digitally empowered society in line with the National 4IR Policy and MyDigital Blueprint 2030.

2. PROBLEM STATEMENT/OBJECTIVES

Growing concerns over safety in Malaysia underscore a critical demand for an integrated, secure, and locally optimized smart security ecosystem across several key customer segments. Homeowners increasingly struggle with fragmented smart home systems that lack interoperability, leading to unreliable surveillance, complex management, and privacy risks due to dependence on foreign cloud servers (Kam et al., 2023). Concurrently, small business operators face challenges related to affordability and scalability when adopting smart security systems needed to protect assets and ensure workplace safety, particularly as property crimes rose to 41,991 cases in 2023 (Department of Statistics Malaysia, 2024). Meanwhile, schools institutions are under immense pressure to significantly strengthen student and staff safety following several tragic incidents that exposed weaknesses in surveillance, supervision, and emergency response within educational institutions including the fatal stabbing of a 16-year-old student in Bandar Utama and the death of a 10-year-old student in a school toilet (The Straits Times, 2025). Furthermore, hardware providers encounter barriers in integrating their diverse devices into unified ecosystems, which limits their market reach and compatibility with emerging smart security platforms. Collectively, these pain points highlight a significant gap in the national security technology landscape, a lack of trusted, interoperable, and locally governed solutions that ensure safety, privacy and seamless user experience across all segments (Smart Home Security Market (2025-2030), n.d.). These challenges reflect a nationwide demand for technology-driven yet accessible security infrastructure that aligns with Malaysia's Personal Data Protection Act (PDPA) and national digitalization agenda (Ministry of Economy, 2025).

The objective of this paper is to develop a conceptual business model for SafeSphere, a unified smart security ecosystem and mobile application designed to address Malaysia's urgent need for safer and smarter environments. SafeSphere seeks to integrate IoT-enabled devices such as cameras, alarms, and smart locks into a single, user-friendly interface that provides real-time monitoring, AI-assisted anomaly detection, and locally hosted cloud storage to ensure PDPA compliance. The platform aims to deliver tailored value to each customer segment: empowering homeowners with simple, privacy-conscious home protection; supporting rental property owners and SMEs with affordable, scalable security; enhancing schools' ability to monitor large areas and respond quickly to emergencies; and enabling hardware providers to integrate and market compatible devices within an interoperable ecosystem. Ultimately, SafeSphere aspires to create a sustainable and inclusive smart security solution that reinforces trust, digital responsibility, and national resilience in line with Malaysia's 4IR and MyDigital Blueprint 2030 goals (Economic Planning Unit, Prime Minister's Department, 2021).

3. METHODOLOGY

This paper adopts the Design Thinking (DT) methodology to construct a validated conceptual business model for the SafeSphere project, a digital platform offering smart and affordable home security solutions. Recent research emphasizes that Design Thinking functions not only as a methodology but also as a strategic mindset for business model innovation (You, 2022). The process began with a literature review and benchmarking of similar smart security companies using the Business Model Canvas (BMC) framework to identify innovation gaps and best practices. Design Thinking integrates effectively with tools like the Business Model Canvas (BMC) and value-focused ideation techniques reinforcing its role in shaping user-centred and socially grounded business models (You, 2022). Surveys and interviews were then conducted with different customer segments with homeowners, rental property owners, small businesses and hardware providers to understand their jobs-to-do, extreme pains and essential gains. Insights from this stage guided the development of the initial business model and a digital app prototype, designed using business modeling tools such as the Ecosystem Map (EM), Business Model Canvas (BMC) and Value Proposition Canvas (VPC). The initial model was then tested and validated through stakeholder feedback to refine its value propositions, channels and revenue streams. The findings were analyzed and discussed to ensure user alignment and practicality. Finally, a Strategy Canvas was created to evaluate SafeSphere's relevance and sustainability compared to existing smart security solutions from the perspectives of various customer segments resulting in a user-centered and market-relevant conceptual business model.

4. LITERATURE REVIEW

It evaluates relevant information that are pertinent to the study and may back up the research topic.

4.1. Smart Home Security Market

Rapid advancement of the Internet of Things (IoT) has transformed how people interact with technology, especially in residential settings. Smart Home is considered as a part of IoT. Smart home security is a subset of smart home technologies that aim to enhance the comfort, safety, and energy efficiency of residences. The idea was to use a suite of high technology tools that allow for remote home control through the use of ambient intelligence to keep an eye on the house. This concept has brought a large impact on the smart home market where Mintel (2025) mentioned over 50% consumers in the United States claim security as their leading reasons for purchasing smart home technology. Furthermore, a report from Statistica (n.d.) highlighting Malaysian consumers are increasingly seeking smart home devices as energy efficiency and home security become their priority. This emphasis on security and privacy is a key motivation of businesses in the smart home industry to constantly promote the consumer benefits of smart home technologies, such as ease, cost savings, and home security (Cannizzaro et al., 2020). It is a massive sum, showing how popular the smart home security industry is growing.

4.2. Interoperability

The current integration in the smart home security system has effectively handled common security threats. But there are problems with interoperability since these systems frequently employ distinct standards, protocols, and technology. This lack of standardization could lead to user frustration, dissatisfaction, and wasteful energy usage in conducting smart home ecosystems. Elmi (2023) says that this problem can be lessened by allowing devices to communicate seamlessly to improve user experience, energy efficiency, and security. It improves overall functionality and usability while reducing system complexity and costs within a unified environment. High compatibility could enhance performance, reduce user frustration, and increase perceived reliability, aligning with the Technology Acceptance Model's emphasis on ease of use and usefulness (Phan & Kim, 2020).

4.3. Attitude toward Technical Performance

The consumer's attitude toward technical performance may be defined as their level of satisfaction with the smart home technology's functional and operational aspects. Li et al. (2025) emphasised that the clear value propositions of smart home technologies are control and convenience. Thus, it was an important factor influencing the adoption of smart home technology as consumers' willingness to utilize a smart appliance would depend on their view of mature technology. Studies show that Malaysians' willingness to adopt home automation is influenced by how effectively the system performs its core tasks as Lau et al. (2022) report merely 4.34 mean respondents were likely to incorporate smart technology features into their homes due to this factor.

4.4. Data Sovereignty in Cloud Computing

Data sovereignty in cloud computing refers to the principle that data must adhere to the rules and regulations of the nation. The involvement of cloud computing in storing and processing data on distant servers in numerous places could raise worries about regulatory compliance and management. Therefore, it is vital for Malaysian enterprises who depend on cloud solutions to understand the idea. This requirement is based on Malaysia's Personal Data Protection Act (PDPA) 2010, which specifies how personal data acquired for commercial purposes must be maintained and secured. Lim (2024) mentioned any businesses failure to comply with the PDPA 2010 is not negotiable and can lead to significant disruptions in operations, including penalties up to RM500,000 and three years imprisonment. So, data sovereignty is not only a legal need but it is also a business necessity that helps achieve national goals like the MyDigital Economy Blueprint by regulating where data is stored, which enhances security and encourages transparency, which in turn builds trust and confidence among consumers. Along with this, enterprises must prioritize data residency by having suppliers, such as Telekom Malaysia or other local vendors, that guarantee local data storage, implement strong security protocols such as encryption, and ensure legal measures that satisfy Malaysian sovereignty needs (Aegis, 2025). Finally, as Malaysia's digital landscape evolves, adopting data sovereignty is vital to safeguarding companies legally and increasing their competitiveness.

4.5. Benchmark of Smart Home Security Business Models

Benchmarking is the practice of comparing your business's performance against a rival in the same market (Business Victoria, 2022). The objective is to learn from the best and figure out how to improve.

4.5.1. Apple Homekit

Homekit is the Apple's underlying software platform/framework for controlling and connecting smart home devices providing dependability and ease of use for tech-savvy consumers and homeowners. Homekit lets the user control smart home products using apps on Apple devices such as iPhone, iPad, or Mac. They offer their items directly to consumers, selling their products through their website, Apple, and other retail partners. Revenue is generated from Smart Home Hub sales and IoT collaborations, while main investments include software development, marketing, and support. Apple fosters long-term client ties through AppleCare and online forums as depicted in Fig. 1.

