International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

# Security & Privacy Challenges in Smart Home

**Renu Sharma**

***Abstract*: Smart Home is changing the way of today's living. Technology is taking each and everything on internet, but when it is home than many considerations are there. Security and privacy is the major issue as far as life is considered. As per technical hazards issues could be, interoperability, integration, energy efficiency. These challenges are huge barriers in their applicability. Incredible work has been done to overcome the barriers. But still gaps are there. This paper is providing comprehensive information about available literature on above parameters and existing research gaps in the area. Findings of this paper can lead researchers to have research gaps in the security and privacy issues in smart home.***

***Keywords* : Block Chain, IoT, MQTT, RFID .**

## I. INTRODUCTION

Smart Home is a network comprising of many devices that can communicate with each other or with outer world through internet. This communication enable a person to watch and manage a home remotely. Internet of things or IoT means we are having devices linked through internet to exchange their information and to create results helpful for mankind. Next era of computing will not be based on desktops but will be of IoT devices.[1]. IoT is most significant electronic revolution after internet[2]. According to Gartner number of IoT enabled devices will be 26 billion by 2020. If we list area of applications of IoT list is keep on expanding to various diverse fields. Some area of applications are:

- Smart Homes
- Remote Health care monitoring
- Smart cities
- Education
- Smart Transport
- Smart Agriculture
- Business
- Energy
- Disaster detection etc….

Smart home concept is mainly to raise level of luxury. But it has given many added advantages other than luxury. Some of the benefits of Smart Homes are:

- Remote monitoring
- Assisted living for elderly. [3]
- Energy efficiency [4]
- Comfort etc.
-

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
**Renu Sharma*,** Department of Computer Science, DAV College, Amritsar, India.



## II. CHALLENGES IN DEVELOPMENTS OF SMART HOME

Although smart home market is quite positive, in user as well as market perspective but many technical as well as social hazards are there in the implementation.[5]. In development of smart home applications, many challenges are there. Some of them are:[6]

- Interoperability and integration[7]
- Security[7]
- Privacy [8]
- Data storage
- Constrained resources
- Data Analysis

### A. Interoperability and integration

Smart home idea is mostly based upon sensors. Sensors do have varied architectures. To integrate is major challenge. Smart home industry lacks in standardization or in other words so many standards are there. Every company is adopted different standards. While integrating these devices many technological issues got arise. So there is a requirement of one standard model for development of IoT devices. So addition of any new device will be simple. For example if we have employed a home automation system and we want to change an A.C. due to lack of unique standardization it might be possible there will be a need of updating our home automation system.

### B. Security

Security is the major challenge for smart home. A cyber security organization has conducted a survey and a large number of MQTT servers are found vulnerable to data leak, posing a serious threat to security[9]. As in BMW cars they found major possibility of intrusion using server of the company. IoT is based upon network and network is vulnerable to threats. As in home automation system main identity of user is RFID card. Copy of that card is possible. As in the recent case in USA alarm of missile attack falsely altered and it has created major havoc in the city. If a person is sing GPRS all its travelling pattern can be monitored and that can create major security issues. If we study health monitoring, intruder can create major blunders. So in all sensitive areas IoT is quite helpful but its implementation is really important to be focused on security.

### C. Privacy

Privacy is also major concern. Somebody can study all patterns of anyone just by analyzing data of sensors. And that information can be used for criminal activities. GPRS, wearable devices [10] and other sensors used for home can easily tell about daily routine of somebody.

So privacy is also one of the major issues in implementation of smart home. Two billion records have been claimed as smart home device breech[11]. This is a huge number, so there is huge scope to find solutions for privacy in smart home gadgets.

### D. Data Storage

In any smart environment huge data is produced. To process that huge data traditional data processing techniques cannot be used or we can say they are not capable enough to process that huge data. To overcome this challenge we need data processing techniques capable to work on high volume and high velocity data. Data mining tools are to be updated.

### E. Constrained Resources

In IoT devices main components are sensors. These sensors are really constrained as far as processing power, battery life and memory is concerned. To overcome these constraints are also a big challenge.

