An Analysis on Factors Hindering the Development of Smart Home

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Jiahe Tan

Spring, 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature _____ Date _____
Jiahe Tan 05/05/2021

Approved _____ Date _____
Sean Ferguson, Department of Engineering and Society

An Analysis on Factors Hindering the Development of Smart Home

Introduction

In the context of the continuous growth of artificial intelligence technology, the concept of smart homes have gradually entered peoples's lives. A smart home refers to a convenient home setup that connects all kinds of equipment in people's home, such as lighting, audio, air conditioning, alarms, electric curtains, sensors, and various other home appliances through a dedicated network. With the interconnection and interaction between devices, a smart home is able to realize multiple automatic control functions, such as remote control and voice control to enhance the convenience, comfort and safety of home life. With the improvement of living standard, people are no longer satisfied with basic household appliances, but instead pursue the safety, technology, interactivity involved in household lives. Smart home technologies not only add new fun to people's household lives, but also give birth to a huge emerging consumer market. The statistics to do with the smart homes throughout the world indicates that the whole smart home industry is rapidly developing. In 2020, there are an estimated 175 million smart homes in the world. The global smart home market has already generated $90.97 billion US dollar in revenue so far and is projected to grow another 25% from 2020 to 2025 (Ljubica, 2021). Smart home technologies gives people a promising vision about household lives; However, there are still gaps between visions and reality. The development of smart homes still has some challenges to overcome to fully benefit people's household lives (Hargreaves, 2018).

Among various elements that may leads to the success of a new industry, the three core components that cannot be separated from the development of the industry are product quality, price and customer service quality. Based on Mohammed et al., service quality, product quality and price are the three elements affecting towards customer satisfaction (Mohammed, 2017). This paper aims to explore challenges faced by the smart home industry from these three aspects

and to discover barriers for smart home in achieving high quality, low price and excellent customer service. The paper begins by analyzing quality challenges faced by smart home industry by breaking down barriers in aspects of safety, stability and availability (fig. 1). After that, the paper explores pricing problems and service problems that limit the development of smart home industry. Finally, conclusion and suggestions for further research are being made.

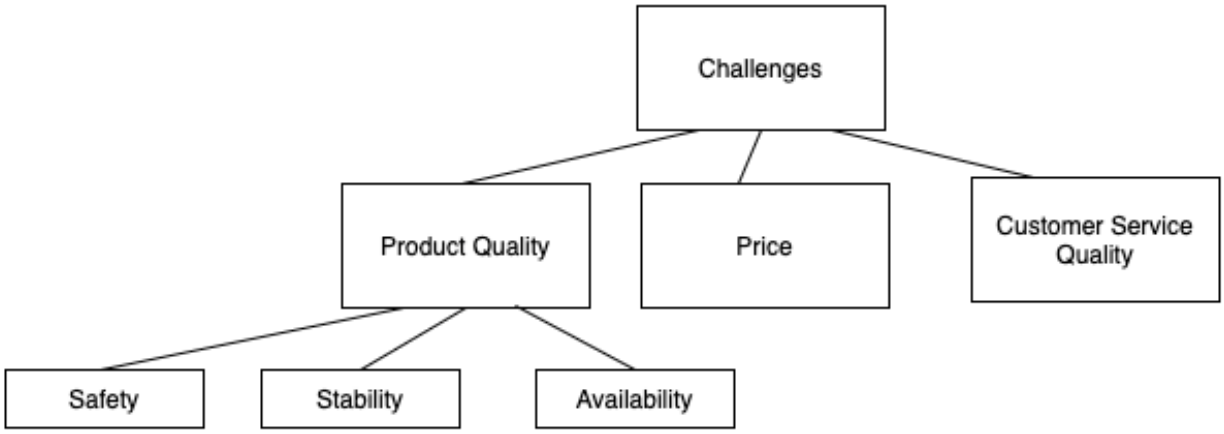

Figure 1. Overall Framework

Product Quality Challenges

For smart home technologies, good quality should include: safety, stability and availability.

Safety Problems

The biggest challenges for smart homes to achieve high quality is the safety problems, such as sensitive information being stolen, resulting in personal privacy being exposed, and illegal intrusion of smart home devices. Now there are more and more devices around that can connect to the internet; even a refrigerator has the same computing power as a mobile phone. Hackers also have discovered the flaws behind and use this convenience to attack. According to

Sunwoo Kim, privacy and user information protection is a big concern for Korean people to adopt smart home technologies. “Whereas the home monitoring camera is very useful for pet care and security, there is a trade-off between the usefulness and the privacy safety. There should be a possibility of 3rd person access to recorded images, which has to be saved somewhere in the cloud storage for the mobile phone access.” (Kim, 2016). In addition, studies also verified that security problem negatively affects people’s attitude towards smart home technologies. “ For example, a poll by market research firm found that almost nine out of ten people said that they were at least “a little” concerned about the safety of their personal information. Moreover, over half of the respondents said that the US government was not doing enough to protect their data, and almost 80 percent said that strong regulations should govern how data brokers and others can repurpose personal information.”(Abomhara, 2014).

