The Role of Smart Home in IOT

[1]Khushbu , [2]Ms.Anjali

Department of Computer Application

[1]Chandigarh School of Business Jhanjeri , Mohali

[2]Chandigarh Group of Colleges Jhanjeri , Mohali

[1] khushbudhariwal6@gmail.com

Abstract –**This paper outlines the design of a smart home system utilizing Internet of Things (IoT). Itexamines the current landscape of IoT in detail and proposes an approach based onService-Oriented Architecture (SOA) and component technology to achieve dynamic semanticintegration of web services. Additionally, it elucidates the software architecture and mainmodules of the system. Finally, the paper explores heterogeneous information fusion in thecontext of the Internet of Things.**

Smart homes, a vital component of the Internet of Things (IoT), seamlessly connect variousdigital devices to serve users effectively. These homes, envisioned as the cornerstone of aconnected future, offer users connectivity regardless of time and place. Smart home technology,based on IoT, has revolutionized human life by providing unprecedented levels of connectivityand convenience. This home's design was very unique and attractive. Today the world is anelectronic world and everyone is using smart homes. but these types of home's are very costlyand everyone does not put effort into these types of home's. So this is the biggest disadvantageof smart homes.

INTRODUCTION

IOT is an internet of Things based on some component technologies. IoT devices are essentialcomponents of the cloud computing ecosystem, especially in smart homes. They provide secureintegration and reduce stress in smart homes.

Smart Home These automated buildings are equipped with detection and control devices suchas air conditioning, heating, ventilation, lighting, and security systems. These gateways serve ascontrol systems with user interfaces that interact with various devices, managed through IoTnetwork connectivity. Smart home technology, synonymous with home automation, offershomeowners security, comfort, convenience, and energy efficiency by enabling control of smartdevices via smartphones or other networked devices.

Smart homes have several technical challenges, particularly regarding electric power qualityand security challenges. The integration of diverse generation sources and power electronicsdevices complicates power-quality control. To address these challenges, advancedcommunication schemes and AI-based techniques are essential to ensure harmony between modern sources and loads. Smart homes have different challenges. for example, securitychallenges, electric challenges, and so on.If you are not connected to the internet, then youcan'taccess this technology. That's why this is one of the biggest challenges of the smart home.The smart home has several applications used in today's world. This application is used veryeasily. There are different types of applications used in today's world. For example: home automation, energy management, remote monitoring and control, voice assistants, etc.Smart home systems automate tasks such as lighting control (light on and off), thermostatadjustments, door locking and unlocking (with unique passwords and fingerprints), andappliance control via smartphones or voice commands (only you can say on and off with yourvoice command). Smart security systems offer real-time monitoring and alerts through cameras,motion sensors, and smart locks, enhancing home security. Smart homes offer very highsecurity.Smart TVs, speakers, and home theater

systems offer seamless integration, allowingusers to control entertainment systems with voice commands and stream content from varioussources. For example, Alexa plays music. With the help of Smart Home, you can change yourlight color very easily with the commands and also on and off your home light. Virtual assistantslike Amazon Alexa, Google Assistant, and Apple Siri are integrated into smart home setups toprovide voice-controlled device management and perform tasks. With the help of these devices,you can turn on and off your home light very easily. You can say just Alexa lights on and off.