### F. Data Analysis

Using IoT sensors, huge amount of data will be generated. It is a huge challenge to process such a large amount of data. To conclude from such a huge data, efficient algorithms are required.

## III. LITERATURE REVIEW

H. A. Khattal et al. (2019) have proposed a solution at perception layer of IoT layered architecture[12]. Authors have described main components of IoT with focus of perception layer. They have concentrated on RFID and sensors network. Various possible attacks and their possible solutions have been given in the paper.

J. E. Klobas et al. (2019) have described how security concerns can effect smart home adoption[13]. Analysis is based upon age, education and gender of user. Perception of security changes with each category.

N. Panwar et al. (2019) have described many existing technologies that can be used to provide security in smart home also[14]. Existing solutions (distance bounding protocols, TLS, Okamotto Identification scheme etc.) can be used.

E. Zang et al. (2019) have developed a prototype app and tested that app for several months and on several users. From data collected challenges and possible solutions has been given[15]. In smart home security is even more challenging because environment comprises of multiple users and multiple devices of diverse architectures. Feedbacks of the designed apps have been studied.

A. Dorri et al. (2017) have discussed block chain technique for providing security and privacy in IoT environment[16]. They have attributed distributed nature of IoT network is major cause of security issue.

V. Sivraman et al. (2015) have suggested network level security for smart home[17]. To provide security main focus is on securing network, thereby smart home can be protected automatically.

W. M. Kang et al. (2017) have purposed a framework for smart homes[18]. It works on integrity by access control techniques. It can help to prevent data modification and fabrication.

B. A. Mozzaquatro et al. (2017) have given MDA based (model driven architecture) based solution for adaptive security for IoT environment [19]. Component model has been used and CIM (component independent model has been given. From CIM, PIM (Platform independent model) has been evolved. Than PSM (Platform specific model) and subsequently code has been generated.

## IV. FINDINGS

Wide range of solutions have been given in literature based upon diverse approaches varying from block chain, MDA based ( Model Driven Architecture), network layer based, prototype based, Distance bounding protocols, perception layer based security etc. but inspite of all these given solutions, no solution has yet developed that can work at each and every layer of architectural model. In Table I strengths and limitations of purposed solutions has been given. Research gaps can help researchers to find topics in this domain.

**Table- I: Findings**

| | Authors | Strength | Limitations | Research Gaps | References |
|---|---|---|---|---|---|
| Security and Privacy | H. A. Khattal et al. (2019) | Focused for perception layer | Based on just RFID and sensor networks | In the layered architecture, other layers can also be vulnerable to threats also. | [12] |
| | J. E. Klobas et al. (2019) | Survey on adoption of smart home based on security | Solution for challenge is not suggested | Implementable solutions are needed for security. | [13] |

| | | | | | |
|---|---|---|---|---|---|
| | N. Panwar et al. (2019) | Tried to integrate existing solutions for smart home | It is having diverse requirements, so different solution should be suggested | Due to diverse devices and many user involved, some techniques has to be found which can be implemented on smart home. | [14] |
| | E. Zang et al. (2019) | Actual prototype app has been tested | Feedback data can't be incorporated fully. | For security, growth could be incremental. | [15] |
| | A. Dorri et al. (2017) | Block chain has been used which is quite secure | All the goals of security has been not taken care of. | To provide security each and every aspect has to be considered | [16] |
| | W. M. Kang et al. (2017) | Framework primarily on integrity | Only data accessing is addressed, no security at network level | To provide a system which can provide security at each layer if the architecture. | [18] |
| | B.A.Mozzaquatro (2017) | Component based model has been purposed | This solution can be applied only on the app developed | Tools to convert one model into another in case of smart home are not available. | [19] |
| | W. M. Kang et al. (2015) | Based on access control | Security breeches could be at many levels | A framework which can cover more layers of smart home architectures. | [17] |

## V. CONCLUSION

Security and Privacy is main concern of a human as far a home is concerned. Many security features has been introduced, but still it is a major challenge. So we need a solution which can incorporate every threat possible at each layer of architecture. This paper can help in finding new ways for security.