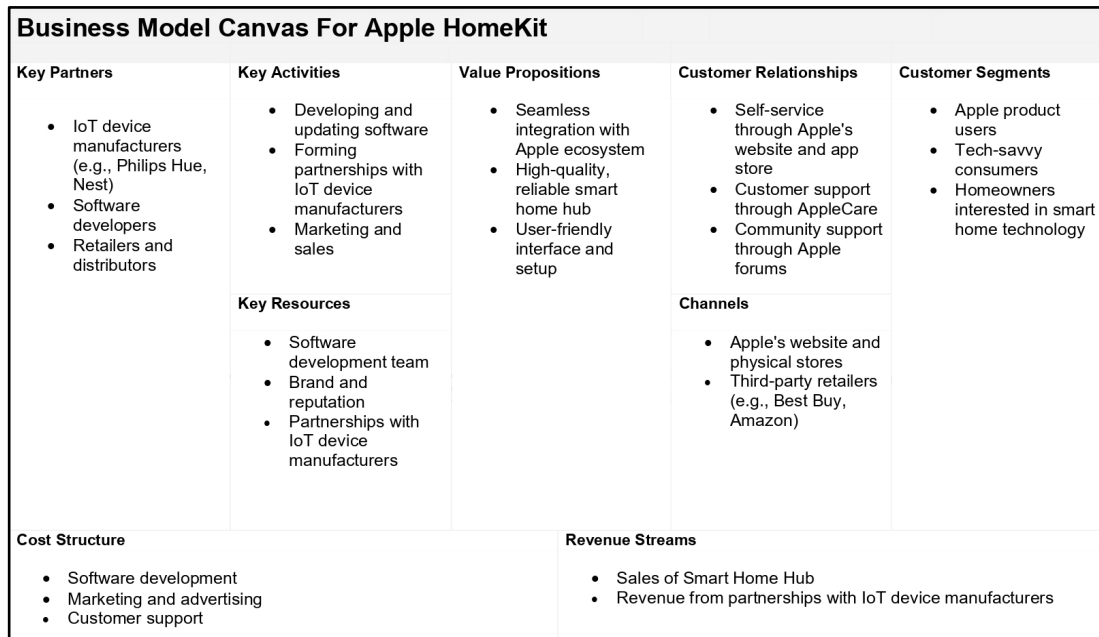


Fig. 1. Business Model Canvas (BMC) for Apple HomeKit

4.5.2. Samsung SmartThings

SmartThings is recognized as one of the most comprehensive and versatile home automation systems developed by Samsung. It offers compatibility with over 5,000 devices, including lights, thermostats, and security cameras through the partnerships with third-party service providers. With the SmartThings app, users can easily set up and manage their homes. The app allows for custom routines and scenes, automating daily tasks such as adjusting lighting brightness or controlling thermostat. The business model of its service is shown on Fig. 2.

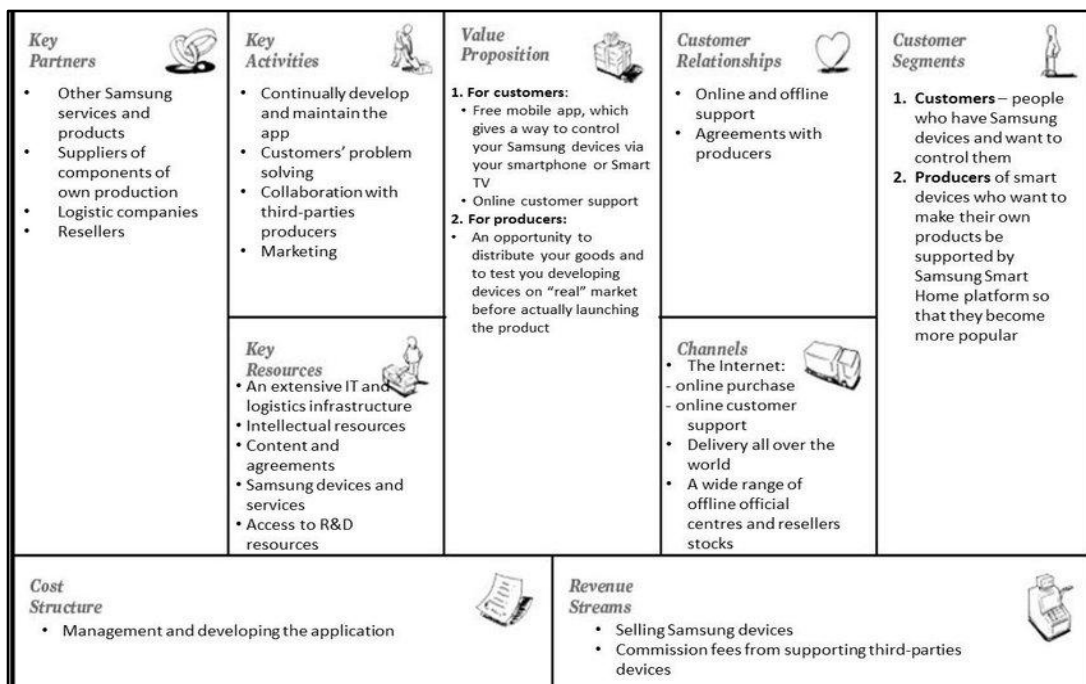


Fig. 2. Business Model Canvas (BMC) for Samsung SmartThings

4.5.3. Wink Hub

Wink operates as a smart home platform primarily targeting homeowners in the United States and Canada. It provides unified control by using the Wink Hub/Hub 2 to translate diverse device protocols like Z-Wave, ZigBee and Wi-Fi into one language. It enables advanced automations like Robots, Schedules, and Shortcuts for security and energy efficiency. including the free Wink App available in iOS and Android. This value is distributed through e-commerce partners like The Home Depot and Amazon.com. Over 50 leading device manufacturers like GE, Nest, Schlage, voice integration services, like Amazon Alexa and many more manufacturer partners alongside. Mandatory monthly subscription for full service access including cloud control and remote monitoring which forms the main revenue stream alongside the sale of Hub hardware. Crucial activities involve delivering the key value which is continuous platform development, security auditing, and partner certification, which contribute to a cost structure that emphasizes the high expense of maintaining and developing the platform. The business model of its service is shown on Fig. 3.

Business Model Canvas For Wink Hub				
Key Partners - IoT device manufacturers (e.g., GE, Nest, and Schlage) - Retailers and distributors	Key Activities - Developing and updating software - Forming partnerships certification - Marketing and sales - Security auditing	Value Propositions - Universal multi-protocol connectivity - Unified Control Platform - User-friendly interface and setup	Customer Relationships - Customer support via Webform, Twitter or Facebook during working hour - Community support through Wink Hub forums	Customer Segments - Homeowners (in the United States and Canada) - Device manufacturers and technology partners
	Key Resources - Software development team - Brand and reputation - Partnerships with IoT device manufacturers		Channels - Direct sales at Wink.com - Third-party retailers (e.g. Amazon.com, The Home Depot, and The Home Depot Canada)	
Cost Structure - Software development - Marketing and advertising - Security auditing - Partner Certification		Revenue Streams - Sales of Hub hardware - Revenue from partnerships with IoT device manufacturers - Monthly subscription		

Fig. 3. Business Model Canvas (BMC) for Wink Hub

5. INITIAL BUSINESS MODEL (BM) – USING BMC & VPC

The Business Model Canvas is a tool that maps out the nine building blocks of a business model including customer segments, value propositions, channels, customer relationships, revenue streams, key resources, key activities, key partnerships, and cost structure. It helps SafeSphere Smart Home Security businesses understand and communicate how we can create, deliver, and capture value which makes it useful for developing the idea of new business models. Fig. 4 depicts the initial BMC crafted for SafeSphere's Smart Home Security Ecosystem, drawing insights from the above literature review.

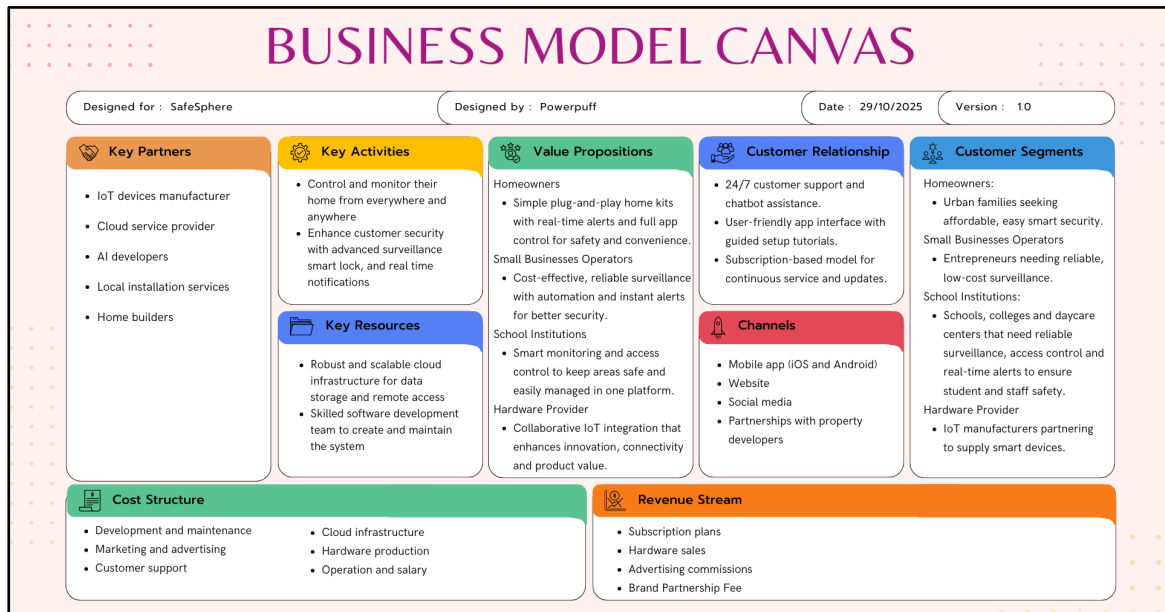


Fig.4. SafeSphere Initial Business Model

The Value Proposition Canvas (VPC) further refines how SafeSphere creates and delivers value to its diverse customer segments by aligning the company's products and services with customer's specific needs, pains and desired gains. It provides a clear view of how the SafeSphere Smart Home Security Platform addresses the widespread challenges of fragmentation, incompatibility and data security in the smart home ecosystem. By mapping customer expectations against SafeSphere's unique offerings such as its centralized gateway hub, AI-driven monitoring and locally hosted cloud services, the VPC demonstrates how the platform delivers meaningful solutions that are both technologically efficient and socially inclusive. Through this framework, SafeSphere ensures that each customer segment including homeowners, small business operators, schools institutions and hardware providers receives targeted value, whether in the form of improved safety, device integration, operational scalability or new business opportunities within a trusted ecosystem.

