How to Cite:
Vineet Kumar Kathuria and Dr.Prerna Pareek (Nov 2020). EXISTING SECURITY, FACTORS AFFECTING THE SECURITY, ITS REQUIREMENTS AND FUTURE CHALLENGES IN IoT BASED SMART HOME
International Journal of Economic Perspectives,*14*(1), 242-255
Retrieved from https://ijeponline.org/index.php/journal/article

EXISTING SECURITY, FACTORS AFFECTING THE SECURITY, ITS REQUIREMENTS AND FUTURE CHALLENGES IN IoT BASED SMART HOME

[1]Vineet Kumar Kathuria, Research Scholar, Department of Computer Science, Shri Khushal Das University, Hanumangarh (Rajasthan)-India
[2]Dr.Prerna Pareek, Research Supervisor, Department of Computer Science and Engineering, Shri Khushal Das University, Hanumangarh (Rajasthan)-India

ABSTRACT

IoT has emerged as one of the most important technologies of the twenty-first century in recent years. Now that we can connect everyday objects to the internet via embedded devices, including as kitchen appliances, vehicles, thermostats, and baby monitors, seamless communication between people, processes, and things is conceivable. The ability of smart homes to make life easier and more convenient is undeniable. Home networking can also provide you a sense of security. The smart home will keep you informed about what's going on whether you're at work or on vacation, and security systems can be built to provide a great deal of assistance in an emergency. Not only would a person be notified of a fire alarm, but the smart home would also unlock doors, call the fire service, and illuminate the way to safety. Security and privacy are particularly threatened as a result of this. While the proposed remedies go a long way toward addressing security issues, there are still some places where further work is required. The main aim of this study is to discuss the Existing Security, Factors Affecting the Security, Its Requirements and Future Challenges in Iot Based Smart Home. The paper's two main contributions are to outline existing network strategies for securing Smart Homes and to propose two areas of particular concern (system auto-configuration and security updates) where more research is needed. The major future criteria for trusted Smart Home systems are identified in this article.

Keywords - Existing Security, Iot, Factors, Future Challenges, Requirement etc.

1. INTRODUCTION

Over the last few decades, smart home development has been a rapidly expanding sector that has faced numerous hurdles. Recent improvements in information and communications technologies, on the other hand, have propelled Smart Home development to a mature state. A Smart Home is a living environment that uses smart home technology to meet the residents' goals of comfort, safety, security, and efficiency.

Smart home technology accomplishes these objectives by combining a range of home technologies into one environment. Home Appliances, Lighting and Climate Control System, Home Entertainment System, Home Communication System, and Home Security System are all examples of Smart Home systems. Based on the applications it supports, each of the above systems has distinct needs (e.g. data rate, distance). As a result, various physical media are appropriate for various Smart Home systems. The physical medium that Smart Home systems can use in a Smart Home is the following: existing wiring, new wiring, and air. The term "existing wiring" refers to the electrical wire, telephone wiring, and coax cable that are already in place. The air refers to wireless networking, and new wiring necessitates the installation of new cable in the walls.

Corresponding author: **Vineet Kumar Kathuria and Dr.Prerna Pareek**
Submitted: 27 Aug 2020, Revised: 09 Sep 2020, Accepted: 12 Oct 2020, Published; 30 Nov 2020

2. CONCEPT OF SMART HOME

It is critical to identify the major components of the Smart Home architectural model in order to comprehend the elements that contribute to security breaches in a Smart Home environment and to recognise security solutions that may be used to reduce the risk of security breaches. The internal network, the external network, and the residential gateway are the three essential components that make up a smart home. In Figure 1, these three elements are depicted.

The internal network, which can be both wired and wireless, is the foundation of a Smart Home. A Smart Home's internal network combines a variety of communication mediums and protocols to enable a variety of Smart Home systems that help occupants simplify their lives and improve their quality of life. The Internet and the service provider, who is responsible for providing Internet-based services to the household members, are part of the Smart Home's external network. Finally, a residential gateway (RG) is an always-connected device in a Smart Home that plays a critical function in connecting the Smart Home's internal network to the outside world.

