International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 12 Issue 10, October- 2022
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

A QUANTITATIVE INVESTIGATION ON SMART HOME SECURITY AWARENESS AMONG SMART HOME USERS

Lakshmi B S
Department of Computer Science, Sunrise University, Alwar, Rajasthan
Dr. Jitendra Rai
Department of Computer Science, Sunrise University, Alwar, Rajasthan

Abstract
The technical innovation and concept of smart home employs coordinated and intelligent technologies to monitor and manage home appliances. In light of the fact that smart home performs as multi-user and multi-device systems, the devices confront new issues in terms of security, and accessibility. The study focuses to perform a survey analysis in context of smart home security among 380 smart home users with usage experience ranging more than 6 months to less than 2 years. The results obtained from the users highlighted that the security precautions must be established with strong Wi-Fi and Bluetooth configurations besides the regular security patch update and validation from manufacturer end.
Keywords: Smart home, Internet of things, Security, Quantitative study.

1. Introduction

Internet of Things (IoT) advancements have facilitated for the development of internet-enabled smart home appliances(Hammi et al., 2022). The underlying nature of smart homes has been identified as multi-user platforms. The provision of mutual authentication and key agreement are primaryactions in the configuration of a secure framework for the smart home environments. These actions are performed to prevent the unauthorised usage of home equipment and systems(Haney et al., 2021).

As development of technology has advanced, user expectations on smart home have shifted significantly, focusing the security systems and the convenience of home automation. In case of inadequate security systems, the users proclaim to attempt to disable the security measures, which will lead to a breach in security. The study focusesto investigate and analyse the security concerns and requirements of smart home in a user perspective context.

2. Literature Review

Zeng & Roesner (2019)conducted a semi-structured quantitative research with data collected from the interview with people using smart homes to learn about the usage and attitudes, expectations, and actions regarding security related to their smart homes. The findings shed light on thesecurity concerns suggesting accessibility methods and lay the foundation for the technology progresses further for increased adoption. An innovative and secure mutual authentication system was designed and built by Lin et al., (2020)which has applications, including smart homes. The proposed method incorporated blockchain technology, group signatures, and message authentication codes to provide a trustworthy securityin an effective manner.

In contrast to generic studies, Yu et al., (2021)provided evidence that demonstrated user scheme's inability to withstand security attacks such as impersonation and session key disclosure attacks, and secure user authentication. The study emphasized that as smart homedevicesmakes use of public-key cryptosystems, it is not appropriate for the use in settings that are associated with smart homes. The weaknesses that can be exploited were recognised as the primary subject of research byAlbany et al., (2022), which was centred on the security and the safety of smart homes devices. According to the findings of the study, the Blockchain system, the IoTArgos system, and the GHOST system were all built with the intention of enhancing the level of system security that is present in smart homes.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 12 Issue 10, October- 2022
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

3. Methodology

A quantitative study utilising large data(big data) from proprietors of smart homes was employed to conduct the investigation. Users with a population count of 380 were considered as the study participants having the usage experience of smart homes older than 6 months and less than 2 yearsin between the years 2020 – 2022. Additionally, participants were classified based on their knowledge on IoT and the data authentication mechanism deployed in their smart home devices. In order to better comprehend the user's knowledge on the safety and security of smart home devices, the responses and investigation in user perspective are crucial. The following questions, along with demographic data, were provided to the participants by means of a questionnaire.

S. No	Privacy questions in Questionnaire	Scale
1	Allowing government entities to retrieve data in the event of fatalities (Fire brigade)	Five-point Likert scale "Strongly agree" to "Strongly Disagree"
2	Setting up high level Bluetooth and Wi-Fi security	
3	Verifying the device makes sure the data source is trustworthy	
4	Smart home users' carelessness or neglect is as harmful as hackers	
5	Regular reviews of system security updates are required (from manufacturer end)	