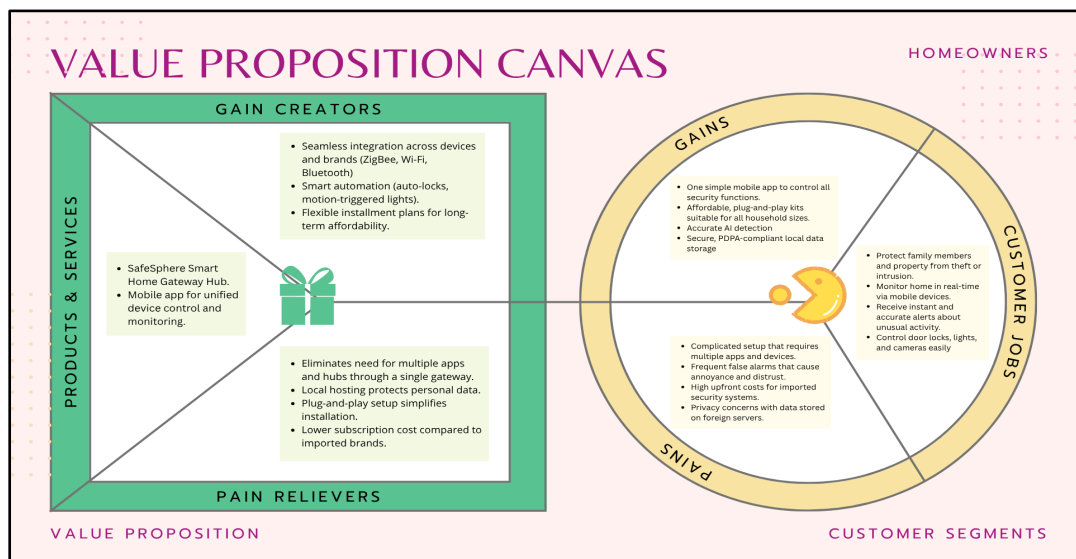


Fig.5. Value Proposition Canvas for Homeowners

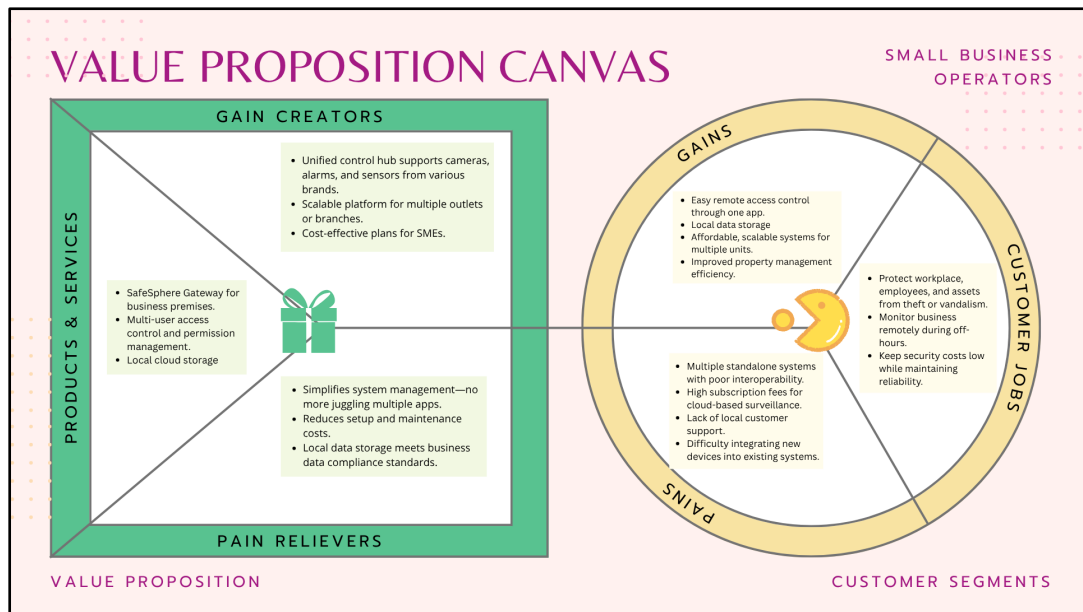


Fig.6. Value Proposition Canvas for Small Business Operators

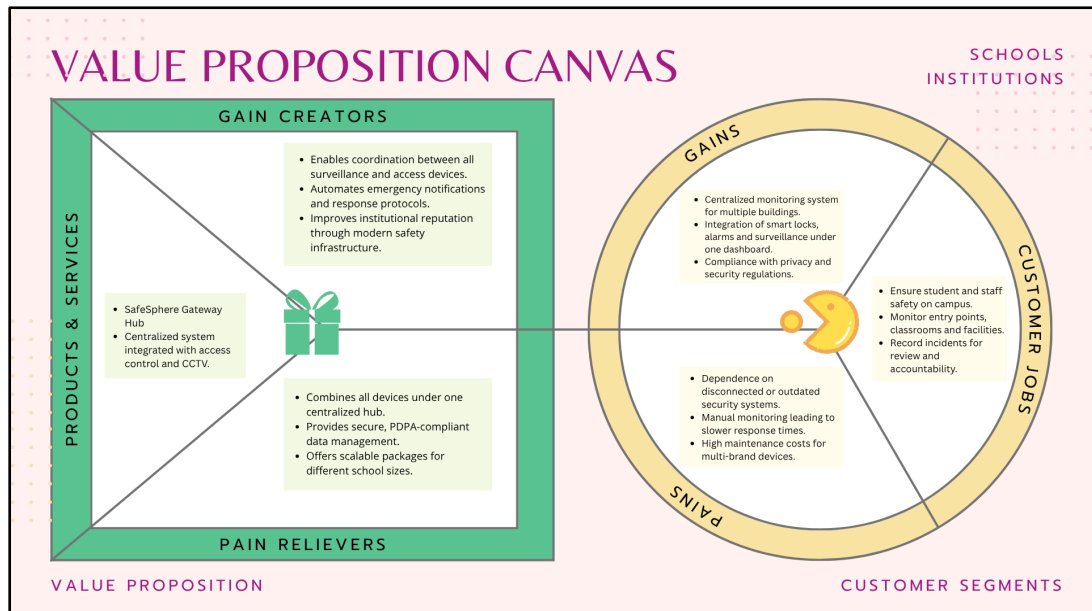


Fig.7. Value Proposition Canvas for Schools Institutions

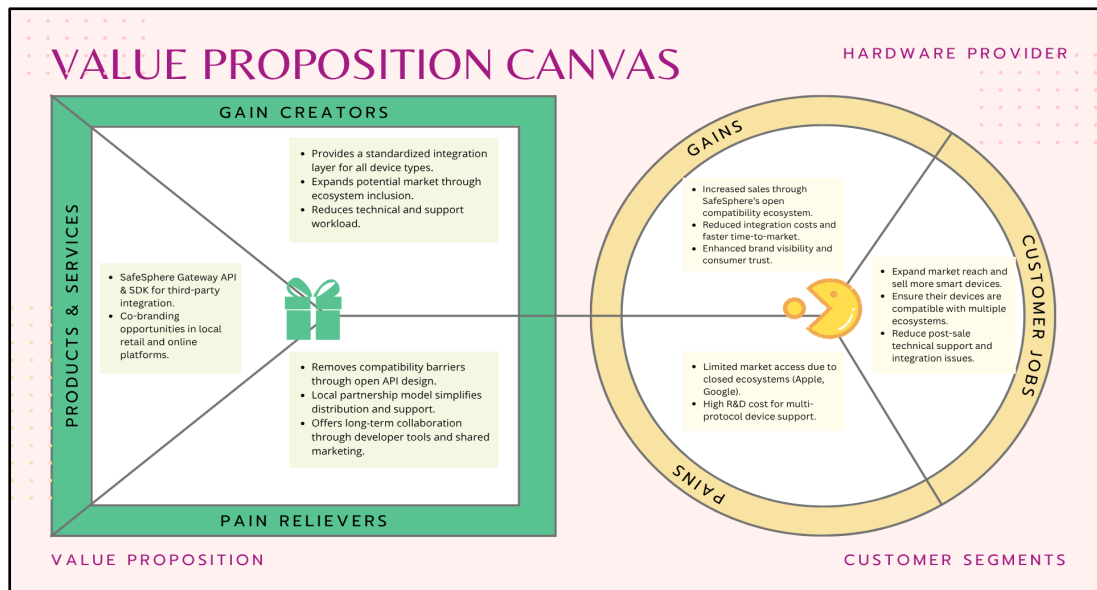


Fig.8. Value Proposition Canvas for Hardware Provider

6. CONDUCT VALIDATION OF INITIAL BM & KEY FINDINGS

To evaluate the initial SafeSphere Business Model Canvas, an online survey was distributed via Google Forms, consisting of 14 questions aimed at understanding the perceptions, preferences and expectations of our targeted customer segments. A total of 32 respondents participated in the survey. Interviews were also conducted with our customer segments to obtain deeper insights into their needs, pain points and experiences related to smart security systems. The findings from both the survey and interviews were analyzed to validate the core elements of the SafeSphere business model.

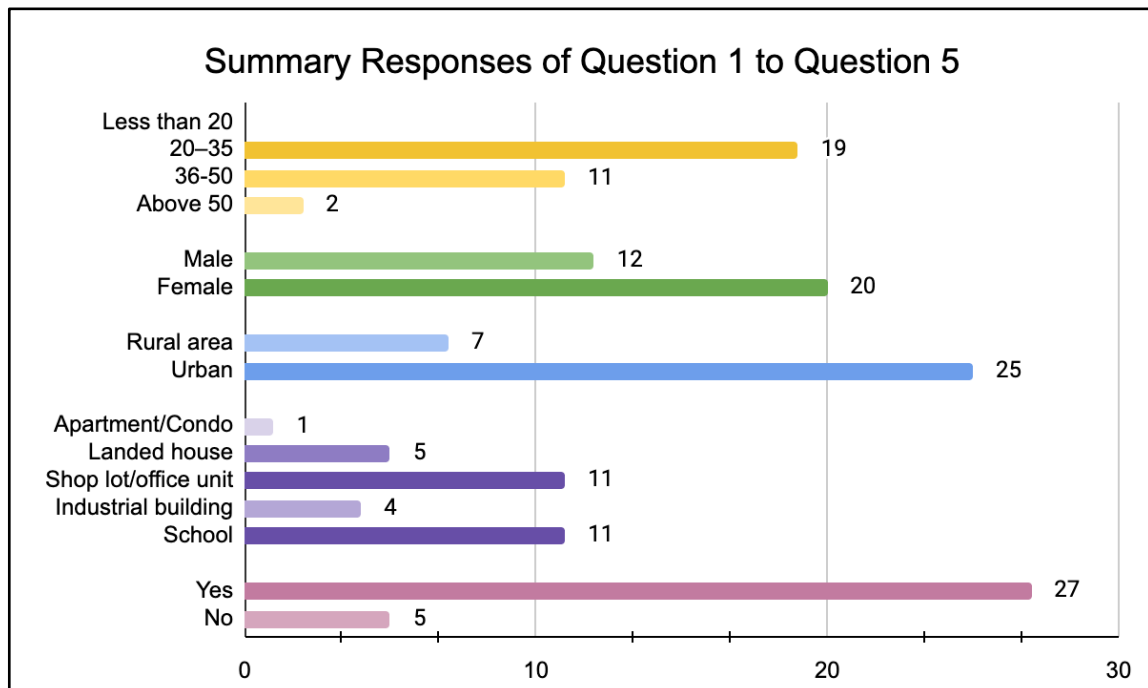


Fig.9. Summary Responses of Question 1 to Question 5

Fig. 9 illustrates the summarized responses for the first five questions of the survey, which aimed to capture the demographic background and early exposure of respondents to smart home security systems. For the first question, which asked about age distribution, most respondents were between 20 to 35 years old. This indicates that SafeSphere's potential market primarily consists of young to middle-aged adults who are generally more familiar with digital technologies and more inclined to adopting smart security solutions for convenience and safety. The second question focused on gender, where the majority of respondents were female compared to male. Furthermore, for the third question, respondents were asked about their area of residence. A