THE ARCHITECTURE OF SMART HOME INTERNET OF THINGS

DOI: 10.36724/2072-8735-2021-15-8-58-61

Manuscript received 07 June 2021;
Accepted 30 June 2021

Al namer Zainal,
Moscow Technical University of Communications and Informatics, Moscow, Russia,
zainalnamer29@gmail.com

Keywords: *Smart home, smart buildings, smart devices, gateway, network topology*

Modern society lives in the age of high and smart technologies. Innovative technologies are included in every part of our life. Almost all people use the innovations of scientific and technological progress in order to reduce costs, effort and time. Smart technology – a new approach to the organization of its goals, which allows to combine all available information at an early stage, to determine the list of necessary materials, set deadlines for execution of works and perform the task and clear to all participants of the process. Smart Home is a solution in which the operation and control of all systems at the level of an individual household is automated, providing a specific room with a high level of security and all the necessary living conditions, while remotely without unnecessary interference from service organizations. The building is equipped with special monitors with sensors that help detect threats to both the system and the residents themselves. One of the popular and developing trends and technologies in the Internet of Things today is "Smart- Home Internet of Things" (smart home of the Internet of Things) – SH-IoTs, which is designed for the most comfortable life of people through the use of modern high-tech means. In the modern concept of the smart home system of the Internet of Things SH-IoTs, as a rule, they invest in the automation of everyday, routine actions. For example, in the event of a fire in a room with special sensors installed, the smart home system will de-energize all electrical appliances in this room, etc.

Information about author:
Al namer Zainal, *PhD student, Moscow Technical University of Communications and Informatics, Moscow, Russia*

Для цитирования:
Аль намер Зайнал. Архитектура умного дома интернет вещей // T-Comm: Телекоммуникации и транспорт. 2021. Том 15. №8. С. 58-61.

For citation:
Al namer Zainal (2021). The architecture of smart home internet of things. *T-Comm*, vol. 15, no.8, pp. 58-61. (*in Russian*)

A smart home defined, as a cyber-physical system built based on the Internet of Things computers and smart electrical appliances with human interaction through home communication networks on the Internet. In a smart home system, the controller is the gateway and controls the smart home devices that control the home environment and serve home users [1-3].

The concept of "smart home - SHIoTs" implies the automation of processes occurring in the household. For this, a network of interconnected mechanical and digital devices is used that can communicate with each other and with the user to create an interactive space [4]. This goal can be achieve in two ways [5]:

- Defining user activities as a basis for increasing the degree of automation in the household.
- Applying remote home control to improve comfort, improve safety, monitor and reduce energy consumption, as well as reduce emissions of harmful gases and environmental pollution.

To make it clearer what we will study and what models we can assume to eliminate gateway problems, we are conducting a typical architecture of a smart home. SH-IoTs devices use for a variety of home monitoring and automation tasks such as smart locks and doorbells, temperature (medical) and humidity sensors, and smart speakers for home help or music streaming. The SH-IoTs market has grown rapidly over the past few years. More than 832 million devices for SH-IoTs expect to be shipping worldwide in 2022 [6].

SH-IoTs devices connect to the Internet to perform many of their tasks, such as accessing weather forecast services to control the home environment and accessing media streaming services for entertainment. Perhaps unsurprisingly, SH-IoTs traffic is currently the primary source of overall Internet traffic. SH-IoTs traffic expects to account for more than half of all Internet traffic by 2022. It is expecting that by 2022, 48% of all IoT traffic will be SH-IoTs devices [7].

The proliferation of the smart home IoT has caused many problems such as governance (e.g. device identification [8], [9]), security ([10], [11]) and privacy (e.g., SH-IoTs devices leaking confidential information. [12], [13]). Addressing these challenges is driving research to understand how SH-IoTs devices designed, deployed and used. However, carrying out this study is fraught with a number of problems.

First, the IoT ecosystem of the smart home fragmented by a multitude of devices, which, as a rule, cannot be verifies through standard interfaces. To solve this problem, we use the home gateway as a universal point of view to inspect the network traffic generated by SH-IoTs devices without the need for their individual tooling.

Second, the behavior of IoT devices in a smart home depends on the environment in which they are located. While SH-IoTs devices can be studding in controlled test environments [14, 15] this may not reflect their behavior in the real world.

Therefore, we study SH-IoTs devices in real-world settings using home gateway tools. This allows us to capture the behavior of an IoT device in the real world. Finally, studying the behavior of a smart home on the Internet of Things at scale is cumbersome.

The diversity in the SH-IoTs market in terms of device types and manufacturers makes it difficult for researchers to obtain information or propose solutions that are applicable to the broader IoT ecosystem of the smart home.

The smart home environment can be observing through a layered architecture, which is a characteristic of the IoT concept, consisting of four main layers (perception, network, middleware and application) as shown in Figure 1 [7].