Table 1: Details of Security questions considered for Questionnaire

4. Results and Discussion

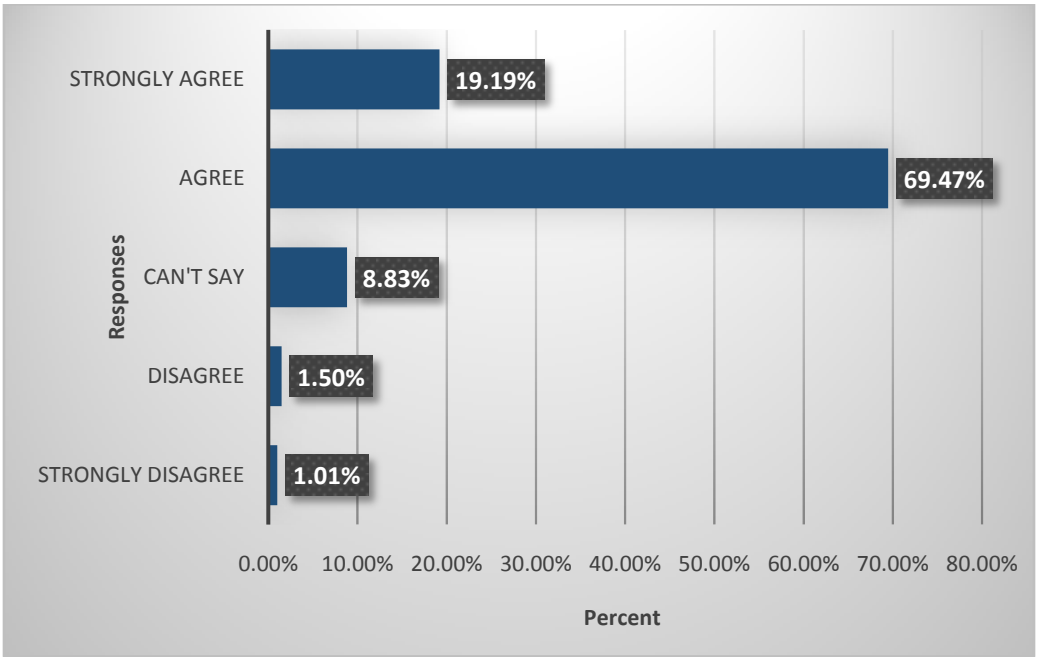

Figure 1: Representation showing responses on data retrieval by government entities

Figure 1 represents the responses and data obtained from the participants concerning the data retrieval by government entities in case of emergency.88% of users of smart homes agreed to share data with government agencies in the event of accidents/hazards or natural disasters, whereas 19% among them strongly agreed to reach for support from government for data retrieval.8.8% were not sure about the decision to reach government entities for support. 1.5% and 1.01% have shown that they disagree and strongly disagree with the idea of data sharing, respectively. The data presented in the figure 2 shows that 54 % of respondents strongly

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 12 Issue 10, October- 2022
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

acknowledged the importance of configuring their Wi-Fi networks. 36.4% of people shared the same viewpoint with low significance compared to the prior case.

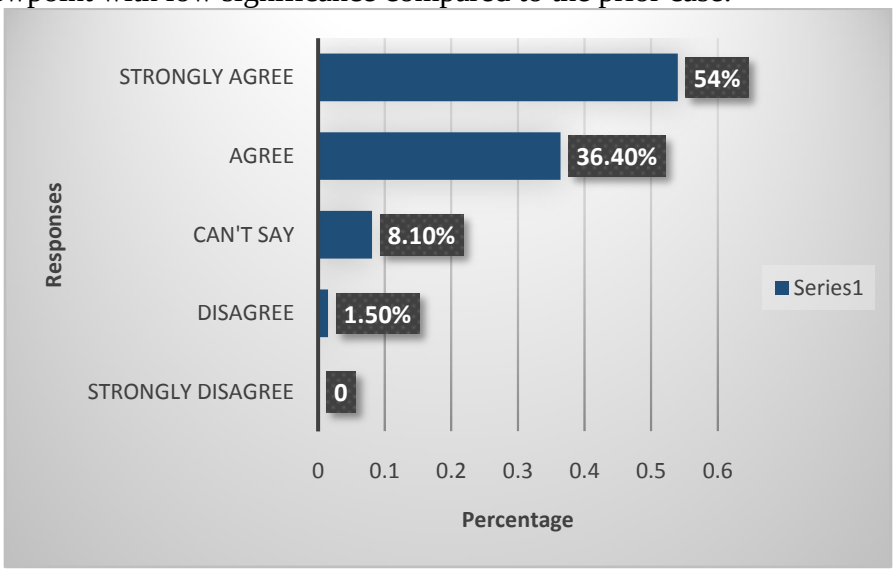

Figure 2: Representation showing responses on high level Bluetooth and Wi-Fi security requirement

