Innovative Computing Review (ICR)

Volume 1 Issue 1, Summer 2021
ISSN(P): 2791-0024 ISSN(E): 2791-0032
Journal DOI: https://doi.org/10.32350/icr
Issue DOI: https://doi.org/10.32350/icr.0101
Homepage: https://journals.umt.edu.pk/index.php/icr

Article: **Security and Privacy Challenges for the IOT-based Smart Homes with Limited Resources and Adoption Immaturity**

Author(s): Farzana Kausar Gondal

Affiliation: Govt. Graduate College for Women, Islampura, Lahore, Pakistan

Article History:
Received: March 31, 2021
Revised: June 23, 2021
Accepted: June 30, 2021
Available Online: June 30, 2021

Citation: M. R. Gondal, “Security and privacy challenges for the IOT-based smart homes with limited resources and adoption immaturity”, *Innov Comput Rev*, vol. 1, no. 1, pp. 43–59, 2021. https://doi.org/10.32350/icr.0101.04

Journal QR

Article QR

Farzana Kausar

A publication of the

School of Systems and Technology

University of Management and Technology, Lahore, Pakistan

Security and Privacy Challenges for the IOT-based Smart Homes with Limited Resources and Adoption Immaturity

Farzana Kausar Gondal[1]

ABSTRACT: The Internet of Things (IoT) is technically a developing model looking at the connectivity of different devices or "things" to each other, as well as with the users and also with the Internet. IoT is projected to be an important necessity for the advancement of intelligent smart homes to facilitate homeowners because it provides opportuneness and effectiveness in order to help them attain an improved quality of life. The incorporation of IoT into smart homes entails integrating devices with the Internet. Even though it offers many advantages to the users, it also poses new security and privacy challenges based on connectivity, confidentiality, integrity, authenticity, resource limitation, and adoption immaturity. These challenges make the IoT-based smart homes with limited resources enormously susceptible to diverse forms of security vulnerabilities. Thus, it is pivotal to detect the probable security threats to establish a comprehensive and secure status of smart IOT-based homes. This paper incorporates the security risk assessment approach in order to evaluate the potential security and privacy risks and challenges faced by smart homes. The basic goal of this study is to identify and point up diverse security and privacy threats to smart homes and to unveil the risks for their residents. The paper also presents methods to mitigate the recognized dangers. This study provides a foundation to future applications aimed at refining the security necessities of the IoT-based smart homes.

INDEXED TERMS: Internet of Things (IoT), smart homes, risk assessments, security

I. INTRODUCTION

In most cases, the Internet of Things (IoT) is regarded as a problematic field with planned resolutions envisioned to be incorporated in diverse application choices [1]. Nevertheless, the confidentiality and safety requirements of critical engineering substructures and subtle viable processes are far different from the necessities of a preliminary

[1] Farzana Kausar Gondal is with Govt. Graduate College for Women, Islampura, Lahore, Pakistan.

Farzana Kausar Gondal the corresponding author available at the given Email ID:farzana.gondal@gmail.com

smart home setting. Moreover, the security implementation processes and infrastructure differ significantly among various domains of smart application like smart healthcare, smart home smart governance [2]. In the home-related settings, human problems are considered more critical than technical issues. Subsequent research on many prevailing resolutions for improving IoT safety is presented in this paper. It determines the extensive security and privacy challenges for the IoT-based smart homes with limited resources [3]. The primary purpose of the IoT is to increase the potential of the Internet by increasing the capability to connect with many devices simultaneously [4]. By incorporating the IoT model, the users obtain a platform to share equally the data provided by user behaviors and the data gathered by the linked devices in the physical space.

There are diverse definitions of a smart home from a technical perspective but the primary idea is to link sensors, home applications and smart devices through the Internet to attain the remote monitoring, access, and control of a residential setting [5]. Therefore, the smart home setting targets the rich integration of minor computational schemes to find and distribute personalized amenities to the operators. It emphasizes the computerization and regulation of the environment to attain a secure and private setting [3]. Thus, all the other components of computing, security and privacy are the main challenges for the designing of smart homes. Contrary to the enterprises which dedicate specific professional resources to systems security, IoT with limited resources gives smart homes a relatively ad hoc system with no dedicated system management resources, making it more vulnerable to privacy and security threats [6]. This also contributes to the challenge of the immature adoption of smart systems [7]. There is no awareness and adoption of these systems due to the lack of knowledge and training to use them, hence the security and privacy of the systems are compromised and not fully implemented.

II. IoT AND SMART HOMES

A smart home-based setting can be regarded as a limited physical space with various sensors, computational software, electronic appliances, and a display screen that aids the exchange of information and interaction between the residents [8]. An overview is presented in Figure 1.

In many instances, IoT technology is expected to be implemented to the already existing homes, portion by portion, depending on the emergent security needs. Mostly, there is a lack of progressively specialized sustenance in the project or process stages of IoT placement in a smart home [9].

