A Holistic Framework To Protect Privacy &Security In Iot Based Smart Home

Supriya Nagarkar*1
Research Scholar, Department of Computer Science, Tilak Maharashtra Vidyapeeth,
Vidyapeeth Bhavan, Gultekadi,
Pune 411 037, Maharashtra, India

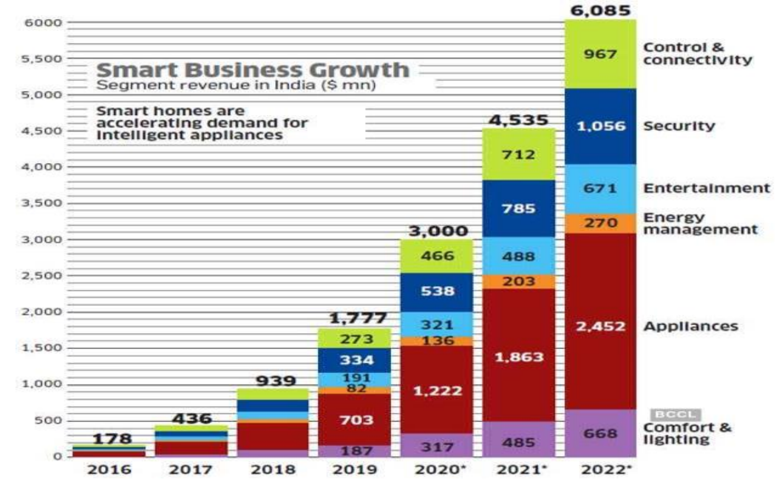
Dr.Vikas Prasad*2
Associate Professor, School of General Management, National Institute for Construction
Management & Research, Balewadi,
Pune 411 045, Maharashtra, India.

Abstract

Since ever Emergence of the Internet, the emergence of Smart Home Automation has spread and made Home users lives convenient, comfortable and secure. With the progression of digital technology new smart devices, smart TVs, Smart refrigerators,Security cameras and Smart air conditioners including tablet PCs, have expanded their Domains from individuals to business and houses.Smart home services as a human-entered services have gained much attention.It is the environment wherein householdGadgets and smart devices are connected to the internet in order to provide control to user services. The latest smart home system focuses simply on wireless home network to execute the connected home properties.The connected Smart home faces several types of safety and privacy threats and Threats.As a result, Home users may suffer a monetary loss from information spill or hacking of home appliances. Therefore, the protection of smart devices should be taken into account in implementing smart home service to the environments. This paper, tries to propose aholistic securityand privacy protectiveframework in a smart home environment. The framework is divided into components like Key objectives, Users, Physical infrastructure, Supporting mechanism, and finally guidelines. We assume that the comprehensive Framework designed in this paper can be served as a foundation for potential designers of smart home solutions based on the IoT.

Keywords *– Authentication, Authorisation, CIA triplet, Confidentiality, HomeGadgets, Internet-of-things (IoT), Information Privacy,Smart home Automation*

Introduction - Smart home systems have taken a big step over the past 20 years, enabling Home users to manage and track their appliances even while they are away from home. Smart home technology enables the use of computers to automatically or remotely monitor the basic functions and features of a home. Smart homes began to become affordable choices for many buyers, and thus viable innovations. Home networking, domestic and numerous other user gadgets have offered. As a result many builders now introducing smart home technology.



ISSN: 2233-7857 IJFGCN

Source - https://economictimes.indiatimes.com/tech/software/home-smart-home-the-indias-booming-home -Automationmarket/articleshow/74630996.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

India has also started taking lead in using the smart home technology. Seeing the consumer demand companies are also responding to meet the requirement of market. Recent smart home devices include voice interaction microphones and cloud use for storage or processing purposes.Bestowing to market research firm IDC, in 2018 near about 753,000 Smart Speakers were delivered to the Indian marketplace. This is projected to knockout around 1 million in near future.