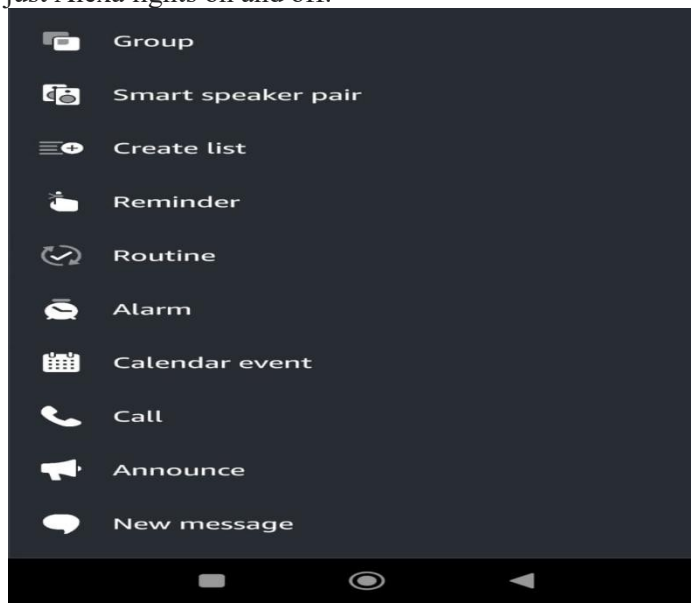

Figure 1: Connect with different devices

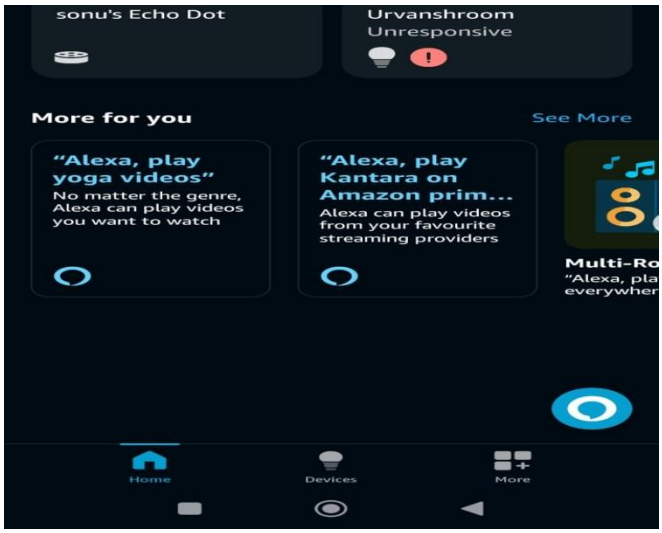

Figure 2: used different device

In the above figure, (1), and (2) show how to connect and control our smarthomes with smartphones. You can control your smart home with the help of smartphones anytime, anywhere, and with the help of the internet.

For example, if you are not in your home and guests are coming to your home, then youcan open your smart door lock with the help of your smartphone. There are differentdevices that you can handle very easily with the help of smartphones and the internet. If there is no internet connection, then you can't access and control this device.

For example, Alexa, a smart washing machine, lighting, etc.—everything you canhandle very easily. Alexa plays music, and you can also change your light color with thecommands and also on and off.

LITERATURE REVIEW

Disabled passwords: Many smart devices come with default or disabled passwords, so theft isvery easy to hack.Unencrypted Communication: Communication between smart devices andthe central hub or cloud servers may be unencrypted, exposing data to interception. InsecureAPIs and Interfaces: Insecure APIs or interfaces can be exploited by attackers to gainunauthorized access to smart devices or control them remotely. Privacy Concerns: Smartdevices collect a significant amount of personal data, raising privacy

concerns if this data ismishandled or accessed by unauthorized parties.Physical Security: Physical access to smartdevices can compromise their security, especially if they are easily tampered with or stolen.Denial-of-Service (DoS) Attacks: Smart home devices may be vulnerable to DoS attacks,disrupting their functionality or causing them to become unresponsive. Third-party Integrations:Integrating third-party services or devices with smart home systems can introduce additionalsecurity risks if these integrations are not properly secured. Insufficient User Awareness: Usersmay inadvertently compromise the security of their smart homes due to a lack of awareness about security best practices or the risks associated with certain actions.

RESEARCH METHODOLOGY

Security issues in smart homes can arise due to various vulnerabilities in the devices, networks, and protocols used.

1. Weak Passwords:Many smart devices come with default or weak passwords, making them susceptible to brute-force attacks.

Solution:Encourage users to change default passwords to strong, unique ones and enable two-factor authentication whenever possible.

2. Third-party Integrations:Integrating third-party services or devices with smart home systems can introduce additional security risks if these integrations are not properly secured.