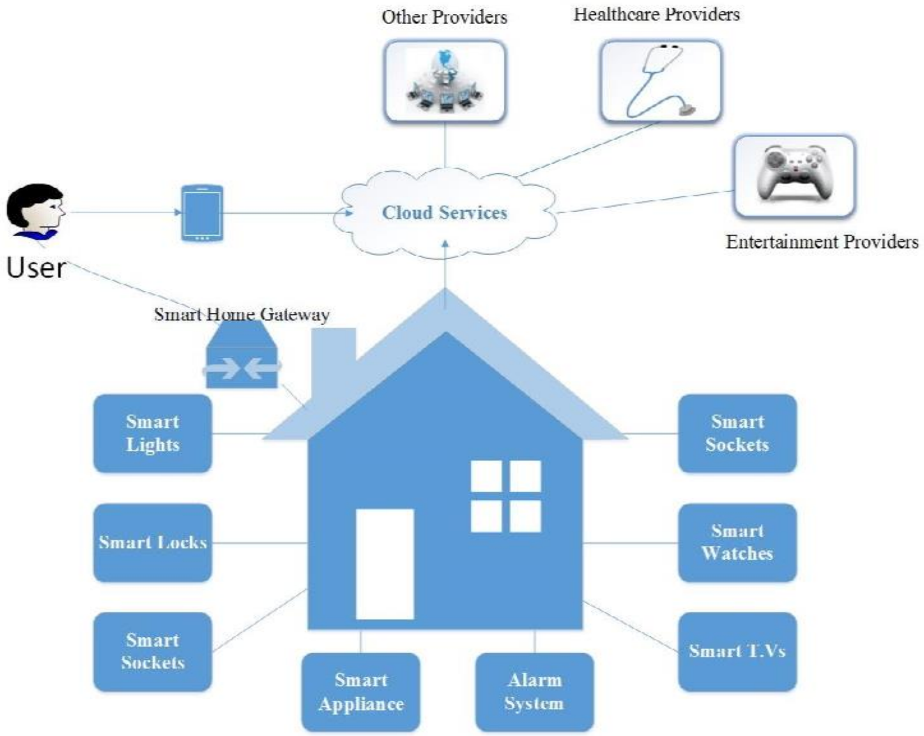


Fig. 1. IoT- based smart home [14]

Although there are diverse smart home designs, the lack of particular security approaches before home control networks are interconnected poses great privacy and security issues to smart homes. Currently, there are many networking standards that can be incorporated into smart homes such as Bluetooth, Wi-Fi, and Z-Wave [1]. Each one of these has its advantages and disadvantages. Moreover, imagining such an assorted network environment with diverse procedures to be competently secured and manageable presents many detrimental challenges [10]. The smart home offers additional comfort and setting. Still, neither of the advantages is probable to be booked up if these home systems are not safe and trusted. In order to identify the privacy and security challenges, this study conducts the security evaluation approach of the IoT-based smart homes taking into consideration limited resources and immature adoption by the users.

III. Security and Privacy Threats in the IoT-based Smart Home

A. IoT Architecture for Smart Homes

IoT deployment in smart homes entails the incorporation of different

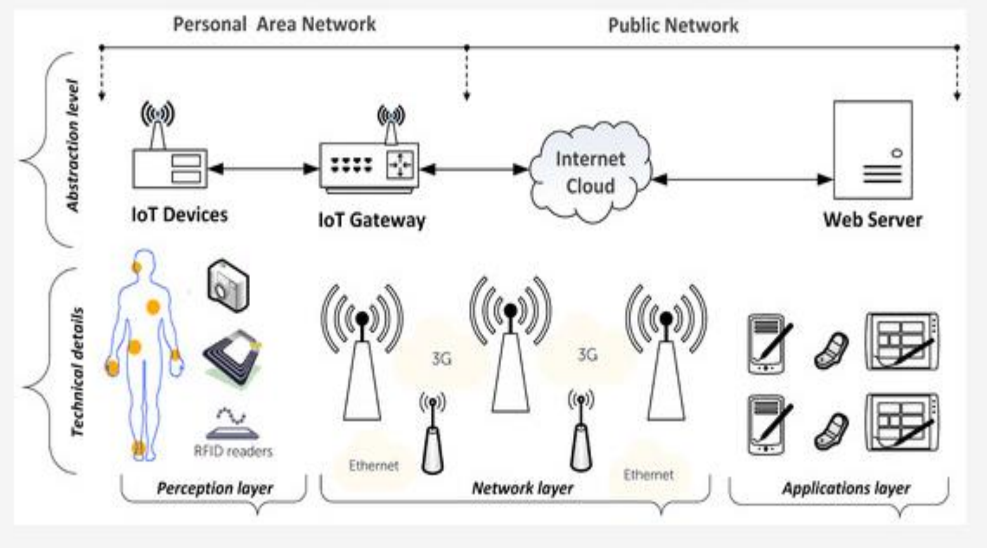


Fig. 2. Smart home based IoT architecture [3]

technologies such as Wireless Sensor Networks (WSNs), Internet Protocol (IP), Wireless Fidelity (Wi-Fi), RFID, Bluetooth, and different sensors [11]. The main goal of the IoT protocol is to help the users to distinctively identify, control and access other things at their convenience through the Internet [12]. The interrelated device network can yield diverse intelligence and independent applications that offer many advantages. Technically, a home authentication system is made up of five components or units. These include appliances under regulation, sensing devices and actuators, the regulator, the control network, and the remote-control devices [13]. A comprehensive image of the IoT devices, service providers, diverse layers of IoT and their probable safety matters are illustrated in Figure 2.