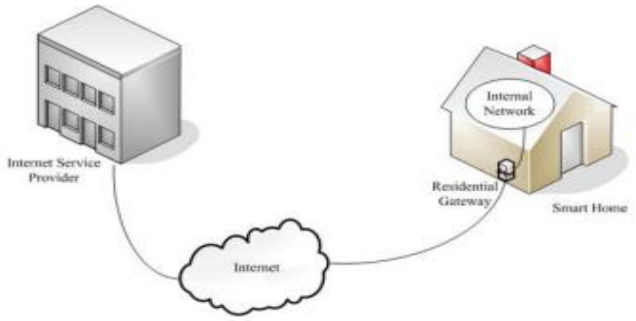


Figure 1: Smart home concept243

2.1 Smart Home Systems

The Smart Home internal network can connect a variety of Smart Home devices to provide a convenient and safe environment for household members while also assisting them in accomplishing their daily activities. There are four different types of smart home systems: Home appliances, lighting and climate control, home entertainment, home communication, and home security systems are all examples of home appliances.

- Home Appliances, Lighting and Climate Control System
- Home Entertainment System
- Home Communication System
- Home Communication System

3. IoT

The Internet of Things, or IoT, refers to a network of linked devices as well as the technology that enables communication between devices and the cloud as well as between devices. We now have billions of devices connected to the internet, thanks to the introduction of low-cost computer chips and high-bandwidth telephony. Sensors can be used in daily products such as toothbrushes, vacuum cleaners, vehicles, and machinery to collect data and respond intelligently to consumers.

The Internet of Things combines the internet with daily "things." Since the 1990s, computer engineers have been attaching sensors and processors to everyday things. However, because the chips were large and cumbersome, progress was slow at first. RFID tags, which are low-power computer chips, were first employed to track expensive equipment. As computing machines became smaller, quicker, and smarter, these chips became smaller, faster, and smarter.

Corresponding author: **Vineet Kumar Kathuria and Dr.Prerna Pareek**
Submitted: 27 Aug 2020, Revised: 09 Sep 2020, Accepted: 12 Oct 2020, Published; 30 Nov 2020

The cost of incorporating computing power into small things has decreased dramatically in recent years. Connectivity with Alexa speech services capabilities, for example, can be added to MCUs with less than 1MB embedded RAM, such as light switches. A whole industry has built up around the idea of putting IoT devices in our homes, businesses, and offices. These intelligent objects can autonomously send and receive data over the Internet. The Internet of Things refers to all of these "invisible computing devices" and the technology that supports them.

4. **IoT AND THE SMART HOME** When smart electronics are integrated as part of a new home build, professional system design, installation, and setup may be available. Smart Home IoT technology, on the other hand, is most likely to be adapted to an existing home piece by piece as needs emerge. In the design and operation phases of IoT adoption in the Smart Home, there is frequently no continuous expert support. While some specific Smart Home standards are quite widely used, such as X.10 powerline-carrier communications, they lack security and were created before these home management networks were connected to the Internet (Ricquebourg, V, et al 2006). There are now numerous networking technologies that can be utilised in the home (Zwave, Insteon, Bluetooth, Zigbee, Ethernet, Wifi, RS232, RS485, C-bus, UPB, KNX, EnOcean, Thread, etc). (Alam, M.R, et al 2012). Each has advantages and disadvantages, and expecting a non-expert to handle a heterogeneous network with several distinct protocols effectively and securely creates considerable hurdles.

The Smart Home has the potential to deliver increased comfort and security as well as improved environmental sustainability. Instead of using basic manual or fixed-schedule control techniques, a smart air conditioning system can leverage a range of household sensors and web-based data sources to make intelligent operational decisions. By collecting location data, the smart air conditioning system can estimate projected house occupancy and ensure that the air conditioner meets the appropriate comfort level while the house is inhabited while conserving energy when it is not.

In addition to improved comfort, the Smart Home can help the elderly live independently. Cleaning, cooking, shopping, and laundry are just a few of the duties that the Smart Home can help with. Low-level cognitive decline can be aided by intelligent home devices that deliver prescription reminders on a regular basis. Home health monitoring can alert caregivers to intervene before costly and inconvenient hospitalization is required. However, none of these advantages are likely to be utilized unless the Smart Home system is secure and reliable.

5. SECURITY THREATS IN THE SMART HOME

5.1 Threats

Despite the fact that the Smart Home is a totally diverse setting, the nature of security risks is identical across all domains.