large portion of 25 respondents reported living in urban areas, while only seven lived in rural areas. This shows that the concept of smart home security is more recognized and relevant in urban communities, where security challenges and access to technology are higher. The fourth question explored the type of property respondents manage or own. This variety shows that SafeSphere's solution can be adapted beyond homes to cater to commercial, industrial and educational environments, expanding its potential customer base. Lastly, 27 respondents had prior exposure to smart home security systems, demonstrating strong awareness and market readiness for a localized and user-friendly solution like SafeSphere.

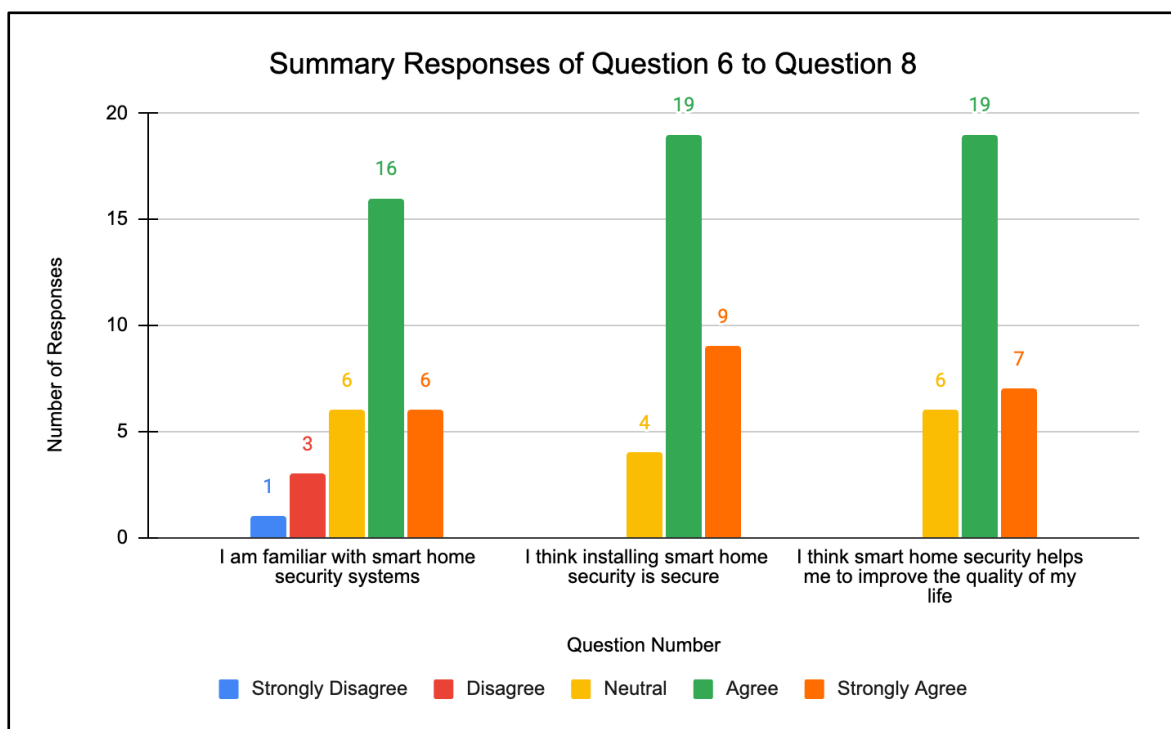


Fig.10. Summary Responses of Question 6 to Question 8

The survey shows that most people have a basic understanding of smart home security systems, as seen in Question 6, "I am familiar with smart home security systems," where 22 respondents agreed, which suggests that awareness is fairly high likely because these systems are becoming more common in homes. However, four respondents disagreed, indicating that a small group still needs more information or education. For Question 7, "I think installing smart home security is secure," and Question 8, "I think smart home security helps me improve the quality of my life," the results are very strong, with zero disagreement, which suggests that

most people already trust the technology and accept its value, likely due to positive experiences shared in media, advertising or by relatives who have tried similar security system. Additionally, 19 respondents strongly agreed with both statements, indicating that users not only recognize the benefits but also feel positive about them, likely due to these systems genuinely improving their safety and convenience.