Even though IoT-based smart homes are completely different in their configurations, the entire outlook of security issues is similarly relatable to the existing network connections.

B. Threats to Smart Homes

Although there are many threats to smart systems but the more critical and vulnerable ones encountered by smart homes are confidentiality, authentication, and unauthorized access.

1) Confidentiality Threats. These are the threats that arise due to the breaching of the confidentiality of data or unauthorized access of data. For instance, privacy breaches in home-based monitoring structures can result in the unintentional issue of the leakage of subtle banking information [14]. Even information that is seemingly harmless such as the temperature of internal home setting and the information of air conditioning system might be analyzed to determine if the house is currently occupied or not [15]. This acts as a basis for break-ins. Moreover, the loss of privacy regarding passwords and pin codes results in unauthorized access to the system.

2) Authentication Threats. Verification threats can result in the identification and monitoring of data by unauthorized personnel, causing interference [1]. For instance, unauthenticated environment or user's status signals may confuse the supervisor of the house into assuming that there is an emergency condition. They then rush to open doors and windows for the exit but, in the real sense, allow unauthorized entry into the house. Also, if software updates are not properly authenticated, then systems might as well be altered [1].

3) Access Threats. Access threats are the primary threats facing the IoT-based smart homes. Unauthorized access to system controls, specifically administrative positions, makes the overall structure insecure [16]. This can be attained over unauthorized access via PIN key codes or through the use of illegitimate devices linked to the system. Even though maximum regulation of the system can be attained, still having an unofficial link to the system may lead to the stealing of network bandwidth and the denial of service (DOS) to genuine network operators [17]. Subsequently, most smart home appliances are wireless networked and battery operated with little operative duty sequence, thus the flooding of the network with many requirements can result in an energy exhaustion outbreak leading to a denial of services (DOS).

C. Privacy in Smart Homes

Privacy refers to a state of not being observed and disturbed by others. Privacy emphasizes protecting people's identity, location, information, and movement. [18]. Smart homes' sensitive information includes aspects such as digital information, photos, and videos. Smart devices with dynamic IP cameras can capture pictures and videos wherever. Feature microphones have the ability to snoop on personal discussions. There are mainly two privacy threats facing smart homes.

Data Privacy Threats: Information confidentiality is a significant concern when it comes to the exchange of confidential data [19]. This is because everything is or will be connected to the existing internet, thus penetrating into the network and access to network tariff remains less challenging for cyber terrorists. By merely getting access to a part of the system, a hacker may obtain the general information about the homeowner [3].

Context-aware Privacy: Context cognizance entails noticing, sensing, and tracing operators' movements and actions, as well as actions by the means of data to offer amenities that might be of importance to them [17]. Context cognizance has the capability of sensing and responding when things change, for example, if devices are moved to a new location.

IV. Security Challenges in the IoT-based Smart Homes

Security refers to a state of being which is free from distress [15]. Security deals with aspects of messaging, confidentiality, integrity, and authenticity. IoT strategies are used to gather and process an enormous quantity of individual information that is very delicate. Having IoT devices with limited resources poses greater risks to smart homes. Home security in smart homes relies on biometric identification recognition systems. These include aspects such as fingerprinting, face recognition, voice recognition, smart cards, and RFIDs that allow access and control [3]. IoT devices connected in smart households with limited resources do not have the required computational control and also have an inadequate storage capacity. Figure 3 shows household devices that require computational control. Thus, implementing intensive security solutions is a challenging approach.

In order to provide a protected connection among IoT devices and the gateway to the smart home-based setting a dispersed encryption approach is used, for instance, triangle-based security algorithms. IoT-based smart households are extremely vulnerable to intrusions [3].