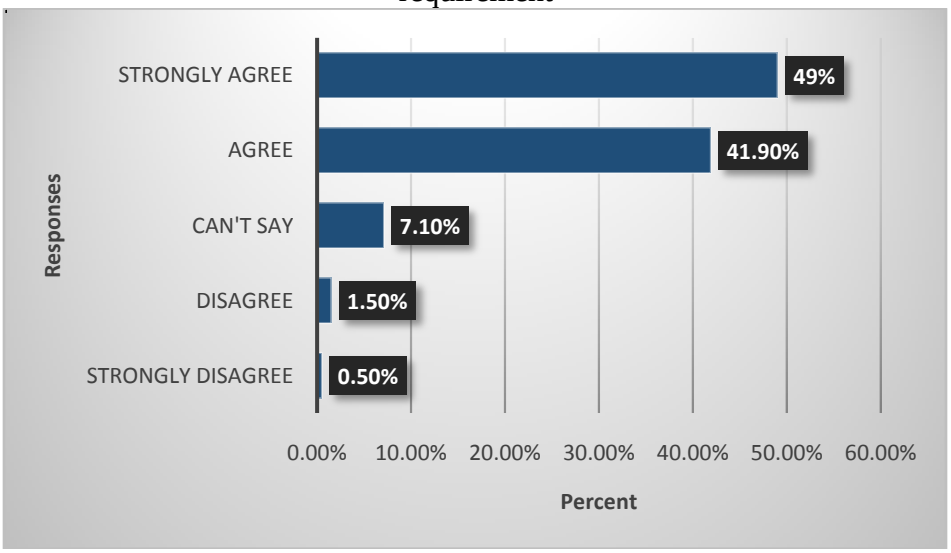

Figure 3: Representation showing responses on careless attitude towards smart home devices

Figure 3 shows only 2% of respondents (strongly disagreed & disagreed) with the fact that carelessness should be avoided to the greatest extent possible, while 90.9% of respondents (strongly agreed & agreed) that it is a threat and carelessness should be avoided whenever possible. It is evident that 7% of respondents do not have a clear understanding of the implications of the dangers that can result from user negligence. Figure 4 represents the statistical score for trust reliability in smart devices preventing security breaches, whereas 80% of users of smart homes have a general awareness of the significance of verifying their smart home devices. Only 15% of those polled were of the opinion that device verification wasn't all that important, and the rest of them had no concerns.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 12 Issue 10, October- 2022
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

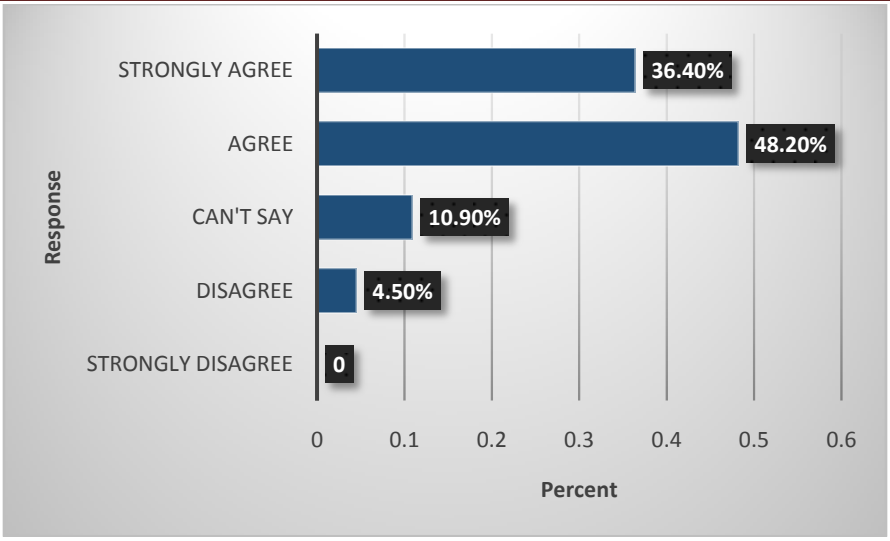

Figure 4: Representation showing responses on trust reliability on the smart device