Security goals & Objectives – Security goals seeks to prevent information from being stolen, or hacked. So to make data to be secure, all of the security approaches must come into effect. There are security policies that all function together, so it might be unfair to neglect any of one policy.The CIA Triad (Confidentiality, Integrity, and Availability) is considered as the foundation of all security programmes. [1][5][9]

Security Goals	**Descriptions**
Confidentiality	The main purpose of 'Confidentiality' is to ensure the safety of data by avoiding unauthorised expose of information
Integrity	Integrity in the field of information security means ensuring the authenticity and completeness of the data. It is about preventing data from being changed or misused by an unauthorised party
Availability	Availability applies to approve users who are free to access the systems, networks and data required to perform their daily tasks. Hardware and software along with routine maintenance, is essential to keeping the systems up and running
Access control	Access Control defines rules and regulations to restrict access to a device or to physical or virtual resources. It is a mechanism in which users are given access rights to system, services or information. In access control systems, users must need to provide credentials before access is been given, such as the name of the person or the serial number of the device.
Non-repudiation	Istechnique by which the IoT device will verify / Validate the incident or a non-incident case
Accountability	IoT system keeps users accountable by sending different alerts for their operations
Ease of Use	Is an important factor for adoption? Ensures Effective, Efficient, Engaging, Error Tolerant, and Easy to Learn
Trustworthiness	Ensure the capacity of the Smart home system to prove identity andConfirm confidence in third parties

Table 1 Security Goals

Security& Privacy Concerns - Smart home offers many more efficient and effective services that are integrated and intelligent for all home appliances.The security expert and researchers have quoted couples of issues related to privacy and security of Data. There have been a lot of vulnerabilities in modern automotive systems. [1].

Security issues– Handle security issues is not easy task in IoT-based Smart homes. Weakly protected Gadgets gives hackers the opportunities to exposed users private data. Authentication is one of the major problem. IoT faces a variety of vulnerabilities, which remain one of the most important security concerns in many applications.Being closely integrated with human beings and their

surroundings, IoT can be misused and a single vulnerability can result in adverse consequences, such as physical harm, financial losses, violations of privacy and organised crime.
Security threats can be classified into 5 categories Namely Hardware associated, Software correlated, information related, communication related and Human related [5].

Threats Categories	Probable threats	Security objectives compromised
Hardware related threats	• Device Theft / Removal of devices • Tampering the devices (damages, interrupts, destroys, or causes a permanent or temporary)	Availability Integrity Access control
Software related threats	• Inadequate authentication • Illegal access control • Inadequate accountability	Availability, Unauthorised access Accountability
Information related threats	• Insufficient authentication and access control • Absence of access control policies • Information leakage and manipulations	Availability, Unauthorised access Accountability
Communication related threats	• Eavesdropping • Replay attack • Message manipulation • Leakage of information	Confidentiality Integrity
Human related threats	• Careless end-users • Week password selection • Poor system configuration	Integrity Confidentiality

Table 2 Security issues of Smart home

Privacy issues–Most of the IoT devices don't have built in privacy control mechanism. Many times due to advertisement users leave them unattended and kept wide open to unauthorised assess. As many third party vendors are involved in the IoT based smart system. Users lost the control on data sharing on Network. Many times the devices are working/opened all the times attackers can easily peeped into it and misuse the data collected by devices. Privacy policies specified by device vendors are vague in nature most of the times.
Related Work–There are different research and activities which have been carried out on the latest trends in Protection of Smart home Environment**.**

Lo'aiTawalbehet. al.(2020)in the study entitled **"**IoT Privacy and Security: Challenges and Solutions**"**[1]has recommendedfresh IoT layered prototypes, which is all-inclusive in nature and which is extended with the privacy and security components and identification of layers. The prototype has used the Amazon web service (AWS) and cloud assistedenvironment andRaspberry pi 4 kit. Author have executed security certificates that allow data transmission between the layers of the projected IoT model indorsed by the cloud that ensure the privacy of user's information.