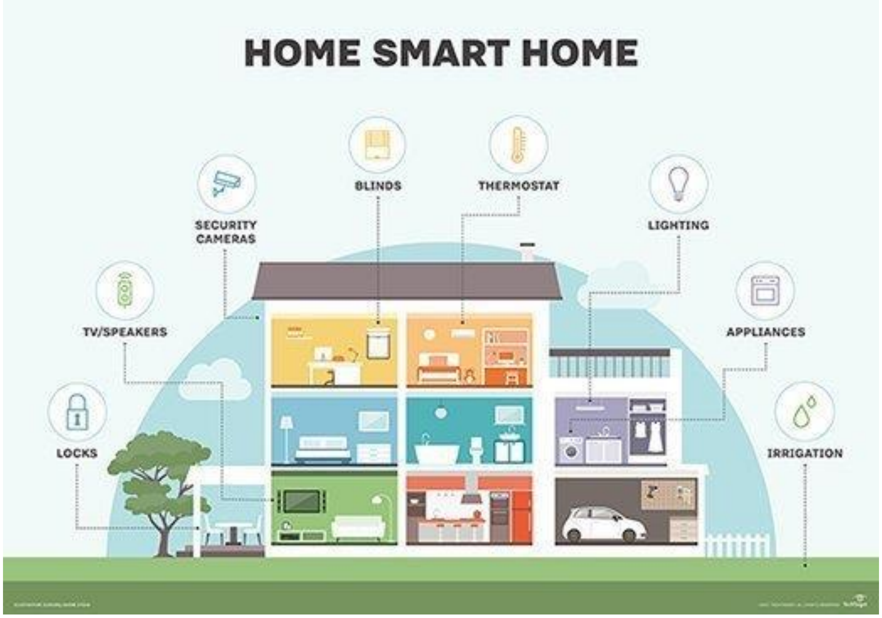


Fig. 3. Smart Home Devices [13]

They face the following security and privacy challenges.

A. Lack of Technical Support

The absence of technical support is the main problem with the housed environment of smart homes. Households are loaded with monotonous, tedious, and fault-related physical equipment required to manage smart devices in the home network, mainly due to little power and little computationally controlled structure strategies. This can pose a major security issue [20]. Thus, for the fruitful execution of smart homes, the protected auto-configuration method is used to make the connection and care of smart home appliances easier and to enhance security.

B. Openness of the Networked Systems

The openness of the networked system is among the major weaknesses of the IoT-based smart households [3]. Smart home strategies are linked to cyberspace. Figure 4 highlights the points of weakness of systems corresponding to the layers of IoT. This provides a greater chance for attackers to remotely access the networks and control their interface, either directly or indirectly. They can also upload malware to the devices, thus interrupting the entire system.

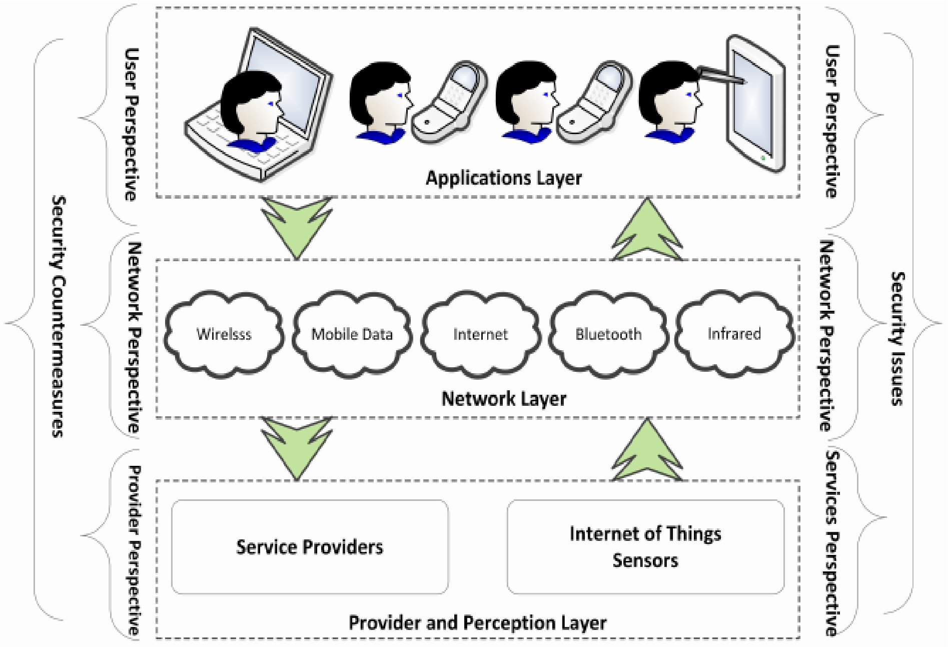


Fig. 4. An IoT scheme from the provider, system, and operator viewpoints. The image pinpoints the weaknesses in the IoT layers [3]

C. Physical Accessibility to the System

Physical accessibility to the system is another paramount safety and confidentiality issue of the IoT-based smart households [21]. The diversification of IoT devices is also a most significant and serious challenge that needs to be fixed on an urgent basis. Figure 5 illustrates the diversification of IoT devices in the IoT-based smart homes. A device comes with heterogeneous networking protocols and various supporting software as well as different features due to diverse manufacturers [3].

D. Data at Risk in the Cloud

Information kept in the cloud can be lost for many causes apart from malevolent attacks. Figure 6 shows the cloud-based architecture of a smart home. For instance, the unintentional removal of information by cloud service providers and unprecedented events such as fire outbreaks can result in the permanent loss of data [5].

E. Weak Passwords

The use of weak passwords is among the biggest issues with the IoT-based smart homes. The users of the network systems need to take care of their passwords and should use authenticated passwords that they can easily remember [14]. Weak password selection also shows immaturity towards system use.