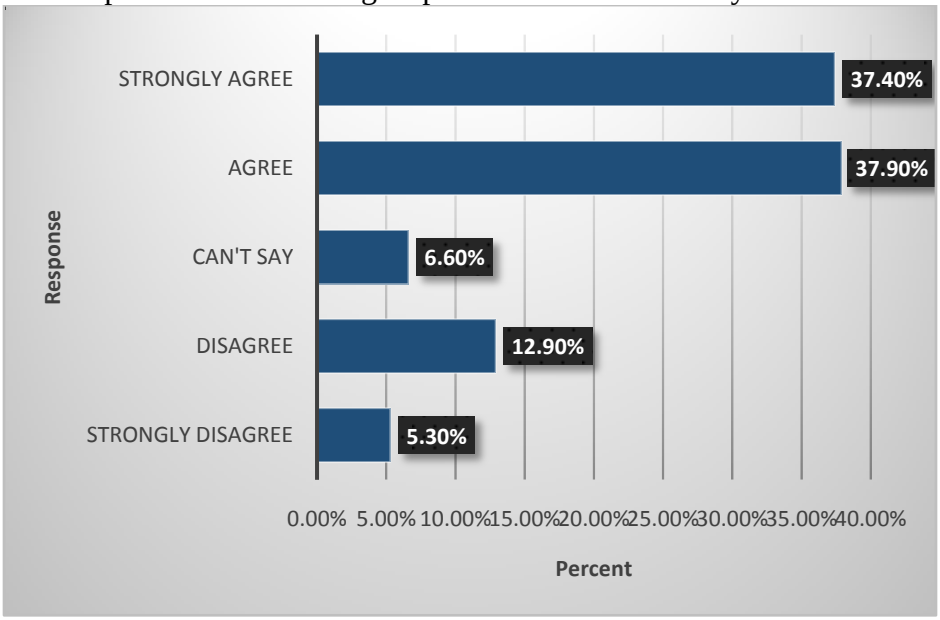

Figure 5: Representation showing responses on security updates from manufacturer end

According to the data from figure 5, the significant majority of respondents (75.3%), in this survey, manifested that the manufacturer or service provider should periodically review the access in smart home security systems. Only 18.2% of respondents disagreed with this statement, and 6.6% were clueless about it.

In the event of accidents, hazards, or natural disasters, it is clear from the responses that majority percent of those users are willing to share the day with government agencies. Certain percentage of users neglect asconsidering it as precautions to prevent data theft and misuse. Updates for IoT smart homes are recommended practice from manufacturers to distribute patches to fix security flaws. Security updates are one among the security measures available to users, as few expandable security options are insufficient or unavailable.The respondents displayed an adequate level of awareness regarding the dependability of the data source and validation. The device verification feature in smart home ecosystem garnered support from the vast majority of the survey's participants.Hackers will always focus their attention on vulnerable networks and devices. If a Wi-Fi or Bluetooth-based device operates with a low level of security, it has the possibility of being attacked by hackers with a malicious

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 12 Issue 10, October- 2022
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

programme.The question about the trade-off between cost and security elicited a variety of responses and indicated that there is still a need to develop the significance of security.

5. Conclusion

The discussed study focused on the security awareness and requirements among the smart home users. Henceforth, the study was performed with the quantitative data obtained from the smart home users providing valuable insights for the investigation and research. The findings of the study interprets that the smart home manufactures emphasisesthat the security patch has to be updated on a regular basis, for strengthening the security of smart devices. Since the capabilities of the device need to be an essential element of the service that is provided, these metrics can be of tremendous benefit to the supplier of the service for the device.

Reference

1. Albany, M., Alsahafi, E., Alruwili, I., & Elkhediri, S. (2022). A review: Secure Internet of thing System for Smart Houses. *Procedia Computer Science*, *201*(C), 437–444. https://doi.org/10.1016/J.PROCS.2022.03.057
2. Hammi, B., Zeadally, S., Khatoun, R., & Nebhen, J. (2022). Survey on smart homes: Vulnerabilities, risks, and countermeasures. *Computers and Security*, *117*. https://doi.org/10.1016/j.cose.2022.102677
3. Haney, J., Acar, Y., & Furman, S. (2021). "It's the company, the Government, you and I": User perceptions of responsibility for smart home privacy and security. *Proceedings of the 30th USENIX Security Symposium*.
4. Lin, C., He, D., Kumar, N., Huang, X., Vijayakumar, P., & Choo, K. K. R. (2020). HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes. *IEEE Internet of Things Journal*, *7*(2). https://doi.org/10.1109/JIOT.2019.2944400
5. Yu, S., Jho, N., & Park, Y. (2021). Lightweight Three-Factor-Based Privacy-Preserving Authentication Scheme for IoT-Enabled Smart Homes. *IEEE Access*, *9*, 126186–126197. https://doi.org/10.1109/ACCESS.2021.3111443
6. Zeng, E., & Roesner, F. (2019). Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. *Proceedings of the 28th USENIX Security Symposium*.