Solution*:*Vet third-party services for security vulnerabilities, use secure authentication mechanisms, and limit the privileges granted to third-party integrations.

CONCLUSION AND FUTURE WORK

Smart home technology offers convenience, energy efficiency, security, and accessibility, but faces challenges like interoperability, security, privacy,and user acceptance. The future of smart homes is promising, but challenges include security,user experience, healthcare, smart cities, and ethical implications. Research is needed todevelop robust security mechanisms, understand user needs, and design user-friendlyinterfaces. Smart homes can also support aging in place, improve healthcare outcomes, and
integrate with urban infrastructure. Ethical considerations are also crucial to ensure technologybenefits all members of society.

Smart homes will continue to emphasize energy efficiency, automatically adjusting lighting,heating, and cooling based on occupancy and environmental conditions. They will also integraterenewable energy sources like solar panels more frequently. Health monitoring will becomestandard, with wearable sensors and smart appliances tracking vital signs and providingfeedback to users and healthcare providers. Security systems will advance with facialrecognition and predictive analytics, possibly incorporating drones and robotics for surveillance.Personalized experiences will be offered, catering to individual preferences in lighting, music,and even meal preparation. AI assistants will play a central role in coordinating devices andproviding personalized recommendations. Augmented reality interfaces will enable new ways ofinteracting with smart homes, such as visualizing renovations before making changes. Remotemonitoring and control will become more sophisticated, allowing homeowners to manage theirhomes from anywhere. Smart homes will also increasingly integrate into broader smart cityinitiatives, sharing data to optimize resource usage and enhance public safety. Additionally, theywill promote environmental sustainability through features like water-saving fixtures andautomated waste management. Interconnectivity will grow, facilitating seamlesscommunication between different systems and devices for more intelligent living spaces.

.

REFERENCES

1. Y. Nakamura, Y. Arakawa, T. Kanehira, M. Fujiwara, and K. Yasumoto, “SenStick:comprehensive sensing platform with an ultra tiny all-in-one sensor board for IoTresearch,” *Journal of Sensors*,vol. 2017, Article ID 6308302, 16 pages, 2017.View at: Publisher Site |Google Scholar
2. Mordorintelligence, “Global smart homes market—growth, analysis, forecast to2022,” https://www.mordorintelligence.com/industry-reports/global-smart-homes-market industry?

gclid=CIjd6MXjydYCFYYDKgod4ZQFaw.
View at: Google Scholar

3. V. Ricquebourg, D. Menga, D. Durand, B. Marhic, L. Delahoche, and C. Loge,"The smart home concept: our immediate future," in *2006 1ST IEEE InternationalConference on E-Learning in Industrial Electronics*,pp. 23–28, Hammamet,
Tunisia, 2006, IEEE.
View at: Publisher Site |Google Scholar

4. W. K. Edwards and R. E. Grinter, "At home with ubiquitous computing: sevenchallenges," in *Ubicomp 2001: Ubiquitous Computing*,pp. 256–272, Springer,Berlin, Heidelberg, 2001.
View at: Publisher Site |Google Scholar

5. N. Balta-Ozkan, R. Davidson, M. Bicket, and L. Whitmarsh, "Social barriers to theadoption of smart homes," *Energy Policy*,vol. 63, pp. 363–374, 2013.View at: Publisher Site |Google Scholar

6. R. Lutolf, "Smart home concept and the integration of energy meters into a homebased system," in *Seventh International Conference on Metering Apparatus andTariffs for Electricity Supply*,pp. 277-278, Glasgow, UK, 1992, IET.View at: Google Scholar

7. C. Kidd, R. Orr, G. Abowd et al., "The aware home: a living laboratory forubiquitous computing research," in *Cooperative Buildings. IntegratingInformation, Organizations, and Architecture*,pp. 191–198, Springer, Berlin,Heidelberg, 1999.
View at: Google Scholar