- **Confidentiality** - Threats to confidentiality are those that result in the unintentional release of sensitive data. Confidentiality breaches in home monitoring systems, for example, can result in the unintentional publication of sensitive medical data. Even seemingly harmless data, such as inside home temperature and air conditioning system performance parameters, could be utilised to detect whether a residence is occupied or not, as a preliminary to theft. Unauthorized system access is a hazard if confidentiality is lost in things like keys and passwords.
- **Authentication** threats can lead to the tampering of either sensing or control information. Unauthenticated system status alerts, for example, may lead a house controller to believe there is an emergency and open doors and windows to allow an

Submitted: 27 Aug 2020, Revised: 09 Sep 2020, Accepted: 12 Oct 2020, Published; 30 Nov 2020

emergency exit, when in fact they are permitting criminal entrance. Automated software updates are one concern that will be discussed later; if these are not properly authenticated, difficulties can develop.

- **Access** - Threats to access are perhaps the most serious. Unauthorized access to a system controller, especially at the administrator level, renders the system insecure as a whole. This might happen as a result of poor password and key management, or it can happen as a result of illegal devices connecting to the network. An unauthorised connection to a network might steal network bandwidth or cause a denial of service to legitimate users even if control cannot be gained. Because many Smart Home gadgets are battery-powered and have a low operational duty cycle, flooding a network with requests might result in an energy depletion attack, which is a type of denial of service?

5.2 Vulnerabilities

- ***Access to networked systems is a serious vulnerability***. Because modern Smart Home systems are networked, attacks can be carried out remotely, either through direct access to networked control interfaces or through the distribution of malware to devices.
- ***Physical accessibility to the system is also a concern***. The networks can be physically accessed from outside the house for both wireless and power-line carrier technologies, even if the house is securely closed. The next weakness is a lack of system resources. Small 8-bit microcontrollers with low computing and storage resources have traditionally been used as device controllers, limiting their capacity to perform complicated security algorithms.
- ***The vulnerability of a system is its heterogeneity***. Devices are made by a variety of companies and have varying networking standards and software update capabilities. Frequently, the gadgets lack documentation about their internal software, operating systems, and security procedures.
- ***Another issue is updated firmware***. Only a few smart home gadgets offer any kind of regular software update service to address security flaws. For devices that cost a few dollars, there appears to be no incentive to constantly patch software to stay ahead of security problems.
- ***Slow adoption of standards exposes a company to risk***. While some proprietary systems, such as a health monitoring subsystem, may have well-designed standards-compliant security, the majority of existing Smart Home gadgets have little, if any, security features. The absence of dedicated security professionals who can manage the complexities of a Smart Home network is the biggest threat, according to us. Few people can afford to hire a professional to operate their home network on a long-term basis. Instead, novice homeowners must be able to self-manage their systems in a simple, safe, and secure manner.

5.3 Vulnerability Example

For example, a homeowner may believe that only users who have been granted the web cam's host name and port number can access it. Many gadgets are suddenly known and visible because to Internet device–scanning search engines like Shodan (https://www.shodan.io) and Censys (https://censys.io), which properly search for available sensors.

Traditional search engines, such as Google and Bing, crawl the Internet by downloading webpages and indexing webpages, photos, and some popular file types by following hyperlinks on those pages. Internet device–scanning search engines, on the other hand, operate similarly to a network scanner, scanning the open ports of Internet nodes and indexing the header or banner data returned by connected devices; the headers or banners of the reply frequently include the device type, model, vendor, firmware version, and other data. Apart from HTTP and HTTPS, Internet device–scanning search engines connect to open ports of nodes using a number of protocols (FTP, SSH, DNS, SIP, and RTSP, for example). These search engines also provide an application programming interface (API) that allows programmatic access to their search results. These search engines can be used by attackers to locate susceptible devices on the Internet. For example, Shodan will return a list of home surveillance cameras with their IP addresses, geographic locations, and screenshots if you search for "has screenshot: true port:"