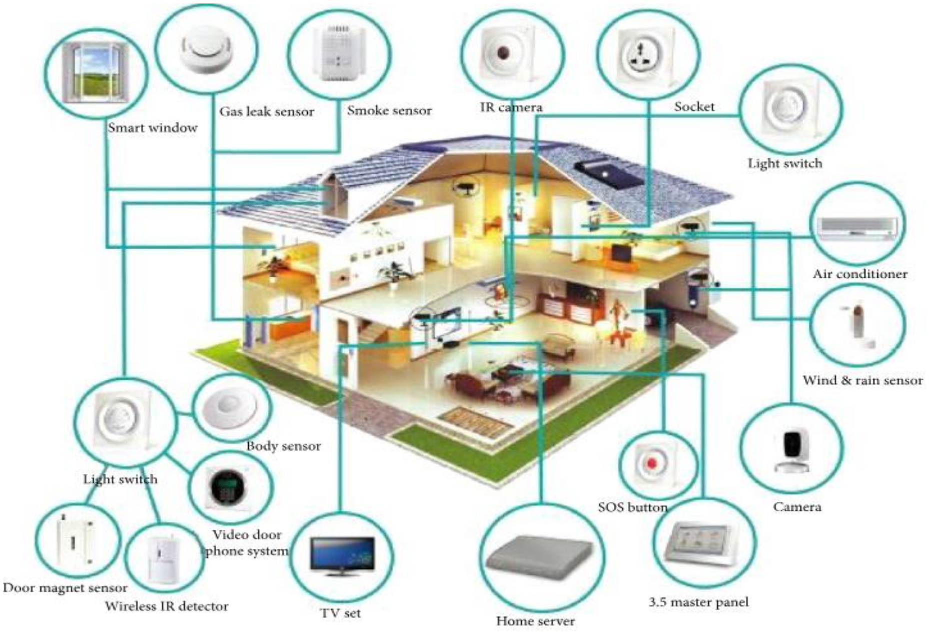


Fig. 5. Diversification of the IoT Devices [9]

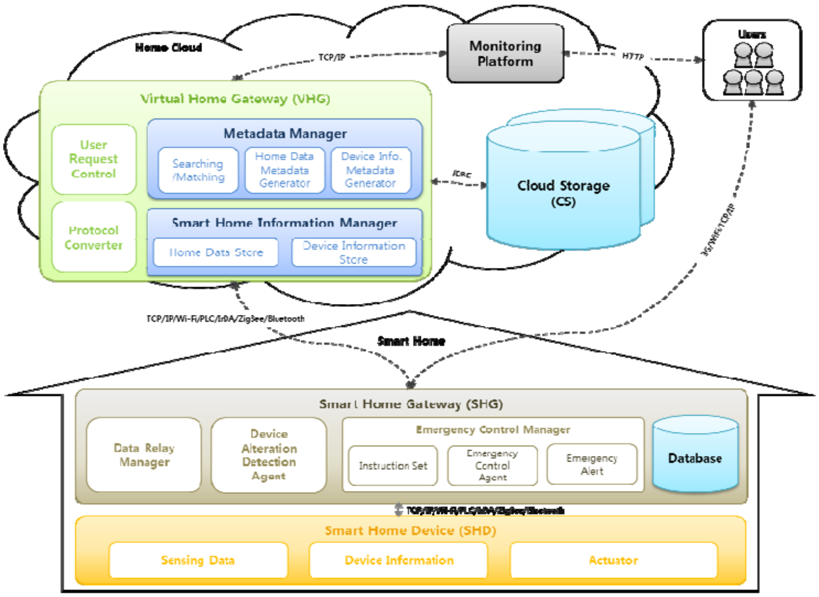


Fig. 6. Cloud-based Architecture of a Smart Home [29]

F. Fixed Firmware

In most instances, to mitigate security vulnerabilities, reprogramming and software updates are needed. Computerized functioning systems are habitually automatically updated when safety susceptibilities are recognized [1]. Likewise, there are regular software updates sent to mobile devices such as smartphones, which lower security vulnerabilities as much as possible. However, smart homes have a fixed firmware that mostly does not support these dynamic patches. Firmware is a kind of software that is automated into the non-volatile memory of a smart device and remains an indispensable part of the IoT systems [22]. It unswervingly connects with the hardware and thus operates the system's processes and functions by initializing the device interface [23]. It implies that a smart device's firmware should be kept updated to help solve security susceptibilities and to advance its operationality. The smart home setting typically lacks technical assistance making this process challenging. There are limited smart home devices that offer steady software update services to resolve the existing security issues. Currently, there is little motivation to patch the software frequently and to stay ahead of security breaches in smart home appliances with low cost. Attackers can easily block new software and disguise the legitimate old firmware with security vulnerabilities [1].

