International Journal of Inventive Engineering and Sciences (IJIES)
ISSN: 2319-9598 (Online), Volume-11 Issue-12, December 2024

Augmenting Security of Smart Homes

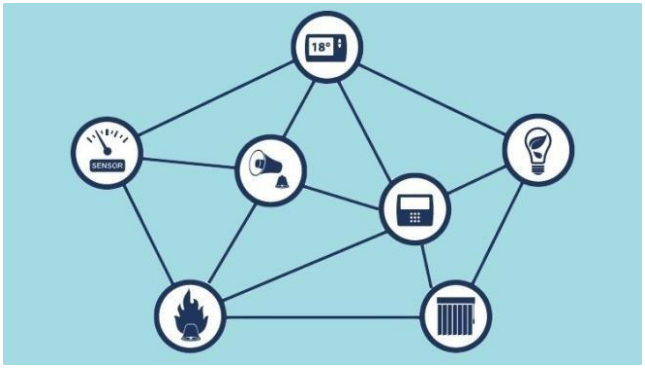
Narsaiah Putta, Raman Dugyala, Pallati Narsimhulu

Abstract: ***The development of new technology and people's propensity to rely on it more and more each year have led to enormous advancements in human technology. The idea of the Internet of Things (IOT) and later "Smart Homes" was one such vast step. The introduction of efficient and affordable technologies drives the surge in the smart home sector. However, the expanded use has also created a new set of security and privacy risks for those who rely on smart home technology. This article explores the fundamental concept of smart homes and IoT devices, including current risks and proposed countermeasures.***

Keywords: Internet of Things (IOT), Smart Homes, Network Security, Wireless communications and Sensor Networks.

I. INTRODUCTION

A subset of the widely acknowledged and adopted idea of "Internet of Things," the smart home or home automation (IOT). It offers homeowners a wide range of features, including privacy, security, and remotely controlled and automated lighting and sound [1]. Most commonly, smart houses use three well-known protocols, namely WiFi. such as Z-wave and Zigbee [2]. ZigBee and Z wave have only been used in the realm of home automation, but WiFi is more known for its usefulness in general internet applications [3]. They are both mesh network-based and excellent for near-field communication.



[Fig.1: ZigBee Based Architecture] [1]

Manuscript received on 25 August 2024 | Revised Manuscript received on 13 December 2024 | Manuscript Accepted on 15 December 2024 | Manuscript published on 30 December 2024.

* Correspondence Author

Narsaiah Putta*, Assistant Professor, Department of CSE, Vasavi College of Engineering, Hyderabad (Telangana), India. Email ID: p.narsaiah@staff.vce.ac.in

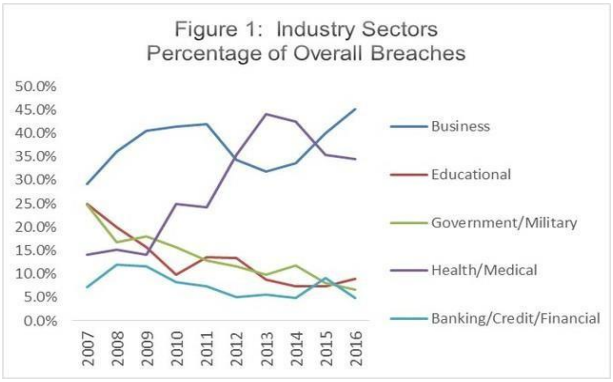
Raman Dugyala, Professor, Department of CSE, Chaitanya Bharathi Institute of Technology, Hyderabad (Telangana), India. Email ID: raman.vsd@gmail.com

Pallati Narsimhulu, Assistant Professor, Department of CSE, Chaitanya Bharathi Institute of Technology, Hyderabad (Telangana), India. Email ID: narsimhulupallati_cse@cbit.ac.in

II. SECURITY CHALLENGES OF SMART HOMES

Due to its interconnectedness, home automation and the IOT concept as a whole face the same difficulties as the rest of the internet. Smart homes are also a source of concern for the three main areas of cybersecurity, namely confidentiality, authenticity, and access [4].

Interconnected networks and devices were already relatively common in commercial settings before they started to appear in the housing sector [5]. According to research done in the UK in 2015 [6], network security breaches affected 90% of large firms and 74% of small organizations, up around 14% from the year before [7].