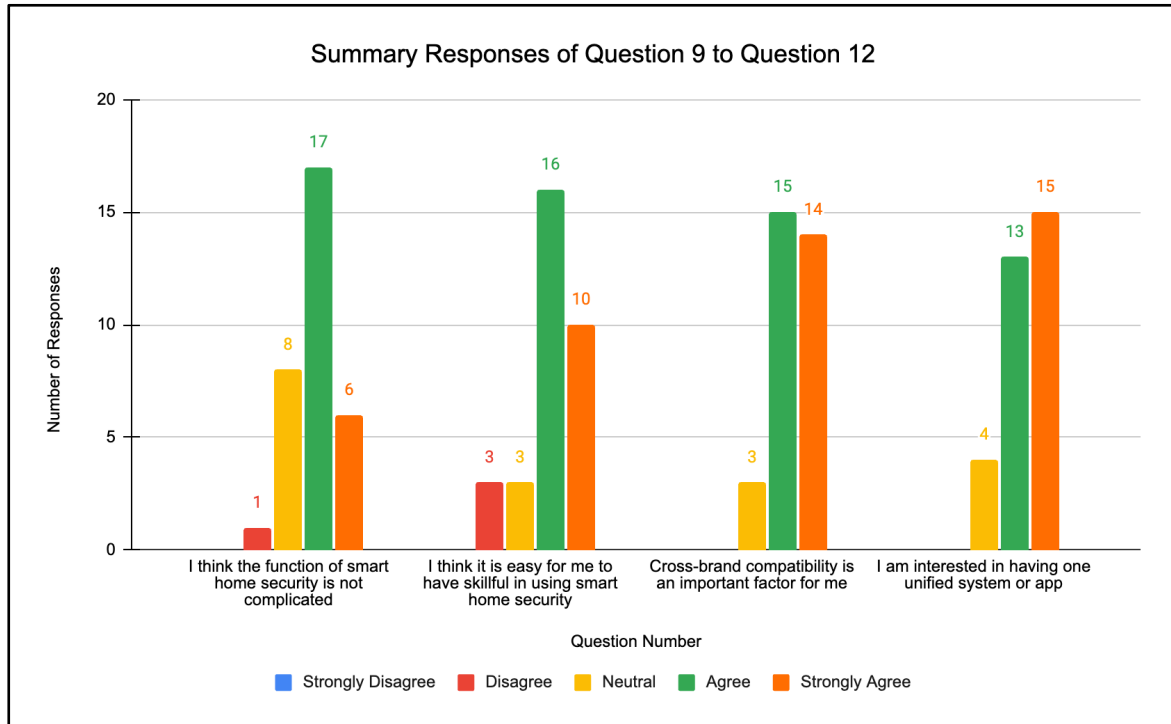


Fig.11. Summary Responses of Question 9 to Question 12

The survey responses for Questions 9 to 12 provide a clear picture of what users value and how they perceive smart home security systems. For Question 9, “Cross-brand compatibility is an important factor for me,” most respondents agreed, showing that users prefer systems that work with multiple brands rather than being limited to one. Furthermore, in Question 10, “I am interested in having one unified system or app,” where 26 respondents agreed. This shows a strong desire for a streamlined interface, likely because managing multiple apps can be confusing and time-consuming, and a unified system makes controlling smart devices easier and more convenient. Question 11, “I think the function of smart home security is not complicated,” and Question 12, “I think it is easy for me to become skillful in using smart home security,” received high positive responses. This shows that users generally feel confident in their ability to operate these systems, which is likely because modern smart home devices are designed to be user-friendly. Overall, the data suggests that the market is ready for smart home security systems that are both flexible across brands and easy for anyone to use, making adoption smoother and more appealing.

Table 1: Summary Responses of Question 13

Number	Challenges Faced in Smart Security System
1	High maintenance cost / expensive installation
2	Data privacy and security risks / sensitive data can be stolen
3	System limitations such as outdated, lag, not real-time, false alarms, hard to monitor, blind spots, no early danger detection
4	Reliance on electricity / dependency on WiFi
5	Hard to operate / not user-friendly
6	Compatibility issues / not integrated with other devices
7	Too many non-threat notifications / false alerts causing users to ignore real danger
8	Risky / general security concern / trust issues

Table 2: Summary Responses of Question 14

Number	Suggestions to Improve Smart Security Systems
1	Make the system more user-friendly / easy for staff or family to operate
2	Improve AI accuracy / AI for unusual behaviour or dangerous activity detection
3	Unified system for all security devices and school staff apps
4	Automated notifications and alerts
5	Improve cybersecurity / encrypt all data end-to-end
6	Ensure system works offline / reduce dependency on WiFi / backup energy system
7	Better hardware: cameras with wider angles, better audio, high-quality video
8	Make system more cost-friendly for people to buy
9	Make it compatible with other devices or systems

The questionnaire included an open-ended question where respondents shared challenges and suggestions for smart security systems. Key recommendations focused on making the system more user-friendly, integrating AI for threat detection, improving device compatibility and integration and providing cost-effective solutions. These insights can guide future upgrades and add-on features to improve system effectiveness and reliability.

For the interview question, the findings presented are derived from secondary data collected from industry representatives on smart home interoperability. The interviewees include Alex Yang from Tuya Smart and George Yianni from Philips Hue, who shared their perspectives on the factors affecting cross-brand smart home device compatibility. Data were obtained from publicly available interviews

published through the Connectivity Standards Alliance (CSA) channels. The insights highlight both the enablers as well as the challenges for achieving interoperability in smart home devices.

Table 3: Summary Responses of Interview Questions

Questions	Responses
What are the key enablers toward achieving interoperability among smart home devices from different brands?	For standardized connectivity • Alex Yang highlights strong connectivity protocols like Zigbee and standards from Project CHIP, which improve data management and enable AI implementation for enhanced production. • George Yianni emphasizes mesh networking, allowing systems to self-organize and provide reliable coverage across the home. For ease of use • Alex Yang notes that setup must be simple, with multiple methods such as hub discovery or direct touch linking of a remote to a light. • George Yianni notes that Philips Hue ensures devices from different manufacturers can communicate reliably through certifications.
What technical or business challenges currently limit device compatibility in the IoT or smart home industry?	For protocol and functionality • Alex Yang notes the diversity of protocols and functions in the market makes it difficult to provide seamless device compatibility. For security standard immaturity • Alex Yang highlights a lack of mature IoT security standards, which hinders interoperability efforts. For product longevity • George Yianni mentions that the long life cycle of products such as bulbs lasting up to 15,000 hours which is equivalent to 15 years, requires software support and interoperability for at least five years, unlike the shorter lifespans common in most consumer electronics

7. VALIDATED BM – BMC FRAMEWORK

7.1. Validated BM

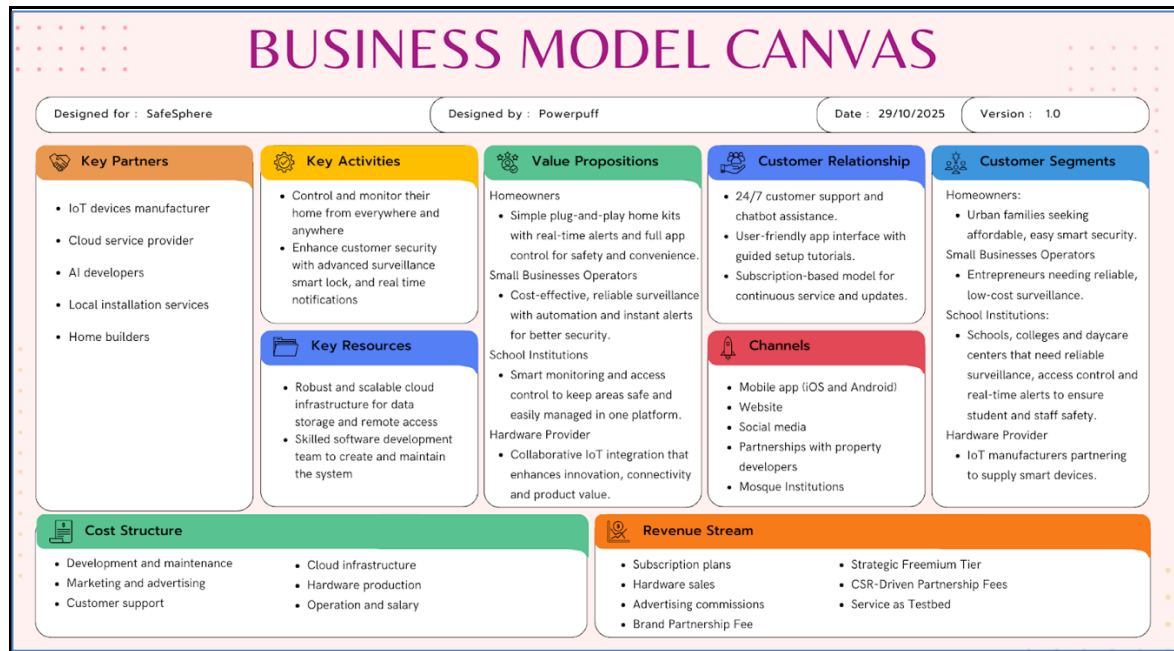


Fig.12. Validated Business Model Canvas

7.1.1. Customer Segments

Customer Segments refer to the specific groups of people or organizations a business aims to serve. In this model, SafeSphere targets four key customer groups. Homeowners, especially urban families, seek affordable and user-friendly smart security solutions to protect their homes. Small business operators consist of entrepreneurs who require reliable, low-cost surveillance to protect assets and streamline operations. School institutions, including primary schools, colleges, and daycare centres, need smart monitoring and controlled access systems to ensure the safety of students and staff in response to growing safety concerns nationwide. Finally, hardware providers represent IoT manufacturers that partner with SafeSphere to integrate and distribute their smart devices within the ecosystem.