The security attacks of smart home can be classified into two categories: passive attacks and active attacks (Ali, 2017). In passive attacks, attackers are trying to retrieve information of the system, but they do not alter or destroy actual system resources. In this type of attacks, attackers will monitor the system and obtain private information of the system, and even transmit messages to other antagonists. Common passive attacks are attacks on privacy, such as eavesdropping and passive monitoring, traffic analysis and data mining. Another category of attack is active attacks, which is often used in combination with passive attacks. In active attacks, hackers uses information collected using passive attacks for an attempt to change system resources and alter system settings. Common active attacks include worms, malicious software, and denial of services (Dos).

One of the most infamous active attack is Mirai IoT Botnet, which leads to a nationwide network paralysis which caused many major websites including Twitter, Amazon and PayPal, causing users fail to logging in. The malfunctioning of these websites lasts for a long time, and

only after two and a half hours, these websites began to resume their services. The source of this incident mainly came from smart home devices. A piece of malware called Mirai infects a large number of vulnerable smart home devices, especially smart cameras, smart gateways. After being infected, these devices instantly became broiler devices in the botnet and are used in large-scale Distributed Denial of Service (DDos) attacks. At its peak, Mirai infected over 600,000 vulnerable smart home devices ("Inside The Infamous", 2020). The working principles behind DDos attack is to combine multiple computers as an attack platform to launch DDos attacks against one or more targets; thereby attackers are able to exponentially increase the power of denial attack of services. Simply speaking, the hackers behind Mirai were able to control a large number of computers and used false access to consume all the server resources of major websites, causing normal users to be unable to access them. According to Andy Green, a blogger of data privacy and security regulations, the biggest problem behind these vulnerable smart home devices is that "Privacy by Design is not part of the vocabulary of the makers of these IoT gadgets." Green suggests that consumers are bad at changing default settings. "The hackers behind the recent Mirai attack exploited the consumer's default-itis. Specifically, they took a brute force approach, scanning tens or even hundreds of thousands of routers worldwide searching for exposed telnet ports. They then gained shell access by trying a short series of typical default passwords —"12345", "admin", etc. — until they succeeded in logging in." (Green, 2020).

Currently, there are some security measures that can be taken for ensure security of smart home devices. Some examples of these measures are user and device authentication, network monitoring and cryptography and key management strategies. However, few companies in the entire smart home industry can guarantee in preventing safety problems in the above aspects because there are too many fields to be covered by a single companies. A more reliable solution

is cooperation between enterprises. However, this approach may involve many intricate interest relations, which may result in weak connections between the entire smart home systems. The security problem can also be solved more effectively by establishing security standards, but there is still no complete sets of security standards for smart home systems in the world.

Stability Problems

Low stability is also an issue restricting user adoption of the smart homes thereby limiting the development of smart home industry. Currently, many manufacturers of smart home devices are overly pursuing some flashy functions, but they often overlook the most fundamental requirement of smart home system, which is the stability of the system. At the same time, with the prevalence of wireless technology, manufacturers have launched many wireless smart home products which adds flexibility and convenience to their products. However, one of the major challenges affecting stability of wireless technologies is batteries. Wireless smart home technologies are expected to change batteries once every few weeks, depending on actual usage. Products with low-energy consumption, such as smart door locks claim to have three to six month battery lives; other high-energy costs devices, such as motion sensors and cameras need new batteries at a much faster rate. However, the real energy consumption rate is not ideal like they claimed to be due to reasons such as home Wi-Fi coverage and activity frequency.“Take security camera Arlo as an example. When you go down and see the review on Amazon, some customers only get one to two weeks of battery usage. Three to six months of battery life is under some assumptions, like Wi-Fi coverage perfect or the camera doesn’t take much movements and activities. The real situation sometimes get people frustrated,” according to Victor Vaisleib, the CEO of Wi-Charge (Yang, 2018). Imagine in the cold winter, when we use the mobile phone app to turn on the air conditioner, but when we get home, we found that the air conditioner has not been turned on successfully and the entire house is in a very low temperature.

A smart home device without energy supply is even more useless than a regular home appliance. Currently, we haven't seen an example wireless products that can withstand the market's proof and inspection, because wireless smart homes have not been on the market for a few years. Although wired smart home products started earlier, the maturity, durability and stability of the current products are better than wireless smart home products, but it is the wireless products that can really promote the popularization of smart homes. Therefore the durability and stability of the product can be said to be one of the bottlenecks restricting the development of smart home industry.