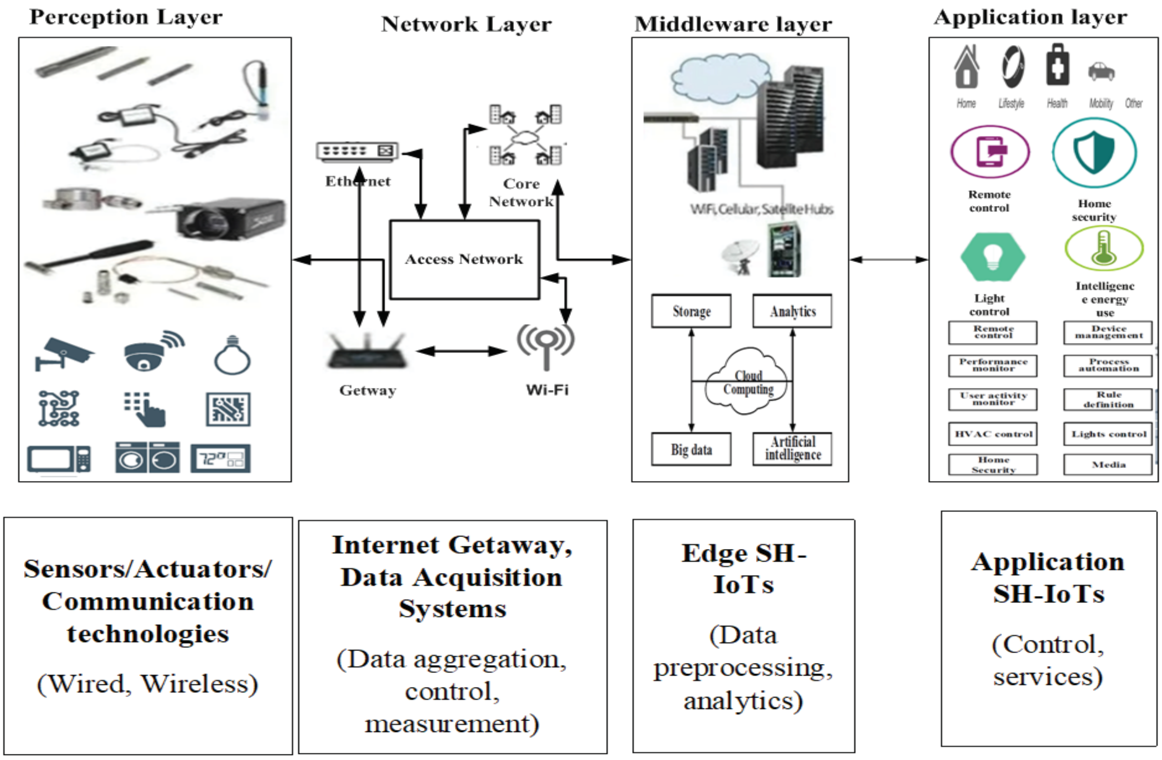

Fig. 1. Architecture of Smart Home Internet of Things environment

Perception Layer. The sensory layer includes sensors, actuators, and communication technologies that allow data to be transmitters to an IoT hub. The hub in this system is located at the network level, and the gateway is the hub of the Internet of Things in this system. Sensors and actuators use energy-efficient communication technologies, according to how much energy is needed (extended autonomy). The smart home most often uses short-range technologies such as IEEE 802.15.4 ZigBee, ITU-T G.9959 Z-Wave, or Bluetooth Low Energy BLE.

The gateway of the Internet of Things in the smart home system will provide mutual communication of the device, the levels of perception and its connection with the access network for transmitting data packets to the intermediate level [8].

Middleware layer. Traditional access technologies such as XDSL, fiber optic, mobile data packet networks (3G, 4G, and 5G) and similar are used to transfer data packets from the access network to the intermediate layer.

The middleware layer is based on the concept of cloud computing and contains resources and data processing elements generated in the middleware layers to convert received messages into useful information for the user. This level has three main functions:

1. Remote connection of users to devices of the smart home system SH-IoTs for remote control,
2. Automation of management of SH-IoTs devices based on information obtained without the mediation of users,
3. Transfer of information to user terminal devices to provide information.

Application layer. The application layer allows you to provide various services as well as remote control of devices using various applications. SH-IoTs network is a network connecting device intelligent appliances and actuators that respond to user input and system monitor each other (provider), e.g., remote control devices, or intelligent actuators and heating systems, automatically adapting to the outdoor temperature [16].

The smart home network is rapidly evolving and including heterogeneous physical access (both wired and wireless) and a large number of smart devices that generate different types of traffic with different distributions. In addition, a variety of applications in the smart home system (VoIP, instant messaging, video conferencing, video, etc.) to different requirements imposes additional restrictions on traffic planning in the system of smart home, such as congestion and delay.