MiJeongKim et.al.(2020) in the study entitled "Developing the design solution for Smart home through user-centeredscenarios" [2] has proposed a framework for smart home services in a standardised way. Author has considered space, technology, and users. These three aspects and tried to integrate cross-cutting relationships built on conceptions of smart homes and users. This intelligent framework delivers solution to Basic everyday life support (Housekeeping assistance, and purchase preferences), Health care and management (health counselling and exercise guidance), Environment (safety & security), Psychological well-being (internet Education and entertainment), Social relation enhancement (social connection)

Verena Zimmermann et.al. (2019) in the study entitled “Assessing Users’ Privacy and Security Concerns of Smart Home Technologies” [3] has discussed the different privacy & security issues in adapting smart home technology. To understand the users concerns about potential threats author have conducted semi-structured interviews. After in-depth analysis study found that there may be psychological pressure to the user related to the attacks, security of data, loss on control etc. finally author delivers the recommendations to the smart home developers, researchers

Mookyu Parket.al. (2019) in the study entitled “Security Risk Measurement for Information Leakagein IoT-Based Smart Homes from a Situational Awareness Perspective”[4]. This paper describes the fearsof IoT security which may cause data leakage from the Cyberspace hierarchy perspective. As smart Home-based IoT devices are closely linked to human life, given that social harm is a problem. To resolve this, authors gave a method for calculating the risk of IoT devices based on safety Scenarios that could be present in a smart home. These researches highlight on detection than risk measurement. This study implemented factor analysis of information Risk (FAIR) method which randomly accesses each cause to fight assets and threats. This research provides a foundation for a real-time approach to the rapidly evolving future safety operating environment. It may also contribute to the periodic risk assessment of cyber threats, cyber-attacks and cyber threats Warfare from a National Security viewpoint.

ZaiedShouran et.al. (2019) in the study entitled “Internet of Things (IoT) of Smart Home: Privacy and Security”[5]. The main aim of this study is to examine the security requirements for safe home services, including integrity, availability, and authentication. In the smart home region, security threats typically attempt to compromise one or more of the safety objectives. Author have classified the impact in to low, moderate and high categories depending on major damage to assets, major financial losses or severe harm to individuals. Finally the study concluded to use proper security mechanism to home devices and network. Disabling the features that are not used will decrease the chances of security attacks. Do not use default password and change it time to time.

Moussawitti& Dimitri (2018)in the study entitled“IoT privacy & security Concerns: A systematic mapping of study”[6], the study aims to explore the question related to privacy & security and its issues in IoT Environment. They also tries to find out the context, security solutions and research trends. The study reveals that the issues are mainly related authentication, data encryption and key exchange mechanism. Study come up with the fact that there are many solutions to mitigate security issues but no algorithm is developed for privacy issues.

Nina Gerber et.al. (2018)in thisstudy “Home Sweet Home? Investigating Users’ Awareness ofSmart Home Privacy Threats” [7]. The study emphases on the awareness of potential privacy threatsand concerns. 1052 respondents were assess for privacy & security issues. Findings indicate that most oflay users are indeed unaware of adverse consequences whichcould arise from using smart home devices, but also lack online social network (OSN) and smart health devices. Finally author prosed the consequences loss of safety, negative impact on behaviour due to loss of private information, legal action should be taken in case of theft of personal information, negative impact on carrier etc.

Dr. D. Usha and M. Bobby (2018) in the study entitled “Privacy Issues in Smart Home Devices Using Internet of Things – A Survey” [8] present an approach to secure devices, network connectivity and firmware. Author has suggested data encryption is necessity to a great extent. Security and privacy at the device level, protecting the user and encrypting communication links these two things are identified as the key solution for many privacy and security threats.

Won Min Kang et. al.(2017) in the study entitled “An enhanced security framework for home appliances in smart home” [9]. Author have proposed holistic framework for protecting smart devices. The security framework provides the system of integrity through the self-signing and access management strategies to prevent hazards to protection, such as data Manufacture of updates, leakages, and code manipulation. This framework provides security services that ensure device authentication, integrity, and availability (CIA tried).