## REFERENCES


1. G. Jayavardhana, R. Buyya, S. Marusic and M. Palaniswami.,"Internet of Things(IoT): a vision, architectural elements and future directions " , Journal of Future Generation Computer Systems, Vol. 29, Issue 2, September 2013, pp. 1645-1660,.
2. A.H. Ngu, .M. Gutierrez, V. Metsis, S. Nepal and Q. Z. Sheng ., " IoT Middleware: A Survey on Issues and Enabling Technologies", IEEE Internet of Things journal, vol 4, issue 1, February 2017, pp. 1-20,.
3. S. J. Daraby,"Smart technology in the home : time for more clarity", Building Research & Information, Vol. 46, Issue 1, March 2017, pp. 140-147.
4. S. T. Herrero, l. Nicholls and Y. Strengers," Smart home technologies in everday life :do they address key energy challenges in households?", Current Opinion in Environmental Sustainability, vol. 31, April 2018, pp. 65-70.
5. C. Wilson, T.Hargreaves and R. Hauxwell-Baldwin," Benefits and Risks of smart home technologies", Energy Policy, Vol. 103,pp. 72-83, April 2017.
6. D. Raggett, " The Web of Things: Challenges and Opportunities," IEEE Computer, vol. 48, Issue 5,pp. 26-32, May 2015.
7. M. Elkhodr, S. Shahrestani and H. Cheung., "The internet of things: new interoperability, management and security challenges", International Journal of Network Security & Its Applications, Vol. 8, No. 2, March 2016.
8. S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman and R. Boreli, "An experimental study of security and privacy risks with emerging house-hold appliances", In Proc. IEEE Conference on Communications and Network Security, 2014, pp. 79-84.
9. A. Spadafora, "Thousands of smart homes and business at risk of data breach",https://www.itproportal.com/news/thousands-of-smart-homes-and-businesses-at-risk-of-data-breach/
10. J. A. Martin,"10 things you need to know about the security risks of wearables", para. 4, March 24, 2017.[online]. Available: https://www.cio.com/article/3185946/wearable-technology/10-things-you-need-to-know-about-the-security-risks-of-wearables.html. [Accessed Feb. 12, 2018].
11. D. Winder, " Confirmed : 2 Billion Records Exposed in Massive Smart Home Device Breech", .[online]. Available: https://www.forbes.com/sites/daveywinder/2019/07/02/confirmed-2-billion-records-exposed-in-massive-smart-home-device-breach/#3225791a411c.
12. H. A. Khattak, "*Perception Layer Security in Internet of Things",* Future Generation Computer Systems, 2019, pp. 144-164.
13. J. E. Klobas, "How perceived security risk effects intention to use smart home devices: A reasoned action explanation", Computers and Security, 2019.
14. N. Panwar et al., "*Smart Home Survey on Security and Privacy*", arXiv:1904.05476v2, 2019.
15. E. Zeng et al, Understanding and Improving Security and Privacy in Multi-user smart Homes: A Design Exploration and In-home user Study, 28th USENIX Security Symposium, August 2019.
16. A. Dorri et al., " Blockchain for IoT Security and Privacy: The Case Study of Smart Home", IEEE International Conference on Pervasive Computing and communicating Workshops.
17. V. Sivaraman et al., " Network-level Security and Privacy control for Smart-Home IoT Devices", 2015 International Conference on Wireless and Mobile Computing, Networking and communications (WiMob).
18. W. M. Kang et al.," An enhanced Security Framework for home appliances in smart home", Human-Centric Computing and Information Sciences 2017.
19. B. A. Mozzaquatro et al.," A Model Driven Adaptive Approach for IoT Security", Model-Driven engineering and software development 2017, pp. 194-215.


## AUTHORS PROFILE

**Ms. Renu Sharma** pursed Masters in Computer Applications from Guru Nanak Dev University, Amritsar in 2001. She is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Sc. & IT, DAV College, Amritsar . She has published 10 research papers in reputed international journals and conferences. Her main research work focuses on Internet Of Things, Big Data Analytics, Data Mining and Computational Intelligence. She has 15 years of teaching experience.