This requires automated traffic load management at the home gateway, by pretending more than one priority class. From the perspective of the provider of the Internet (Internet service Providers- ISP), these classes are determined based on the bandwidth requirements for mission-critical applications with a field view of IP ToS services (Internet Protocol Type of Service) [17].

From another point of view, that is, from the point of view of the home user, the priority classes correspond to traffic latency, especially for a streaming video application. For example, packets that are generating by medical sensors have a higher priority than packets generated streaming devices (video streaming traffic).

On the other hand, TV streaming devices from 400 kbps to 14000 kbps require lower priority and lower maximum latency compared to periodic sensing objects such as medical sensors with data rates from 12 bps to 12 kbps [18, 19].

Conclusion

Smart technology – a new approach to the organization of its goals, which allows to combine all available information at an early stage, to determine the list of necessary materials, set deadlines for execution of works and perform the task and clear to all participants of the process. Smart Home is a solution in which the operation and control of all systems at the level of an individual household is automated, providing a specific room with a high level of security and all the necessary living conditions, while remotely without unnecessary interference from service organizations. The building is equipped with special monitors with sensors that help detect threats to both the system and the residents themselves.

References

1. B.S. Goldstein, A.E. Kucheryavy (2013). Communication networks post NGN. St. Petersburg: BHV-S. Petersburg. 160 p.
2. A.V. Roslyakov, S.V. Vanyashin, A.Y. Grebeshkov, M.Yu. Samsonov (2014). Internet of Things. Samara: PSUTI, As Guard Publishing House. 342 p.
3. S. Suresh and P. V. Sruthi (2015), "A review on smart home technology," in 2015 Online International Conference on Green Engineering and Technologies (IC-GET), Nov 2015, pp. 1-3.
4. G. Lobaccaro, S. Carlucci, and E. Löfström (2016), "A review of systems and technologies for smart homes and smart grids," Energies, vol. 9, no. 5, pp. 1-33.
5. A. Saad al-sumaiti, M.H. Ahmed, and M.M. A. Salama (2014), "Smart Home Activities: A Literature Review," Electr. Power Components Syst., vol. 42, no. 3-4, pp. 294-305.
6. IDC. Double-Digit Growth Expected in the Smart Home Market. https: //www.idc.com/getdoc.jsp?containerId=prUS44971219, March 2019.
7. Cisco Visual Networking Index: Forecast and Trends, 2017–2022, White Paper, 2019.
8. A. Sivanathan, H. H. Gharakheili, F. Loi, A. Radford, C. Wijenayake, A. Vishwanath, and V. Sivaraman (2018). Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics. In IEEE Transactions on Mobile Computing'18.
9. J. Ortiz, C. Crawford, and F. Le (2019). DeviceMien: network device behavior modeling for identifying unknown IoT devices. In ACM IoTDI'19.
10. M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou (2017). Understanding the Mirai Botnet. In USENIX Security'17.
11. L. Franceschi-Bicchierai (2016). How 1.5 Million Connected Cameras hijacked to make an Unprecedented Botnet. https://motherboard.vice.com/en us/article/8q8dab/15-millionconnected- cameras-ddos-botnet-brian-krebs.
12. G. Chu, N. Apthorpe, and N. Feamster (2019). Security and Privacy Analyses of Internet of Things Childrens Toys. IEEE Internet of Things'19.
13. D. Wood, N. Apthorpe, and N. Feamster (2017). Cleartext Data Transmissions in Consumer IoT Medical Devices. In ACM Workshop on Internet of Things Security and Privacy (IoT S&P)'17.
14. J. Ren, D. J. Dubois, D. Choffnes, A. M. Mandalari, R. Kolcun, and H. Haddadi (2019). Information Exposure from Consumer IoT Devices. In ACM IMC'19.
15. O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose (2019). SoK: Security Evaluation of Home-Based IoT Deployments. In IEEE Symposium on Security and Privacy (S&P)'19.
16. D. Marikyan, S. Papagiannidis, and E. Alamanos (2019), "A systematic review of the smart home literature: A user perspective," *Technol. Forecasting Social Change*, vol. 138, pp. 139-154, Jan. 2019.
17. H. Pfeffer (2016), "Dynamic changing tier service on test device," U.S. Patent 9 425 977, Aug. 23, 2016.
18. (2018). *Internet Connection and Recommended Encoding Settings*. Accessed: Dec. 16, 2018 [Online]. Available: https://support.video.ibm.com/hc/en-us/articles/207852117-Internet-connection-andrecommended-encoding-settings.
19. W. Leister, P. A. Floor, Y. B. Woldegiorgis, I. Balasingham, and H. Abie (2012), "De_ning the asset lab," Norsk Regnesentral, Norway, Tech. Rep., 2012. [Online]. Available: http://publications.nr.no/1362402875/DART-16-2012.pdf.