MarkandeshwarJerabandi(2017) in the study entitled "Internet of Things Based Technology for Smart Home System: A Generic Framework" [10]. In this paper authors have studied existing frameworks and come up with different design issues to smart home system like Serviceability, Scalability, Auto-Configuration, Programmability, and Robustness etc.finally author have introduced the new generic framework which will solve all the problem of design issues mentioned above. The core components were - Auto-Configuration and Device Management, Communication Protocol, Auto Monitoring and Control, Objects Access Control, User Interface (UI), Context Aware Adaption Scheme, Data Analysis and Visualization. The author believes that robust in nature in providing services at any time and framework is helpful to make every home comfortable and secure.

[11] Tilak, G., & Bhaumik, A. A Review on Security and Usability of Graphical User Interface Design. This paper focusses on the interface usability which is depends on the planning and designing of the goods and products. The differentiation among the phones and desktops are origin by the changing demands by the clients like memory, screen size, lack of feedback, performance etc. Systems transmit responsive information. There's important to secure the system for contemporary applications. The utilization of internet is rapidly rising from years. Due to this high-speed travelling lifestyle, where they lets the user to connect with systems from everywhere. When client is paying no attention to the functionalities within the system then the system isn't secure but, in other systems there exist some threats can harm the system.

Proposed Framework –The proposed framework is explored in depth in this section. The framework is comprised of different modules. The design of the framework is explained in Figure. 1.

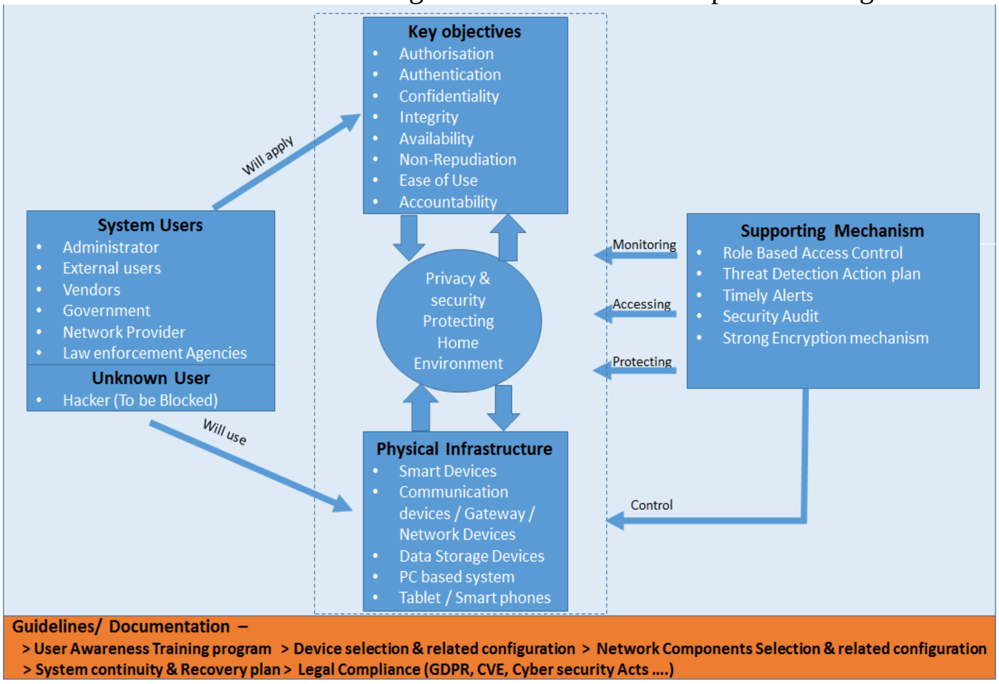


Fig. 1 – The Framework – Privacy & security protecting Home Environment

Proposed Framework Opening up with Key Security objectives, Different user/Stakeholders, Physical infrastructure, Supporting Mechanism and Guidelines to the stakeholders. Security of Private and confidential data are front protection keys for all the Activities made by user and also administrators. These keys represent the basic principles of the Smart home control system. Functions of these principles are to provide worthy and protected access to the system.It also makes maintains the availability of data usage, detection of the source that data received, authentication and authorization of users and administrators. Supporting mechanism contains a mechanism to defend safety security plan.