7.1.2. Value Propositions

Value Propositions describe the products and services that create value for each customer segment. For homeowners, SafeSphere provides simple plug-and-play home security kits complemented by real-time alerts and full mobile app control, ensuring convenience and peace of mind. Small businesses benefit from cost-effective, scalable surveillance paired with automation features and instant alerts. Schools receive smart monitoring tools and access-control systems designed to keep high-risk areas safe and manageable from one centralized platform. For hardware providers, SafeSphere offers a collaborative IoT integration environment that enhances product visibility, innovation, and ecosystem compatibility.

7.1.3. Channels

Channels describe how a company communicates with and reaches its customer segments to deliver the value proposition. SafeSphere connects with customers through multiple digital channels. The mobile app (iOS and Android) serves as the primary point of interaction, allowing users to control and monitor devices. The website provides product information, onboarding guidance, and customer support. Social media acts as a platform for community engagement, awareness, and real-time updates. Additionally, partnerships with property developers enable SafeSphere to reach homeowners and schools through integrated installations in new buildings, and specialized outreach through partnerships with local religious councils helps connect with Mosque Institutions.

7.1.4. Customer Relationships

Customer Relationships outline the type of interaction a business establishes with each customer segment. SafeSphere maintains strong ongoing relationships through 24/7 customer support and a built-in chatbot assistant to address troubleshooting needs instantly. A user-friendly app interface, complete with setup tutorials, ensures customers can adopt and navigate the system easily. The business also uses a subscription-based model, which supports continuous updates, AI improvements, and long-term service engagement with users.

7.1.5. Revenue Streams

Revenue Streams represent the ways a company generates income from each customer segment. SafeSphere earns through subscription plans, which provide access to cloud storage, AI analytics, and premium features. Additional income comes from hardware sales, including smart cameras, locks, and sensors. Advertising commissions are generated when hardware providers promote their devices through the platform. The company also collects brand partnership fees from IoT manufacturers who collaborate to integrate and distribute their devices within the SafeSphere ecosystem. Furthermore, SafeSphere incorporates a strategic freemium model with the "Community Basic" tier, offering free basic service and necessary security hardware to qualified B40 social centers (like old folks' homes or disabled centers). While these centers receive the core security services at no cost, this program is designed to strengthen the primary revenue streams by attracting key corporate sponsors who pay significant Brand Partnership Fees to fund the hardware rollout as a Corporate Social Responsibility (CSR) initiative, and by utilizing these high-demand social centers as real-world testbeds to continuously improve the quality and reliability of the premium features offered to paying customers.

7.1.6. Key Resources

Key Resources refer to the most important assets required to make the business model work. SafeSphere relies on a robust and scalable cloud infrastructure that enables secure data storage and real-time remote access for all users. The company's skilled software development team is essential for creating,

maintaining, and continuously improving the digital platform, AI detection features, and app functionalities that support its value propositions.

7.1.7. Key Activities

Key Activities describe the most important actions a company must perform to operate successfully. SafeSphere's primary activities include enabling customers to control and monitor their spaces from anywhere, ensuring seamless and responsive functionality. It also focuses on enhancing customer security using advanced surveillance systems, smart locks, and real-time notifications. These activities allow SafeSphere to deliver reliable, integrated safety solutions for households, businesses, schools, and hardware partners.

7.1.8. Key Partners

Key Partners are external organizations or stakeholders that help the business function effectively. SafeSphere collaborates with IoT device manufacturers to supply compatible hardware. Cloud service providers ensure secure and scalable data hosting, while AI developers support advanced detection capabilities. Local installation services assist with deploying devices in homes, businesses, and schools to integrate SafeSphere into new infrastructures, expanding market reach.

7.1.9. Cost Structure

Cost Structure outlines the major costs that a business must incur to operate. SafeSphere's expenses include development and maintenance of the app and platform, alongside marketing and advertising to reach target customers. The company also allocates costs to customer support, cloud infrastructure, and hardware production necessary to deliver its services. Additional expenses include operations and salaries, which ensure daily business activities and technical support are sustained.

7.2. Environment Map (EM)

7.2.1. Key Trends

a. Digital Transformation and 4IR Integration

Malaysia's ongoing transition toward the Fourth Industrial Revolution (4IR) continues to reshape industries through the adoption of Artificial Intelligence (AI), the Internet of Things (IoT) and cloud-based solutions. The National 4IR Policy promotes inclusivity and innovation to enhance productivity and quality of life (Economic Planning Unit, Prime Minister's Department, 2021). SafeSphere aligns with this policy by creating an interoperable platform that leverages AI and IoT to connect multiple smart home brands under a unified ecosystem, driving Malaysia's digital transformation forward.

b. MyDigital and Smart City Development

The Malaysia Digital Economy Blueprint (MyDigital) aims to develop a digitally-driven and high-income nation by promoting connected infrastructures and smart cities (Economic Planning Unit, Prime Minister's Department, 2021). SafeSphere supports this initiative by integrating various smart home and security brands into a centralized system, contributing to safer, smarter and more connected communities within Malaysia's growing urban landscape.

c. Interoperability and Open Ecosystems

Consumers now prefer devices that can connect across brands. SafeSphere follows this trend by becoming a central platform compatible with products from brands like Samsung and Xiaomi. Interoperability is a critical success factor in the IoT ecosystem, enabling different devices to communicate effectively and reducing user frustration caused by fragmented systems (Elmi, 2023).

7.2.2. Market Forces**a. Demand for Unified Smart Home Platforms**

Consumers increasingly prefer integrated solutions that can control all devices from a single interface rather than managing multiple apps for different brands. This demand for simplicity, control and convenience drives the growth of centralized IoT management systems (Zaman et al., 2024). SafeSphere meets this need by offering one application that manages diverse brands and security systems within a secure local environment.

b. Expanding Middle-Class and Urban Population

Malaysia's expanding middle-class population and rapid urbanization continue to influence the adoption of modern and connected living solutions. Urban homeowners and small business operators increasingly seek reliable, customizable smart home ecosystems that balance affordability with functionality (Department of Statistics Malaysia, 2024). SafeSphere targets this demographic with scalable, subscription-based access that fits different income levels and security needs.

c. Platform Economy Growth

The rise of the platform economy has reshaped how businesses deliver value by connecting multiple participant groups through digital interfaces. Multisided platforms enhance innovation by enabling collaboration between users, developers and service providers (Ministry of Economy, 2025). SafeSphere leverages this model by connecting homeowners, device brands and installation service providers through a single ecosystem.

7.2.3. Macroeconomic Forces

a. Government Investment in Digital Infrastructure

Malaysia's Budget 2026 highlights increased investment in 5G, AI cloud services and IoT infrastructure to strengthen the country's digital economy (Ministry of Finance, 2025). Similarly, the Thirteenth Malaysia Plan (RMK-13) emphasizes long-term digital development and nationwide technological upgrades (Ministry of Economy, 2025). These combined initiatives support SafeSphere's scalability by enabling faster data transmission, stronger connectivity and better integration with national digital systems.

b. Inclusive and Sustainable Digital Growth

Malaysia's focus on inclusive growth ensures that digital technologies remain accessible to all social and income groups (Ministry of Economy, 2025). SafeSphere supports this through affordable subscription tiers and local partnerships that enable broader adoption among B40 and M40 households. It contributes to Malaysia's sustainable and inclusive digitalization agenda.

7.2.4 Industry Forces

a. Competition from International Ecosystems

Global brands such as Google Home, Amazon Alexa and Apple HomeKit dominate the smart home integration market but often rely on foreign cloud services that may not fully comply with Malaysia's Personal Data Protection Act (PDPA). SafeSphere differentiates itself by providing locally hosted cloud services, ensuring data sovereignty and privacy compliance.

b. Fragmentation of Smart Home Ecosystems

One of the major challenges in the smart home industry is the fragmentation of IoT ecosystems, where devices from different brands and communication protocols often cannot connect seamlessly. This technological fragmentation has been identified as a key barrier to widespread smart home adoption, as multiple connectivity standards such as Wi-Fi create compatibility issues for consumers (Phan & Kim, 2020). SafeSphere addresses this problem through an open, interoperable platform that unifies device management and simplifies user experience.

c. Local Collaboration and Supply Chain Opportunities

SafeSphere promotes collaboration with local hardware producers, software developers and installation service providers. This strengthens Malaysia's digital supply chain, supports local innovation and encourages the growth of domestic IoT businesses (Ministry of Economy, 2025).