АРХИТЕКТУРА УМНОГО ДОМА ИНТЕРНЕТ ВЕЩЕЙ

Аль намер Зайнал, *Московский технический университет связи и информатики, Москва, Россия,*
zainalnamer29@gmail.com

Аннотация
Современное общество живет в веке высоких и умных технологий. Инновационные технологии входят в каждую часть нашей жизни. Практически все люди используют новшества научно-технического прогресса в целях уменьшения затрат, силы и времени. Одна из популярных и развивающихся в Интернете вещей тенденций и технологий на сегодня является "Smart- Home Internet of Things" (умный дом интернета вещей) – SH-IoTs, которая предназначена для максимально комфортной жизни людей посредством использования современных высокотехнологических средств. В современном понятии системы умного дома интернета вещей SH-IoTs, как правило, вкладывают автоматизацию бытовых, рутинных действий. Например, при возгорании в комнате с установленными специальными датчиками система умного дома обесточит все электроприборы в данном помещении и т.д.

Ключевые слова: *умный дом, интеллектуальные здания, интеллектуальные устройства, шлюз, типология сети.*

Литература

1. *Goldstein B.S., Kucheryavy A.E.* Communication networks post NGN. St. Petersburg: BHV-S. Petersburg, 2013. 160 p.
2. *Roslyakov A.V., Vanyashin S.V., Grebeshkov A.Y., Samsonov M.Yu.* Internet of Things; ed. A. V. Roslyakova. Samara: PSUTI, As Guard Publishing House, 2014. 342 p.
3. *Suresh S., Sruthi P.V.* A review on smart home technology // 2015 Online International Conference on Green Engineering and Technologies (IC-GET), Nov 2015, pp. 1-3.
4. *Lobaccaro G., Carlucci S., Lefstrem E.* A review of systems and technologies for smart homes and smart grids // Energies, 2016, vol. 9, no. 5, pp. 1-33.
5. *Saad al-sumaiti A., Ahmed M.H., Salama M.M.A.* Smart Home Activities: A Literature Review // Electr. Power Components Syst., 2014, vol. 42, no. 3-4, pp. 294-305.
6. IDC. Double-Digit Growth Expected in the Smart Home Market. https: //www.idc.com/getdoc.jsp?containerId=prUS44971219, March 2019.
7. Cisco Visual Networking Index: Forecast and Trends, 2017-2022, White Paper, 2019.
8. *Sivanathan A., Gharakheili H.H., Loi F., Radford A., Wijenayake C., Vishwanath A., Sivaraman V.* Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics .. IEEE Transactions on Mobile Computing '18.
9. *Ortiz J., Crawford C., Le F.* DeviceMien: network device behavior modeling for identifying unknown IoT devices // In ACM IoTDI '19.
10. *M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou.* Understanding the Mirai Botnet. In USENIX Security '17.
11. *Franceschi-Bicchierai L.* How 1.5 Million Connected Cameras hijacked to make an Unprecedented Botnet. https://motherboard.vice.com/en us/article/8q8dab/15-millionconnected- cameras-ddos-botnet-brian-krebs, 2016.
12. *Chu G., Apthorpe N., Feamster N.* Security and Privacy Analyses of Internet of Things Childrens Toys // IEEE Internet of Things '19.
13. *Wood D., Apthorpe N., Feamster N.* Cleartext Data Transmissions in Consumer IoT Medical Devices // In ACM Workshop on Internet of Things Security and Privacy (IoT S&P) '17.
14. Ren J., Dubois D.J., Choffnes D., Mandalari A.M., Kolcun R., Haddadi H. Information Exposure from Consumer IoT Devices // In ACM IMC' 19.
15. *Alrawi O., Lever C., Antonakakis M., Monrose F.* SoK: Security Evaluation of Home-Based IoT Deployments // In IEEE Symposium on Security and Privacy (S&P)'19.
16. Marikyan D., Papagiannidis S., Alamanos E. A systematic review of the smart home literature: A user perspective // Technol. Forecasting Social Change, vol. 138, pp. 139-154, Jan. 2019.
17. Pfeffer H. Dynamic changing tier service on test device. U.S. Patent 9 425 977, Aug. 23, 2016.
18. (2018). Internet Connection and Recommended Encoding Settings. Accessed: Dec. 16, 2018 [Online]. Available: https://support.video.ibm.com/hc/en-us/articles/207852117-Internet-connection-andrecommended- encoding-settings.
19. *Leister W., Floor P.A., Woldegiorgis Y.B., Balasingham I., and Abie H.* Dening the asset lab," Norsk Regnesentral, Norway, Tech. Rep., 2012. [Online]. Available: http://publications.nr.no/1362402875/DART-16-2012.pdf.