[Fig.2: Increase in Network Security Breaches] [5]

The issue of vulnerability is one more security issue to be concerned about [8]. The privacy of home inhabitants and the security of their data are now much more at risk due to the introduction [9] of device scanning search engines that look for accessible sensors like unprotected cameras and microphones [10].

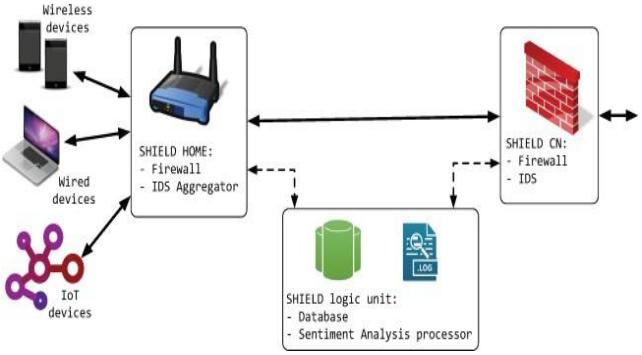
III. LITERATURE REVIEW

The necessity of addressing and overcoming these difficulties and weaknesses has recently come to light [11], and as a result, numerous solutions have been put forth. This essay lists a few of these remedies, including the following:

A. SHIELD System

The authors advocate using a novel architecture that is not dependent on existing IOT network standards but enables the interoperability of numerous devices in a smart home setting [12].

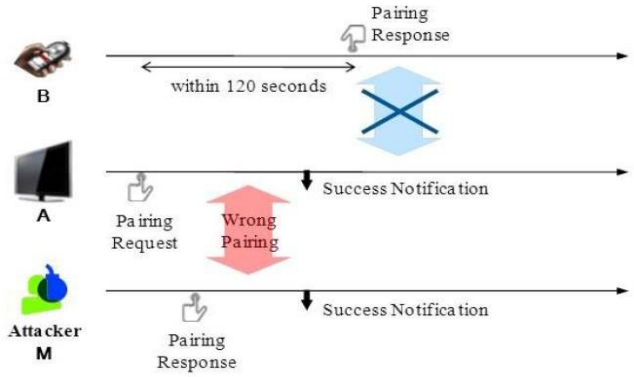
Setting up firewalls at the Internet Service Provider (ISP) level is standard procedure, but that is insufficient because the intrusion could also occur from within the smart home. Using a mobile device that is infected, for instance. It is advised that intrusion detection systems (IDS) be put up both at the ISP and premises level to Address this issue.



[Fig.3: SHIELD Architecture]

B. Security Enhanced Push Button Configuration

The authors of the paper offered a more thorough, "security-enhanced push button configuration for smart home networks" by extending the study from paper [14]. By calculating the distances to each target device, their method employs ultrasound sensors to determine whether the pairing message is coming from the intended device. Their strategy essentially suggests a secure handshake connection distance measuring technique that forbids an attacker from fraudulently modifying data coming from outside the range of a smart home [13].



[Fig.4: Security Enhanced Push Button Configuration] [14]

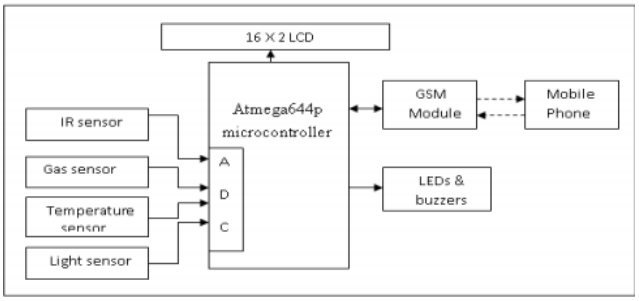
C. Securing 6LoWPAN

For WPANs, IEEE has selected the 802.15.4 standard [15]. The 6LoWPAN protocol, created to transfer IPv6 packets across 802.15.4 standard networks, is one of the few protocols that operate by this standard and is intended to be effective in low-cost, speed, and energy applications [16].

An "Enhanced Authentication and Key Establishment Scheme for 6LoWPAN networks (EAKES6Lo)" has been proposed by the authors of the paper [17]. It is carried out in two stages: The data is encrypted and its integrity is verified in phase 1 using network security methods such as AES (Advanced Encryption Standard) and SHA (Secure Hashing Algorithm). Phase 2 settles the confirmation and key foundation processes by establishing a mutual authentication through the exchange of six messages.