7.3. Strategy Canvas

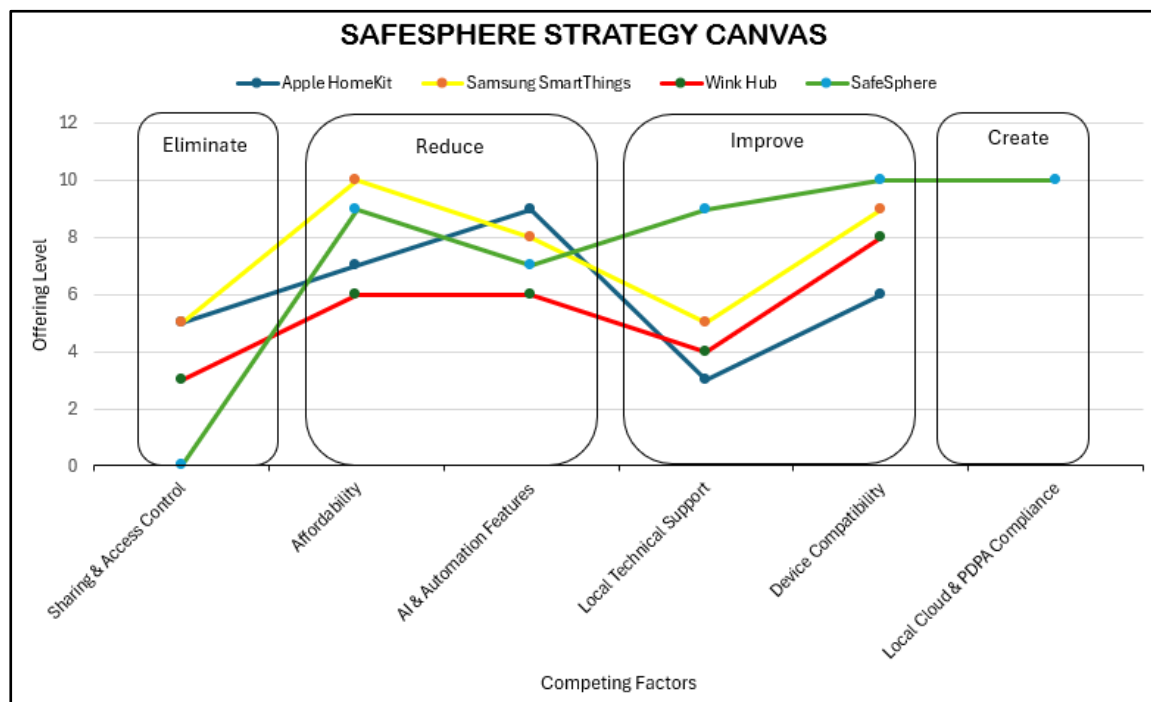


Fig.13. SafeSphere Strategy Canvas

A strategy canvas is a line graph that plots functions or factors against the value of a company and then overlays industry benchmarks. By doing this, information can be built to help create a competitive strategy. It is a central diagnostic tool that graphically shows the current strategic landscape and the future prospects for an organization (Precious, 2023). By mapping out these competitive factors on a single graph, the strategy canvas helps businesses make informed decisions about which aspects to raise, reduce or innovate, guiding product development and positioning. Based on Fig. 13, the strategy canvas compares well-known smart home platforms such as Apple HomeKit, Samsung SmartThings and Wink Hub with our platform SafeSphere. The analysis highlights SafeSphere's ability to outperform existing solutions in areas most relevant to Malaysian consumers such as compatibility, local data compliance and technical support accessibility.

Apple HomeKit dominates in AI automation reflecting Apple's premium positioning but remains limited by its high cost and closed ecosystem that primarily supports Apple-branded devices. Similarly, Samsung SmartThings denotes an affordability platform where it offers free services yet depends heavily on foreign cloud services and lacks localized data protection compliance. Meanwhile, Wink Hub offers multi-protocol connectivity but has limited regional support and a mandatory subscription model which reduces its accessibility in emerging markets.

In contrast, SafeSphere differentiates itself through its focus on interoperability, inclusivity, and local relevance. The platform introduces an open and cross-brand ecosystem that unifies devices from various brands including locally popular smart home brands such as Tapo and Xiaomi under a single, easy-to-use interface. This gateway-based design eliminates the frustration of managing multiple applications and ensures seamless integration for homeowners, schools and SMEs (Phan & Kim, 2020).

Beyond device compatibility, SafeSphere stands out by hosting all data on locally managed cloud servers that comply with Malaysia's Personal Data Protection Act (PDPA) ensuring user privacy, data sovereignty and trust. It has a feature not offered by its international competitors. Furthermore, SafeSphere enhances accessibility through affordable pricing models by having flexible subscription tiers and localized technical support, making smart home technology available to users from diverse income levels and technical backgrounds.

Overall, SafeSphere's "purple cow" lies in its localized, interoperable and inclusive ecosystem. The platform offers a unified smart security platform that connects multiple device brands, complies with Malaysia's data protection laws and provides affordable, scalable solutions for homeowners, SMEs and educational institutions. While global competitors emphasize premium features and closed ecosystems, SafeSphere prioritizes practical integration, local relevance and digital sovereignty, positioning itself as Malaysia's first unified smart security ecosystem that truly bridges innovation with national inclusivity.

7.4. High Fidelity Prototype

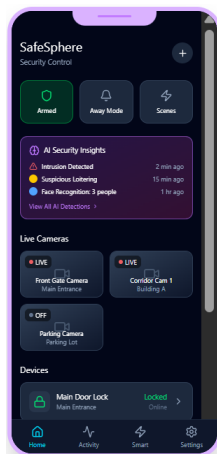


Fig. 14. SafeSphere's Homepage

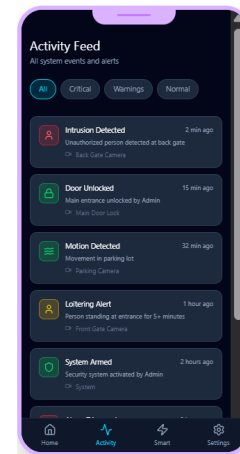


Fig. 15. SafeSphere's Activity Feed Page

Refer to Fig. 14 The Home Dashboard serves as the real-time core of the IoT management system, displaying the status of all connected security devices and enabling system-wide actions. It acts as a universal security hub by allowing the addition of devices from any brand. Central to its function is the AI Security Insights panel, which provides immediate, machine learning-powered threat detections like intrusion alerts and facial recognition, with live camera thumbnails reflecting feeds continuously processed by AI models for automated monitoring.

Refer to Fig. 15 The Activity Feed is the central Big Data Analytics hub, aggregating and displaying all chronological security events (motion alerts, access logs, AI detections) from connected IoT devices. This comprehensive audit trail captures, timestamps, and stores every event, which is then intelligently categorized and color-coded by severity using data classification algorithms. Users can quickly identify patterns and anomalies, utilizing filtering capabilities and detailed event metadata for forensic analysis and compliance reporting.

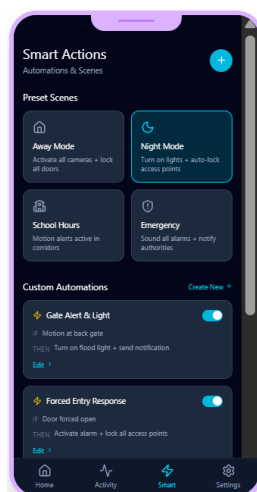


Fig. 16. SafeSphere Smart Page

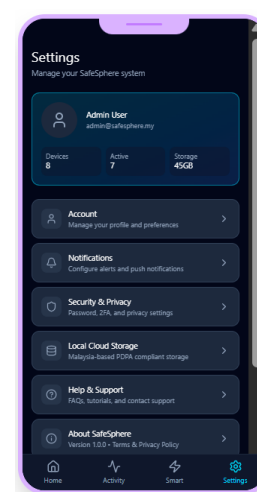


Fig. 17. SafeSphere Settings Page

Refer to Fig. 16 The smart page features preset scenes (Away Mode, Night Mode, School Hours, Emergency) for one-tap system control. Includes custom automation builder using "IF this, THEN

Refer to Fig. 17 The settings page manages account preferences, notification configurations, and security settings. Displays local cloud storage usage with Malaysia-based PDPA compliance

that" logic to create rules like "IF motion detected information, plus access to help resources and at back gate THEN turn on flood light + send system information. notification."