Availability Problems

The definition of availability in Oxford Languages is the quality of being able to be used or obtained. For smart home devices, availability is more like user experience and the degree to which users think that the devices are accessible any time they need without interruption. However, smart homes also have a long way to go in achieving good availability. One bottleneck hindering the availability of smart home is that smart home protocols are not unified and products cannot be interconnected. There are many different smart home brands and apps available in the market, and people may buy smart home appliances from different companies. The current situation of smart homes is that different brands or platforms cannot be compatible, and also different protocols cannot be compatible. The consequence of this problem is that there are multiple products and multiple apps, and the products cannot be linked together, and data cannot be shared, which greatly affects the user experience and availability. For example, if user wants to turn on the lights and air conditioner in his/her house, but the light switches and the air conditioner is from different brands, he/she has to open one app to turn on lights and then open another app to turn on the air conditioner. In this case, the smart home system in user’s house would fail to provide an instant access and provide services instantly. Another example is the

home intrusion detection systems and the alarm systems. Home intrusion detection systems in a smart home need to provide a real-time monitoring function for users. However, if the protocols for home intrusion detection systems is different from the alarm systems, it will take time for intrusion information be transmitted from the detection systems to the alarm systems. If the alarm system fail to provide an instant notification in a timely manner, the whole network of home security devices is useless.

Low Price Challenges

The low price refers to more cost-effective. Under the condition of ensuring quality, a reasonable and acceptable price should be set to make consumers feel that buying is more worthwhile. In terms of product pricing, the entire industry is still somewhat high. Cost is an important factor which affects user's usage decision and tends to slow technology adoption. Mashal et al suggests in his paper that cost in smart home may include many different elements such as, devices purchase cost, installation cost, communication cost, service subscription cost, and maintenance costs (Mashal, 2019). Home automation costs $753 on average. To fully automate a 4-bedroom, 3-bathroom home, people might spend up to $15,000. Luxury fully-connected home may even costs from $10,000 to $150,000. Besides the costs of appliances, labors to install wired systems will also cost $85 per hour. In addition to these one-time purchase, subscription fee and maintenance costs require another $500 to $1,500 per year ("Learn How Much", n.d.). Therefore, compared to regular home technology, smart home technology requires a higher investment. Although people may want to try a smart home device, if they need to spend so much money to buy it, he or she will consider whether it is worth the price and whether it is necessary to buy a smart home device instead of a regular one. Some studies have already incorporated costs of smart home technologies into their model of studying intentions of users to adopt smart homes. For example, Alolayan found that cost is the most significant factor in

determining users intention to adopt not only smart fridge specifically, but also other smart home devices in general (Alolayan, 2014). Also, Shuhaiber indicates in his paper that costs will have a significant negative influence on intention to use smart home (Shuhaiber, 2019). The result shows that the higher the smart home prices the lower the intention to use it. Therefore, high prices is also a major bottleneck restricting the development of smart homes.

Customer Service Challenges

For the issue of service, the effectiveness of after-sales service of smart home service provider is the major shortcoming for big smart homes companies to overcome.

Previous researches and papers indicate that good after-sales service as one of the most important factors affecting user experience and consumer satisfaction positively and leading to increased customer loyalty and brand reputation (Wickramasinghe, 2016). After-sales service is important in consumers' perspective since not everyone has strong hands-on skills. When smart home devices malfunction, it is hard for common people to figure out the exact reasons behind and fix the issue by themselves. In addition, some electrical products need to be operated by professionals who understand electrical technology, otherwise it may probably bring personal safety hazards to the operator. We can imagine, if one night when we go home from get off work, we find that the smart switch in your bedroom suddenly breaks down and the light can't be turned on. But no one can help with this since it is very late and customer service is not available. Although the probability of this happening is not very high, electronic products will have a certain defective rate. When such a situation occurs, if the company fail to take corrective measures in a timely manner and give customers satisfactory feedback and answers, it will leave a very bad impression on users, and it is easy to produce bad reputation and influence. Kim suggests in his paper the consumer concerns of after-sale services for smart home service providers. "When the smart home application doesn't work, it may be hard to know what the real

issue is. Various problems can be considered such as WiFi disconnection, application error, or malfunction of sensors embedded in the smart home appliances. If we need to contact each service provider separately, it would be very painful. All the communication channels should be integrated into single source for a quicker resolution." To solve problem like this, smart home companies need to provide secure internet broadband services and electricity services as well as responsive customer feedback and repair as basic prerequisites (Kim, 2016). In addition, regular inspections are also very important in preventing sudden malfunctions of the smart home devices since if minor problems are found and fixed in time, the possibility of major problems happening will be reduced. However, service costs is naturally indispensable to good service quality. Based on the study conducted by Rolstadaas et al., service costs do not have a well-documented standard unit-production costs as a benchmark. Therefore, service costs can vary greatly by factors such as usage pattern, operating conditions, accessibility and professionalism of technicians (Rolstadaas, 2008). After-sale services of smart homes industry demand easy accessibility and high professionalism of technicians; therefore, in terms of current labor costs, sometimes the labor service costs may even be higher than the product cost. As as result, no smart home company can provide 24-hour online customer service to solve the issues encountered by users at any time currently.