G. Unsecured Network Connectivity

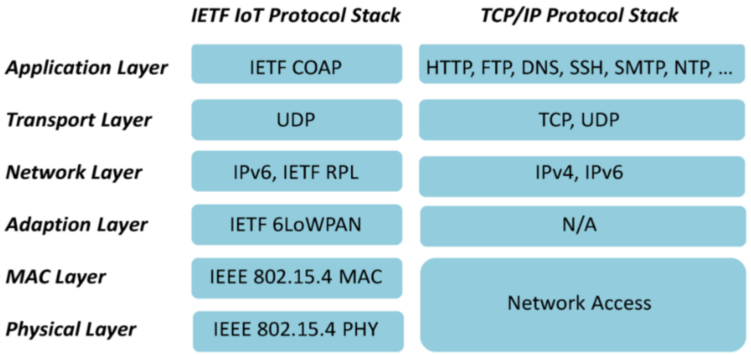
Although some branded schemes such as smart health where 24-hour care systems have well-formulated standards of compliant securities, most of the current smart homes do not have devices with well-implemented security systems [24]. As stipulated earlier, most smart homes rely on the Internet. However, many times their networks are not secure. This is because of the smart home devices. Smart homes are not built from scratch but they are based on the existing homes [4]. Thus, an individual cannot take steps to configure their wireless networks with the specifications of their security in place. Security steps are largely ignored during the installation of wireless networks which leaves the networks more open to anyone within the network connectivity range [25]. This makes it easy for cyber terrorists to access the network and spy on the information traffic. The leading cause of this type of security vulnerability is the lack of dedicated security personnel. Such personnel are expected to manage network complexities in smart homes and make them less vulnerable. Few households can afford these professionals to foster the existing need of network administration aid. As an alternative, unprofessional householders are assumed to have the abilities to manage their systems simply, securely, and strongly [15].

H. Immature Adoption of Smart Systems

Given the idea that the IoT market and smart homes are relatively young and immature, it is challenging to create indistinct workflows [23]. Most smart system users do not have an adequate experience of executing IoT technologies, which can be difficult given the inconsistency of information that is mostly extricated from sources in smart homes ranging from an array of sensors. There is no appropriate awareness and adoption of the smart systems [7]. This is the result of the lack of knowledge and adequate training about the use of these systems. There is a deficiency of dependable means to create the emerging smart technology readiness, capabilities and to avail their benefits. There is also an increased lack of systematic knowledge transfer from different frameworks towards the industry. In most cases, progressively technologies from their earliest stages are always difficult to adopt. Respondents lack adequate funding instruments required for early technological development. The challenge of quantifying the benefits and costs of these technologies makes it harder to make supportive decisions for their implementation [26].

V. Existing Security Support for IoT

As a result of their low cost, IoT devices are usually not very powerful. Most of these devices use less energy, have limited memories, and use a low-end microcontroller [27]. Such controllers have the specifications of standalone controllers like those in air



	IETF IoT Protocol Stack	*TCP/IP Protocol Stack*
Application Layer	IETF COAP	HTTP, FTP, DNS, SSH, SMTP, NTP, …
Transport Layer	UDP	TCP, UDP
Network Layer	IPv6, IETF RPL	IPv4, IPv6
Adaption Layer	IETF 6LoWPAN	N/A
MAC Layer	IEEE 802.15.4 MAC	Network Access
Physical Layer	IEEE 802.15.4 PHY	

Fig. 7. Current security standards for the existing IoT security protocols [1]

conditioners. These aspects have made it more challenging to integrate changes as a result of already designed IPs. Several internet services task force have been formulated to counter these issues. Their efforts regarding IoT standards have played a significant part in the formulation of the required lightweight communication protocols for the controlled environment via the existing IP network [28]-[30]. Even with these specifications put in place, there still exist the above discussed security and privacy challenges in smart homes. Numerous Internet Engineering Task Forces (IETFs) and working assemblies have been formulated to solve these issues as depicted in Figure 7 [1]. IETF adjustment work regarding IoT has played a dynamic role in the formation of the much needed lightweight communication protocols for controlled surroundings over the existing IP network [1]. Figure 7 shows the current security standards for the existing IoT security procedures.

VI. COUNTERMEASURES FOR THE SECURITY AND PRIVACY CHALLENGES FACING THE IOT-BASED SMART HOMES

Smart homes can be made safer and more private in many ways. In Figure 8, some security vulnerabilities and prevention methods of an actual smart home setting are highlighted.

- Security awareness and training, that is, providing awareness and training programs about possible security vulnerabilities and challenges will ensure system configuration and appropriate performance by authentic personnel.
- Data encryption and authentication
- Encryption and monitoring of network traffic
- Monitoring systems' performance
- Replacement of default configuration
- Secure physical locations

- Set-up to secure Wi-Fi networks: Homeowners should avoid using insecure network connectivity such as Wi-Fi that could give hackers access to private information in a smart home environment.
- Homeowners should restrict physical access of the devices to unauthorized individuals.
- The use of intrusion detection systems can be helpful in monitoring and reporting possible attacks.
- Also, the use of strong encryption mechanisms should be encouraged to aid in securing traffic transmissions.