1.1. **Key objectives** –The goal of this module is to protect information from being stolen, compromised or attacked. **Authentication** is the process of verifying the identity of a person or device. **Authorisation** is a security mechanism which gives permission to access the devices or services. **Confidentiality** is approximately similar to protection against privacy, which prohibits unwanted information disclosure. It prevents important information from getting in the wrong hands. **Integrity** involves maintaining the reliability and credibility of data in all phases**. Availability** is the property in which data is accessed and modified in anappropriate manner by lawful persons. It guarantees reliability and persistent entree to our private data by accreditedpeople. **Ease of Use** means that the processes to use the system (authentication, access, modifications etc.) are user friendly & intuitive to user requirements. **Non-repudiation**s to detect that the source of data is confirmed with proof of delivery and the receiver of data is confirmed with proof of the sender's identity. **Accountability** means allocating the duties responsibilities for system services. It certifies that actions are in place to track events back in time to the users, or procedures.

1.2. **Users –**Smart home system can be exposed to different inside as well as outside users. Smart homes would need to provide information and service area customized to the circumstance of the user.**Administrator is a person who** ensure safe system and application authentication and resource authorisation in compliance with established policies.**Device Vendor**is responsible for installation and configuration of devices to be installed in home. **External users** may be the guest or friends to whom the temporary access need to be given. **Government**governments may require to have access to system improve services based on smart home data analysis.**Law enforcement Agencies** may need access to smart home system for crime investigation. **Network Service provider** that makes available the network services to the users. **Anonymous user/Hacker -** Hacker is a person who uses his or her ability to obtain illegal access to systems network to commit crimes. It is necessary to block the access to the hackers and protect the users' privacy.

1.3. **Physical infrastructure -** It consist of Smart IoT enabled devices Security camera, Voice assistance(Alexa), Robotic vacuum cleaner, Music player etc..**Communication appliances /Gateways / Network devices** handles all
Inter-connections between internet, application and users.**Data storage devices** holds the users' data which is very confidential and private. **PC based system** A Smart home system will keep track of all sensors, networking components, devices,sensors, networks.**Tablet/Smart Phone can be used** for performing various functions of monitor, control & configuration remotely.

1.4. **Supporting mechanism -** Supporting mechanism systems may be designed to defend against various types of threats. This mechanism involves Protection system with a mixture of hardware, firmware and applications. These all functionalities will have to work together to protect confidential and sensitive data and process and Environment. **Rolebasedmechanism**Means Separate user group as per functionality. This helps to guard the data integrity and confidentiality. **Threat Detection Action plan** willrapidlynotice the **t**hreat and respond. This can be done using Intrusion detection system(IDS) and Intrusion prevention system (IPS). Timely alerts mechanism will send instantaneous warnings on phone to keep you updated all the time. **SecurityAudit** will systematically evaluate the evidence and also assesses device configuration and environment protection, software, process information management and user practises.Finally **Strong Encryption mechanism** is obligatory to decrease network threat for protected communication.

1.5. **Guidelines & Documentation –** Lastly this framework will provide Guidelines and Documentation to the Smart home user. Following are the Guideline.