8. A. M. Adami, T. L. Hayes, and M. Pavel, "Unobtrusive monitoring of sleeppatterns," in *Proceedings of the 25th Annual International Conference of theIEEE Engineering in Medicine and Biology Society (IEEE Cat. No.03CH37439)*,vol. 2, pp. 1360–1363, Cancun, Mexico, 2003, IEEE.
View at: Publisher Site |Google Scholar

9. H. Andoh, K. Watanabe, T. Nakamura, and I. Takasu, "Network health monitoringsystem in the sleep," in *SINCE 2004 Annual Conference*,vol. 2, pp. 1421–1424,Sapporo, Japan, 2004, IEEE.
View at: Google Scholar

10. T. Koskela and K. Väänänen-Vainio-Mattila, "Evolution towards smart homeenvironments: empirical evaluation of three user interfaces," *Personal andUbiquitous Computing*,vol. 8, no. 3-4, pp. 234–240, 2004.
View at: Publisher Site |Google Scholar

11. A.-G. Paetz, B. Becker, W. Fichtner, and H. Schmeck, "Shifting electricitydemand with smart home technologies—an experimental study on useracceptance," in *30th USAEE/IAEE North American Conference*,vol. 19, p. 20,Washington, DC, USA, 2011.
View at: Google Scholar

12. A. Leeraphong, B. Papasratorn, and V. Chongsuphajaisiddhi, "A study on factorsinfluencing elderly intention to use smart home in Thailand: a pilot study," in *The10th International Conference on e-Business*,Bangkok, Thailand, 2015.View at: Google Scholar

13. A. Alaiad and L. Zhou, "Patients' behavioral intentions toward using WSN basedsmart home healthcare systems: an empirical investigation," in *2015 48th HawaiiInternational Conference on System Sciences*,pp. 824–833, Kauai, HI, USA,2015, IEEE.
View at: Publisher Site |Google Scholar

14. X. Fan, Q. Xie, X. Li et al., "Activity recognition as a service for smart home:ambient assisted living application via sensing home," in *2017 IEEE InternationalConference on AI & Mobile Services (AIMS)*,pp. 54–61, Honolulu, HI, USA,2017, IEEE.
View at: Publisher Site |Google Scholar

15. L. Vadillo, M. L. Martín-Ruiz, I. Pau, R. Conde, and M. Á. Valero, "A smarttelecare system at digital home: perceived usefulness, satisfaction, andexpectations for healthcare professionals," *Journal of Sensors*,vol. 2017, ArticleID 8972350, 12 pages, 2017.
View at: Publisher Site |Google Scholar

16. H. Bao, A. Y. L. Chong, K. B. Ooi, and B. Lin, "Are Chinese consumers ready toadopt mobile smart homes? An empirical analysis," *International Journal ofMobile Communications*,vol. 12, no. 5, pp. 496–511, 2014.
View at: Publisher Site |Google Scholar

17. E. Park, Y. Cho, J. Han, and S. J. Kwon, "Comprehensive approaches to useracceptance of Internet of Things in a smart home environment," *IEEE Internet of Things Journal*,vol. 4, no. 6, pp. 2342–2350, 2017.
View at: Publisher Site |Google Scholar

18. J. Ji, T. Liu, C. Shen et al., "A human-centered smart home system withwearable-sensor behavior analysis," in *2016 IEEE International Conference on Automation Science and Engineering (CASE)*,pp. 1112–1117, Fort Worth, TX,USA, 2016, IEEE.
View at: Publisher Site |Google Scholar

19. S. Tanwar, P. Patel, K. Patel, S. Tyagi, N. Kumar, and M. Obaidat, "An advancedInternet of Thing based security alert system for smart home," in *2017International Conference on Computer, Information and TelecommunicationSystems (CITS)*,pp. 25–29, Dalian, China, 2017, IEEE.
View at: Publisher Site |Google Scholar

20. E. Elmasllari and A. Al-Akkad, "Smart energy systems in private households:behaviors, needs, expectations, and concerns," in *2017 IEEE 14th InternationalConference on Networking, Sensing and Control (ICNSC)*,pp. 152–157,Calabria, Italy, 2017, IEEE.

View at: Publisher Site |Google Scholar