These are just a few measures

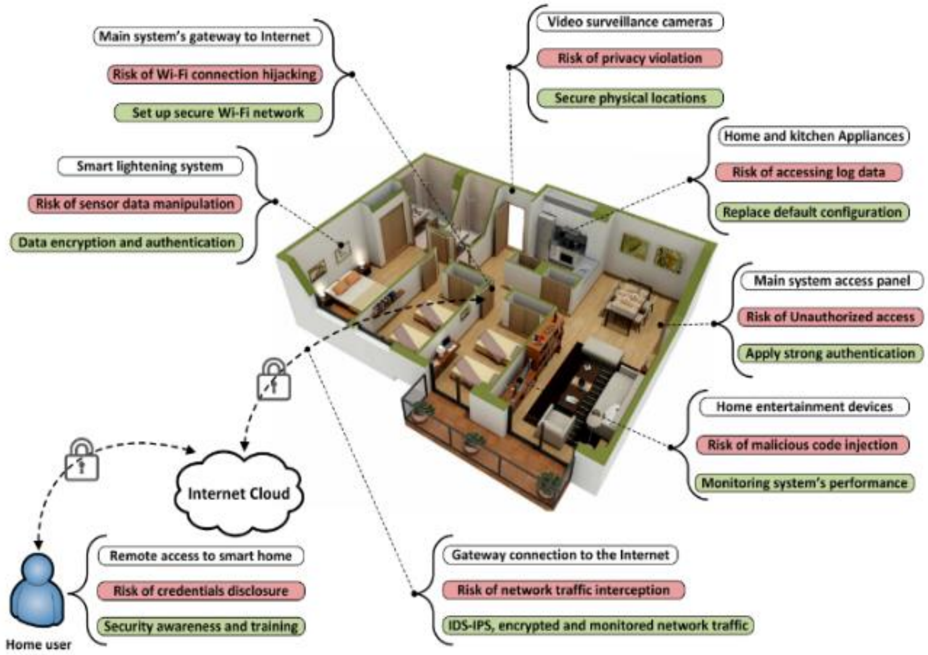

Main system's gateway to Internet
Risk of Wi-Fi connection hijacking
Set up secure Wi-Fi network
Video surveillance cameras
Risk of privacy violation
Secure physical locations
Home and kitchen Appliances
Risk of accessing log data
Replace default configuration
Smart lightening system
Risk of sensor data manipulation
Data encryption and authentication
Main system access panel
Risk of Unauthorized access
Apply strong authentication
Home entertainment devices
Risk of malicious code injection
Monitoring system's performance
Internet Cloud
Remote access to smart home
Risk of credentials disclosure
Security awareness and training
Home user
Gateway connection to the Internet
Risk of network traffic interception
IDS-IPS, encrypted and monitored network traffic

Fig. 8. Security vulnerabilities and prevention methods of an actual smart home environment are highlighted [3]

VII. CONCLUSION

Incorporating the IoT technology in smart homes yields multifaceted outcomes. These include both opportunities and security threats. From the discussion above, it is evident that the IoT-based smart households are extremely susceptible to diverse safety pressures emanating from both external and internal home environment. This is due to limited resourced devices and adoption immaturity linked with the lack of knowledge about the technicality of the system. If a device is compromised, then its user's privacy, confidentiality, and security is in great danger. Thus, suitable measures are needed to be put in place to make the smart home security implementation process a security bounded process. It will guarantee that all the pertinent fundamental security risks are discovered beforehand.

References

[1] H. Lin and N. W. J. I. Bergmann, "IoT privacy and security challenges for smart home environments," vol. 7, no. 3, p. 44, 2016. https://doi.org/10.3390/info7030044

[2] M. Park, H. Oh, and K. J. S. Lee, "Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective," *Sensors*, vol. 19, no. 9, p. 2148, 2019. https://doi.org/10.3390/s19092148

[3] B. Ali and A. I. J. s. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors*, vol. 18, no. 3, p. 817, 2018. https://doi.org/10.3390/s18030817

[4] A. Jacobsson, M. Boldt, and B. J. F. G. C. S. Carlsson, "A risk analysis of a smart home automation system," *Future Generation Computer Systems*, vol. 56, pp. 719-733, 2016. https://doi.org/10.1016/j.future.2015.09.003

[5] S. J. Darby, "Smart technology in the home: time for more clarity," *Building Research & Information*, vol. 46, no. 1, pp. 140-147, 2018. https://doi.org/10.1080/09613218.2017.1301707

[6] Y. Liu, S. Hu, and T.-Y. Ho, "Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks," in *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2014, pp. 183-190: IEEE.

[7] J. M. D. Delgado *et al.*, "Robotics and automated systems in construction: Understanding industry-specific challenges for adoption," *Journal of Building Engineering*, vol. 26, pp. 100868, 2019. https://doi.org/10.1016/j.jobe.2019.100868

[8] L. Satpathy, L, *Smart housing: technology to aid aging in place-new opportunities and challenges* [Doctoral dissertation]. Department of Architecture, 2006.