D. Security System for Smart Homes Based on GSM

Simple network security is insufficient when discussing smart home security because numerous other elements can compromise a house's security [18]. The authors of the paper suggest an interior network of several sensors, including infrared, gas, temperature, and light sensors that are connected via a microcontroller to a GSM unit and can alert the owners or inhabitants anytime there is a breach or abnormality in the systems being monitored [19].

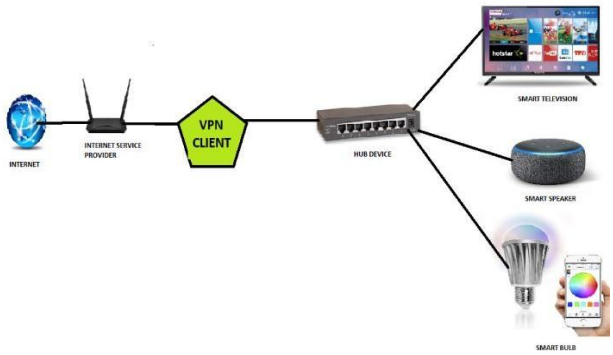


[Fig.5: Security System Design Based on GSM] [18]

IV. PROPOSED SOLUTION

A. VPN Enabled Network Architecture

The majority of smart home appliances use the internet in addition to their low energy standard to gather information for the user, stream videos, music, and other things [20]. The fact that most hub devices are directly connected to the home network of the Internet service provider can make them more vulnerable, as an attacker can easily access and acquire information from them. In this study, a network architecture for smart homes is proposed, in which a Virtual Private Network (VPN) client is used to connect the hub device to a second ISP connection.



[Fig.6: The Proposed Architecture]

The inclusion of a VPN gives the network a different identity, reducing its susceptibility to nearby attacks. As the displayed location was not the actual one, it also makes it more difficult for any attacker to identify the specified network and then target it. Our suggested architecture consists of three hardware components, as shown in Fig. 5, which are listed along with their respective roles.

i. **Smart Home Devices:** A wide variety of smart home devices are available on the market today, which can control various aspects of our homes, connect to the internet, and even respond to voice commands. We can see a smart TV, a smart speaker, and a bright bulb connected to a hub device in the image.

ii. **Hub Device:** There are many different types of hub devices, but we recommend a network hub device that utilises a VPN client to connect all smart home devices to the primary ISP router.

iii. **ISP Router:** A well-known tool that enables us to access the internet is the

internet service provider's router or modem.

B. Role of VPN: The function of a VPN client is crucially important here. We can establish a remote connection to a completely different place using a virtual private network. Due to this network's excellent privacy and security, it is significantly more difficult for a smart home system to experience a security breach. We noted that the architecture we are suggesting is considerably less complex and comparably more cost-effective, even though the proposed solution does not offer the same level of security and encryption as most other systems that have been previously proposed. The cost of research and development, as well as exclusive programming, is also eliminated because all components of our system require only low-cost software and hardware.