- Device selections and related arrangement
- Configuration details
- Users Role Configuration
- Network components selections
- Home-User awareness training
- Security legislation, regulatory guidelines to ensure compliance with the Information Assets

Discussion –

While developing framework, it is necessary to consider the two important things – Upgraded Technology and user's interaction with technology. These two aspects plays vital role in creating safe and secure home environment. A big challenge is discovering reliable ways of delivering a comprehensive overview whole framework to the users. And also to provide suggestions to protect the sensitive information in transit. Since openness is already a function of some IoT solutions, exploring the extent to which security and privacy can be achieved is a fascinating challenge created for the smart home installed in this context. Frameworks that improve protection are especially important in smart home settings, where a lot of private Information is processed. Information protection in this respect requires special attention. Therefore we have introduced the framework thatprotects privacy & security in Smart home Environment.

- Clearly defined security goals; that are required to be met; is the first and foremost step.Eight Security goals (authentication, authorisation, ease of use, availability etc.) have been adopted for the purposes of this study.
- Home environments contain various human actors. So it is necessary to understand the risk and potential misuse of information that may compromise privacy of the user. Different users have different roles; in smart home environment and accordingly role based access is defined.
- Physical infrastructure which should to be safeguarded from unauthorised interventions&device thefts.
- Well defined supporting mechanisms that can be implemented to prevents the risks, losses and provide recovery procedures.
- Finalsection provides important guidelines and standards,to be used in the process of protecting the Home Environment. As the security and privacy model is fully developed, smart home users will have better control on the generated confidential information. They will also have better method to determine use of this information.
-

Conclusion - As smart home technology is becoming popular day by day, the security and privacy threats will pop-up. Many smart devices struggle to maintain protection in a smart home environment, as they are vulnerable to security outbreaks.This study was accompanied to realize the threats that occur in the Smart Home Ecosystem, and how they can be mitigated. This framework provides platform that supports control system, smart devices, networking components for users to connect and collect required data (including real-time as well as historical data). It also enables configuring, monitoring and troubleshooting of resources.The efficiency and effectiveness of the Framework needs more comprehensive validation to strengthen the model presented. The validated model will behighly useful and can be quickly deployed in practise.

References –

1. Lo'aiTawalbehet. al. "IoT Privacy and Security: Challenges and Solutions", doi:10.3390/app10124102 ,2020, pp 1-17
2. MiJeongKim et.al "Developing the design solution for Smart home through user-centered scenarios",doi: 10.3389/fpsyg.2020.00335,2020, pp 1-12
3. Verena Zimmermann et. al. "Assessing Users' Privacy and Security Concerns of Smart Home Technologies" , doi.org/10.1515/icom-2019-0015). 2019, pp197-216
4. Mookyu Park et. al. "Security Risk Measurement for Information Leakage, in IoT-Based Smart Homes from a Situational Awareness Perspective", doi:10.3390/s19092148,2019, 2019 pp 1-24
5. ZaiedShouranet. al "Internet of Things (IoT) of Smart Home: Privacy and Security", DOI: 10.5120/ijca2019918450, *2019, pp 1-7*
6. [6]Moussawitti& Dimitri "IoT privacy & security Concerns: A systematic mapping of study". DOI: 10.5121/ijnsa.2018.10603, 2018, pp 25-33
7. Nina Gerber et.al "Home Sweet Home? Investigating Users' Awareness of Smart Home Privacy Threats", USENIX Symposium on Usable Privacy and Security (SOUPS) 2018, pp1-4

8. Dr. D. Usha and M. Bobby "Privacy Issues in Smart Home Devices Using Internet of Things – A Survey", Journal of Advanced Research · September 2018 DOI: 10.21474/IJAR01/7839, 2018, pp. 566-568
9. Won Min Kang, SeoYeon Moon and Jong Hyuk Park, An enhanced security framework for home appliances in smart home. DOI 10.1186/s13673-017-0087-4, 2017, pp. 1-12
10. [MarkandeshwarJerabandi "Internet of Things Based Technology for Smart Home System: A Generic Framework", IJRITCC | June 2017, Available @ http://www.ijritcc.org, 2017, pp 1038-1046
11. Tilak, G., & Bhaumik, A. A Review on Security and Usability of Graphical User Interface Design.