Conclusion

The paper explores challenges of the development for smart home technologies in aspects of product quality, price and customer service quality. Quality challenges are broken into three major points including security problems, stability problems and availability problems. The case study of Mirai IoT Botnet showed safety concerns related to the adoption of smart home devices (Green, 2020). Subsequently, previous researches indicates stability and availability problems involved (Yang, 2018). To demonstrate how high prices may hinder adoption of smart home,

actual statistics (“Learn How Much”, n.d.) as well as users feedbacks (Alolayan, 2014) are shown and analyzed. Finally, the paper analyzes existing researches on service problems faced by smart home service providers (Kim, 2016).

References

Abomhara, M., & Køien, G. M. (2014, May). Security and privacy in the Internet of Things: Current status and open issues. In *2014 international conference on privacy and security in mobile systems (PRISMS)* (pp. 1-8). IEEE.

Ali, W., Dustgeer, G., Awais, M., & Shah, M. A. (2017, September). IoT based smart home: Security challenges, security requirements and solutions. In *2017 23rd International Conference on Automation and Computing (ICAC)* (pp. 1-6). IEEE.

Alolayan, B. (2014). Do I really have to accept smart fridges. In *ACHI 2014: Proceedings of the 7th International Conference on Advances in Computer-Human Interactions. p* (pp. 186-91).

Bitran, G. R., Rocha e Oliveira, P., & Schilkrut, A. (2008). Managing customer relationships through price and service quality.

Green, A. (2020, June 20). The mirai botnet attack and revenge of the internet of things. Retrieved April 09, 2021, from https://www.varonis.com/blog/the-mirai-botnet-attack-and-revenge-of-the-internet-of-things/

Hargreaves, T., Wilson, C., & Hauxwell-Baldwin, R. (2018). Learning to live in a smart home. *Building Research & Information*, *46*(1), 127-139.

Inside the infamous mirai iot botnet: A retrospective analysis. (2020, August 21). Retrieved April 09, 2021, from https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

Learn how much it costs to install a home automation system. (n.d.). Retrieved April 09, 2021, from https://www.homeadvisor.com/cost/electrical/install-or-repair-a-home-automation-system/

Ljubica Cvetkovska. (2021, February 26). 30 smart Home statistics for All high-tech enthusiasts. Retrieved April 09, 2021, from https://comfyliving.net/smart-home-statistics/#:~:text=How%20many%20smart%20homes%20are,grow%20to%2021.4%25%20by%202025.

Kim, S., & Yoon, J. (2016, July). An exploratory study on consumer's needs on smart home in Korea. In *International Conference of Design, User Experience, and Usability* (pp. 337-345). Springer, Cham.

Mashal, I., & Shuhaiber, A. (2019). What makes Jordanian residents buy smart home devices?. *Kybernetes*.

Mohammed, N. H., Abdullah, S., Salleh, S. M., Rashid, K. M., Hamzah, S. F. M., & Sudin, N. (2017). Relationship among Service and Product Quality, and Price in Establishing Customer Satisfaction. *Journal of Biological and Environmental Sciences*, *7*, 45-50.

Rolstadaas, A., Hvolby, H. H., & Falster, P. (2008). Review of after-sales service concepts. In *Lean business systems and beyond* (pp. 383-391). Springer, Boston, MA.

Shuhaiber, A., Mashal, I., & Alsaryrah, O. (2019, November). Smart homes as an IoT application: predicting attitudes and behaviours. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)* (pp. 1-7). IEEE.

Wickramasinghe, V., & Mathusinghe, K. (2016). After-sales services of home appliances: evidence from Sri Lanka. *International Journal of Consumer Studies*, *40*(1), 115-124.

Yang, H., Lee, H., & Zo, H. (2017). User acceptance of smart home services: an extension of the theory of planned behavior. *Industrial Management & Data Systems*.

Yang, E. (2018, February 12). Challenges in smart home: Battery life and real value from iot data. Retrieved April 09, 2021, from https://www.asmag.com/showpost/26329.aspx