[9] H. Yang, W. Lee, and H. J. J. o. S. Lee, "IoT smart home adoption: the importance of proper level automation," *Journal of Sensors*, vol. 2018, pp. 1-10, 2018.

https://doi.org/10.1155/2018/6464036

[10] S. Wadhwani, U. Singh, P. Singh, S. J. I. R. J. o. E. Dwivedi, and Technology, "Smart home automation and security system using Arduino and IOT," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 2, pp. 1357-1359, 2018.

[11] L. Chhaya, P. Sharma, G. Bhagwatikar, and A. J. E. Kumar, "Wireless sensor network based smart grid communications: Cyber-attacks, intrusion detection system and topology control," *Electronics*, vol. 6, no. 1, pp. 1-5, 2017.

[12] W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Computer Networks*, vol. 148, pp. 283-294, 2019. https://doi.org/10.1016/j.comnet.2018.11.025

[13] B. Mahajan, (2021, March 15), *Civiconcepts*, Home automation system and technologies. https://civiconcepts.com/blog/home-automation-system-and-technologies

[14] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2017, pp. 1292-1297: IEEE.

[15] W. Ali, G. Dustgeer, M. Awais, and M. A. Shah, "IoT based smart home: Security challenges, security requirements and solutions," in *2017 23rd International Conference on Automation and Computing (ICAC)*, 2017, pp. 1-6: IEEE. https://doi.org/10.10.23919/IConAC.2017.8082057

[16] R. Heartfield *et al.*, "A taxonomy of cyber-physical threats and impact in the smart home," vol. 78, pp. 398-428, 2018. https://doi.org/10.1016/j.cose.2018.07.011

[17] P. Anand, Y. Singh, A. Selwal, P. K. Singh, R. A. Felseghi, and M. S. J. E. Raboaca, "IoVT: internet of vulnerable things? Threat architecture, attack surfaces, and vulnerabilities in internet of things and its applications towards smart Grids," vol. 13, no. 18, p. 4813, 2020. https://doi.org/10.3390/en13184813

[18] H. Zadran, *Amazing Architecture*, 2017. http://amazingarchitecture.net/2017/05/19/elegant-home-plan-design-ideas/(accessed on 6 March 2018)

[19] D. Mocrii, Y. Chen, and P. J. I. o. T. Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and security," *Internet of Things*, vol. 1, pp. 81-98, 2018. https://doi.org/10.1016/j.iot.2018.08.009

[20] Y. Yang, L. Wu, G. Yin, L. Li, and H. J. I. I. o. T. J. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250-1258, 2017. https://doi.org/1010.1109/JIOT.2017.2694844

[21] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. J. F. G. C. S. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Generation Computer Systems*, vol. 78, pp. 1040-1051, 2018. https://doi.org/10.1016/j.future.2016.11.011

[22] J. M. Castelo Gómez, J. Roldán Gómez, J. Carrillo Mondéjar, and J. L. J. E. Martínez Martínez, "Non-Volatile Memory Forensic Analysis in Windows 10 IoT Core," vol. 21, no. 12, pp. 1141, 2019. https://doi.org/10.3390/e21121141

[23] S. Falas, C. Konstantinou, and M. K. J. a. p. a. Michael, "A Modular End-to-End Framework for Secure Firmware Updates on Embedded Systems," *arXiv preprint arXiv: 2007.09071*, 2020.

[24] S. Chege, G. Wanyembi, and C. Nyamboga, "IT and Business Strategies in the Kenyan Leading Organizations," *International Journal of Scientific and Technical Research in Engineering*, vol. 41, no. 1, 2019.

[25] R. Budhrani, R. J. I. J. O. A. N. Sridaran, and Applications, "Wireless Local Area Networks: Threats and Their Discovery Using WLANs Scanning Tools," *International Journal Of Advanced Networking & Applications*, pp. 137-150, 2015.

[26] S. Manandhar, K. Moran, K. Kafle, R. Tang, D. Poshyvanyk, and A. Nadkarni, "Towards a natural perspective of smart homes for practical security and safety analyses," in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 482-499: IEEE.

[27] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, and S. R. Chaudhry, "IoT architecture challenges and issues: Lack of standardization," in *2016 Future technologies conference (FTC)*, 2016, pp. 731-738: IEEE.

[28] N. Komninos, E. Philippou, A. J. I. C. S. Pitsillides, and Tutorials, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *EEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933-1954, 2014. https://doi.org/1010.1109/COMST.2014.2320093

[29] G.-W. Lee, S.-H. Na, K.-H. Kim, and E.-N. Huh, "Cloud-based smart home system (CbSH) architecture design for virtual home gateway and cloud interworking," in *International Conference on Convergence Technology*, 2013, vol. 2, no. 1, pp. 1572-1573: 한국융합학회.

[30] C. Paul, A. Ganesh, and C. Sunitha, "An overview of IoT based smart homes," in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, 2018, pp. 43-46: IEEE. https://doi.org/1010.1109/ICISC.2018.8398858