V. CONCLUSION

The complexity of dealing with new and emerging dangers that hinder the efficient and secure operation of technology used to make our lives more comfortable and efficient will increase as that technology's level of development advances. Researchers and developers must adopt a holistic and dynamic approach to address the persistent security issues in the fields of smart homes and IoT. Attacks can differ in their purpose, style, and even location. The requirement of the future isn't to establish a security standard, but rather to develop fundamental principles that support the creation of various security structures according to the circumstances.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/Competing Interests:** Based on my understanding, this article does not have any conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it was conducted without any external influence.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Alam, M.R.; Reaz, M.B.I.; Ali, M.A.M. A Review of Smart Homes—Past, present, and future. *IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev..)* 2012, *42*, 1190–1203. DOI: https://doi.org/10.1109/TSMCC.2012.2189204
2. Lin, H., & Bergmann, N. (2016). IoT privacy and security challenges for smart home environments. *Information*, *7*(3), 44. DOI: https://doi.org/10.3390/info7030044
3. Price Waterhouse Coopers (PwC). *Information Security Breaches Survey 2015*; HM Government: London, UK, 2015. https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf
4. Patton, M.; Gross, E.; Chinn, R.; Forbis, S.; Walker, L.; Hsinchun, C. Uninvited connections: A study of vulnerable devices on the Internet of Things (IoT). In Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference (JISIC), The Hague, The Netherlands, 24–26 September 2014; pp. 232–235. DOI: https://doi.org/10.1109/JISIC.2014.43
5. Pecorella, T., Pierucci, L., & Nizzi, F. (2018). "Network Sentiment" Framework to Enhance Security and Privacy in Smart Homes. Future Internet, 10(12), 125. https://doi.org/10.3390/fi10120125
6. Park, Y.; Park, T.; Park, M.; Han, J. How to Secure Push Button Configuration for Remote Control of Devices. In Proceedings of the 10th International Conference on Remote Engineering and Virtual Instrumentation (REV), Sydney, Australia, 6–8 February 2013. DOI: https://doi.org/10.1109/REV.2013.6502906
7. Han, J., & Park, T. (2017). Security-Enhanced Push Button Configuration for Home Smart Control. *Sensors*, *17*(6), 1334. DOI: https://doi.org/10.3390/s17061334
8. Shelby, Z.; Bormann, C. *6lowpan: The Wireless Embedded Internet*; John Wiley & Sons: New York, NY, USA, 2011; Volume 43. https://www.wiley.com/en-us/6LoWPAN%3A+The+Wireless+Embedded+Internet-p-9781119965343
9. Yue, Q.; Maode, M. An authentication and key establishment scheme to enhance security for M2M in 6LoWPANs. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 2671–2676. DOI: https://doi.org/10.1109/ICCW.2015.7247582
10. V. Karri and J. S. Daniel Lim, "Method and Device to Communicate via SMS After a Security Intrusion", 1st International Conference on Sensing Technology, Palmerston North, New Zealand, (2005) November 21- 23. https://www.academia.edu/20866609/Method_and_Device_to_Communicate_via_SMS_After_a_Security_Intrusion
11. Bangali, J., & Shaligram, A. (2013). Design and Implementation of Security Systems for Smart Homes Based on GSM Technology. *International Journal of Smart Home*, *7*(6), 201-208. https://gvpress.com/journals/IJSH/vol7_no6/19.pdf
12. Robles, R. J., Kim, T. H., Cook, D., & Das, S. (2010). A review on security in smart home development. *International Journal of Advanced Science and Technology*, *15*. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=f07fd4d666c9fe05e49501884054f6041d554ad5
13. Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security Analysis of Emerging Smart Home Applications. In *2016 IEEE symposium on security and privacy (SP)* (pp. 636-654). IEEE. DOI: https://doi.org/10.1109/SP.2016.44
14. Jiang, L., Liu, D. Y., & Yang, B. (2004, August). Smart home research. In *Proceedings of 2004 International Conference on Machine Learning and Cybernetics (IEEE Cat. No. 04EX826)*(Vol. 2, pp. 659-663). IEEE. DOI: https://doi.org/10.1109/ICMLC.2004.1382266
15. Davidoff, S., Lee, M. K., Yiu, C., Zimmerman, J., & Dey, A. K. (2006, September). Principles of smart home control. In *International Conference on Ubiquitous Computing* (pp. 19-34). Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/11853565_2
16. Aloul, F., Al-Ali, A. R., Al-Dalky, R., Al- Mardini, M., & El-Hajj, W. (2012). Smart grid security: Threats, vulnerabilities and solutions. *International Journal of Smart Grid and Clean Energy*, *1*(1), 1-6. https://www.ijsgce.com/uploadfile/2012/1011/20121011121836539.pdf
17. Lee, C., Zappaterra, L., Choi, K., & Choi, H. A. (2014, October). Securing the Smart Home: Technologies, Security Challenges, and Security Requirements. In *2014 IEEE Conference on Communications and Network Security* (pp. 67-72). IEEE. DOI: https://doi.org/10.1109/CNS.2014.6997467
18. Yoon, S., Park, H., & Yoo, H. S. (2015). Security Issues in Smart Homes in IoT Environments.In *Computer Science and Its Applications* (pp. 691- 696). Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-662-45402-2_97

19. Raza, S., Trabalza, D., & Voigt, T. (2012, May). 6LoWPAN compressed DTLS for CoAP.In *2012, the IEEE 8th International Conference on Distributed Computing in Sensor Systems* (pp. 287-289). IEEE. DOI: https://doi.org/10.1109/DCOSS.2012.55
20. Theoharidou, M., Tsalis, N., Gritzalis, D. (2017). Smart Home Solutions: Privacy Issues. In: van Hoof, J., Demiris, G., Wouters, E. (eds) Handbook of Smart Homes, Health Care and Well-Being. Springer, Cham. https://doi.org/10.1007/978-3-319-01583-5_5