8. CONCLUSION AND FUTURE WORKS

Across Malaysia's safety landscape, each customer segment, including homeowners, rental property owners, small businesses, schools, and hardware providers, faces distinct yet interconnected challenges. Homeowners struggle with complex setups, high costs, and privacy risks, while rental property owners and SMEs face difficulties managing multiple locations and ensuring affordable, scalable surveillance. Schools deal with fragmented safety systems and limited emergency responsiveness, and hardware providers encounter barriers in integrating devices and reaching local markets. Their essential job-to-do is to safeguard people, property, and data efficiently, yet they endure extreme pains such as fragmented apps, high maintenance costs, and lack of interoperability. The essential gains sought include real-time monitoring, trusted data protection, and seamless device integration. SafeSphere's core proposition is built around directly addressing the customer's pains and gains, differentiating itself through its unified digital ecosystem, a single mobile platform integrating various IoT-enabled devices (cameras, alarms, smart locks) with AI-assisted anomaly detection, PDPA-compliant local cloud storage, and plug-and-play setup. Its business model emphasizes affordability, interoperability, and inclusivity through subscription plans and local support. By serving as both a pain reliever and gain creator, SafeSphere not only simplifies smart security management for all users but also strengthens local digital sovereignty and community trust, aligning with Malaysia's MyDigital Blueprint 2030 and 4IR objectives, and ultimately contributing to the welfare of all, reflecting the spirit of *Rahmatan lil 'Alamin*.

Building on this foundation, future works will focus on transforming the validated business model into a comprehensive business plan that ensures strategic scalability and long-term sustainability. This plan will include market validation, financial forecasting and the development of partnership frameworks with local IoT manufacturers, installation service providers and educational institutions. Further research and development will also explore AI-driven predictive analytics for enhanced threat detection and expand SafeSphere's interoperability framework to support more device brands and emerging communication protocols. Additionally, pilot deployments in schools, SMEs and residential areas will be conducted to evaluate system performance, user satisfaction and operational feasibility. These initiatives aim to evolve SafeSphere from a conceptual model into a fully operational, multisided smart security platform that contributes to Malaysia's digital transformation and sustainable innovation goals.

REFERENCES

- Aegis. (2025, January 27). *Data Sovereignty in Cloud Computing For Beginners in Malaysia*. Aegis. <https://www.aegis.com.my/data-sovereignty-cloud-computing/>
- AmlInvest Bank Berhad. (2025). *Malaysia Budget 2026 Update*.

- https://www.aminvest.com/docs/aminvestlibraries/knowledge/market-overview/budget-2026.pdf?sfvrsn=4d76ef18_1
- Benchmark your business (Victoria). (2022, September 29). Business Victoria. <https://business.vic.gov.au/business-information/marketing-and-sales/increasing-sales-through-marketing/benchmark-your-business>
- Cannizzaro, S., Procter, R., Ma, S., & Maple, C. (2020). Trust in the smart home: Findings from a nationally representative survey in the UK. *PLoS ONE*, 15(5), e0231615. <https://doi.org/10.1371/journal.pone.0231615>
- Department Of Statistics Malaysia. (2024, Oktober). *Statistik Jenayah Crime Statistics Malaysia 2024*. https://storage.dosm.gov.my/crime/crime_2023.pdf
- Economic Planning Unit, Prime Minister's Department. (2021, July). *National Fourth Industrial Revolution (4IR) Policy*. <https://www.ekonomi.gov.my/sites/default/files/2021-07/National-4IR-Policy.pdf>
- Economic Planning Unit, Prime Minister's Department. (2021, February). *Malaysia Digital Economy Blueprint*. <https://www.ekonomi.gov.my/sites/default/files/2021-02/Malaysia-digital-economy-blueprint.pdf>
- Elmi, Y. A. (2023). Interoperable IoT Devices and Systems for Smart Homes: A Data Analytics Approach to Enhance User Experience and Energy Efficiency. *Journal of Digitainability, Realism & Mastery (DREAM)*, 2(10), 51–66. <https://doi.org/10.56982/dream.v2i10.195>
- Kam, K. J., Wei, L. J., Lim, T. S., Ilmi, H. S., & Soon, L. T. (2023). A Study on the Adoption of Smart Home Technologies Among the Homeowners in Malaysia: In N. F. Peng & U. N. Sonet (Eds.), *Advances in Civil and Industrial Engineering* (pp. 1–21). IGI Global. <https://doi.org/10.4018/978-1-6684-8253-7.ch001>
- Lau, J. S., Lau, J. L., & Harun, Z. (2022). Factors Influencing the Intention to Adopt Smart Home Technology among Households in Johor Bahru, Malaysia. *International Journal of Academic Research in Business and Social Sciences*, 12(12), 2222–2238. <https://doi.org/10.6007/IJARBS/v12-i12/16016>
- Li, W., Yigitcanlar, T., Nili, A., Browne, W., & Li, F. (2025). Responsible smart home technology adoption: Exploring public perceptions and key adoption factors. *Internet of Things*, 32, 101622. <https://doi.org/10.1016/j.iot.2025.101622>
- Lim, J. (2024, May 13). PDPA Malaysia Penalty: What is the Cost of Non-Compliance? Captain Compliance. <https://captaincompliance.com/education/pdpa-malaysia-penalty/>
- Malaysia school stabbing: Handwritten note found on suspect alludes to love, revenge, anger. (2025, October 16). The Straits Time. <https://www.straitstimes.com/asia/se-asia/malaysia-school-stabbing-handwritten-note-found-on-suspect-alludes-to-love-revenge-anger?utm>
- Ministry of Economy. (2025, July). *Executive Summary Thirteenth Malaysia Plan 2026-2030*. Percetakan Nasional Malaysia Berhad. https://rmk13.ekonomi.gov.my/wp-content/uploads/2025/09/Executive_Summary_Thirteenth_Malaysia_Plan.pdf
- Ministry of Finance. (2025, October 10). FOURTH MADANI BUDGET 2026. In Dewan Rakyat [Speech]. <https://belanjawan.mof.gov.my/pdf/belanjawan2026/ucapan/bs26.pdf>
- Mokhtar, W. H. W., & Ismail, A. (2018). Adoption Of Smart Home Technologies Features Among The Homeowners In Hulu Langat, Selangor. *International Journal Of Real Estate Studies*, 12(2), 9–20.
- Phan, L.-A., & Kim, T. (2020). Breaking Down the Compatibility Problem in Smart Homes: A Dynamically Updatable Gateway Platform. *Sensors*, 20(10), 2783. <https://doi.org/10.3390/s20102783>
- Precious. (2023, January 21). Strategy Canvas: How to Make Strategy Canvas with Examples. BusinessYield. <https://businessyield.com/business-strategies/strategy-canvas/>

- Saidi. (2021, May 13). Portal Belanjawan Kementerian Kewangan. Laman Web Khas Belanjawan 2026. <https://belanjawan.mof.gov.my/ms/>
- Saleh, B., Ma-Key, N., & Osman, R. (2013). MyMukim2Cloud Collaborative System A Mosque Collaborative Network for Serving the Societal Needs in Malaysia. *International Conference on ICT for the Muslim World (ICT4M)*, 1–7. https://www.researchgate.net/profile/B-Saleh/publication/281407213_MyMukim2Cloud_Collaborative_System/data/55e5b30008aede0b5736fdc6/ICT4M2013-Paper90-IEEEEXPLORE.pdf?origin=publication_detail&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6Il9kaXJlY3QiLCJwYWdlIjoicHVibGljYXRpb25Eb3dubG9hZCIsInByZXZpb3VzUGFnZSI6InB1YmxpY2F0aW9uIn19
- Smart Home Security Market (2025-2030). (n.d.). Grand View Research. Retrieved November 12, 2025, from <https://www.grandviewresearch.com/industry-analysis/smart-home-security-market-report>
- Smart Home—Malaysia Statista Market Forecast. (n.d.). https://www.statista.com/outlook/cmo/smart-home/malaysia?srltid=AfmBOoqB_oZZ7z4VtvZ8tPuhu82FzCkPz0ZUPWGOZopeHSsryzw3OQif
- The Alliance Interviews Co-Founder and COO of Tuya Smart. (2020, November 23). CSA-IOT. <https://csa-iot.org/newsroom/alliance-interviews-tuya-smart/>
- The Alliance Interviews Head of Technology of Philips Hue. (2018, April 10). CSA-IOT. <https://csa-iot.org/newsroom/zigbee-alliance-interviews-head-of-technology-of-philips-hue/>
- The Rise of Smart Home Technology: Opportunities for the Future of Living. (2025, February 11). Mintel. <https://www.mintel.com/insights/technology/the-rise-of-smart-home-technology/>
- You, X. Applying design thinking for business model innovation. *J Innov Entrep* 11, 59 (2022). <https://doi.org/10.1186/s13731-022-00251-2>
- Zaman, M., Puryear, N., Abdelwahed, S., & Zohrabi, N. (2024). A Review of IoT-Based Smart City Development and Management. *Smart Cities*, 7(3), 1462–1501. <https://doi.org/10.3390/smartcities7030061>