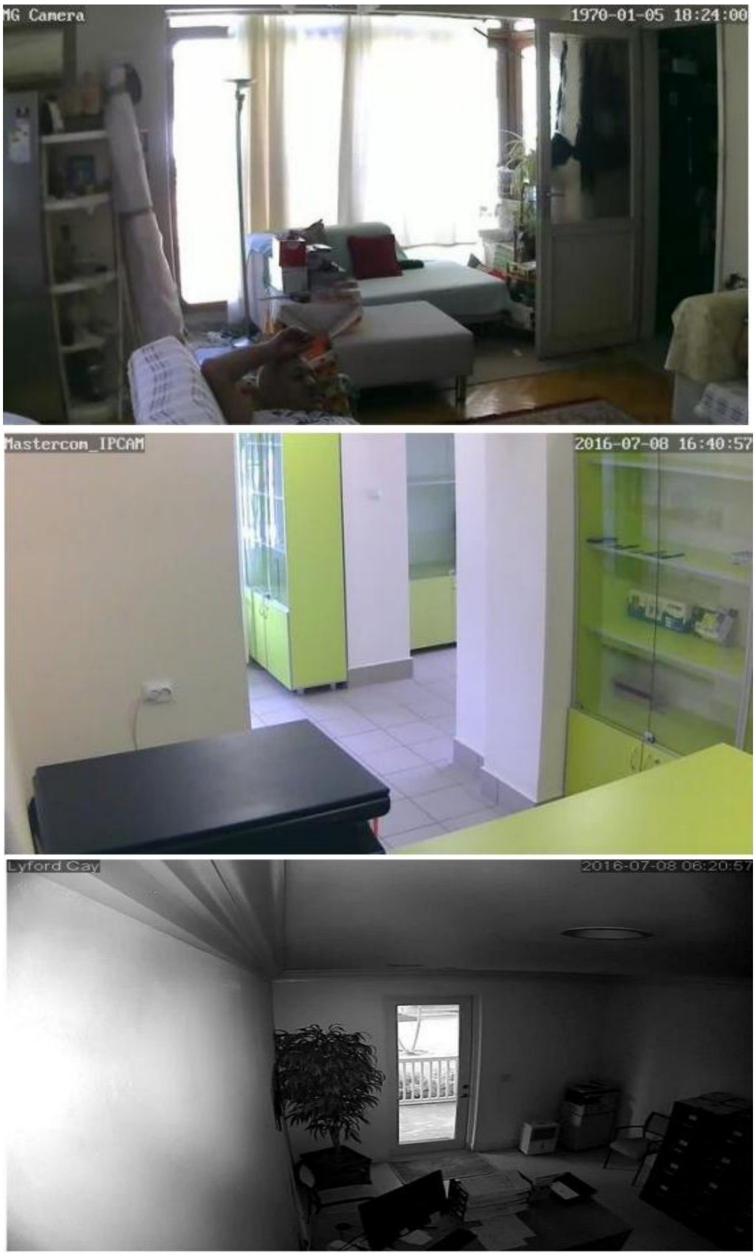
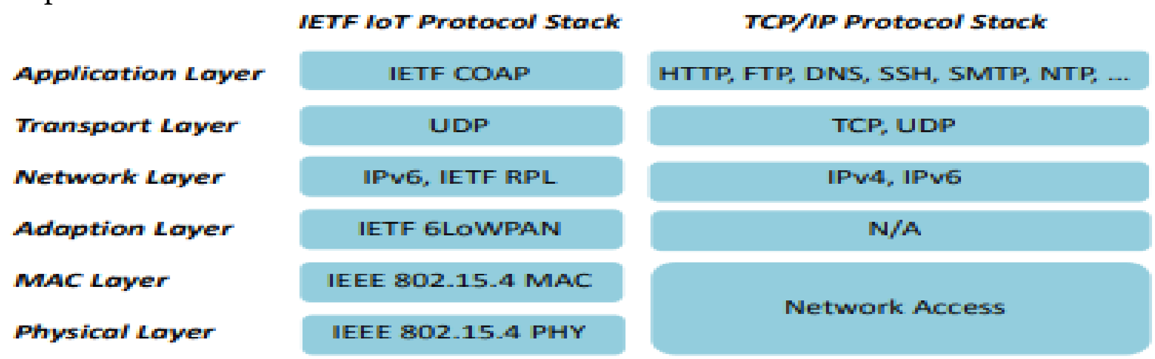


Figure 2:The Internet device–scanning search engine Shodan has compiled a list of home surveillance cameras

Corresponding author: Vineet Kumar Kathuria and Dr.Prerna Pareek
Submitted: 27 Aug 2020, Revised: 09 Sep 2020, Accepted: 12 Oct 2020, Published; 30 Nov 2020

6. SOME EXISTING SECURITY SUPPORT FOR IOT

IoT computing devices are typically less powerful than regular desktop and laptop computers due to their low cost. The majorities of Internet of Things devices are low-power, employ a low-end microprocessor, and have minimal memory. These controllers are well-suited to the needs of standalone controllers in washers and air conditioners. However, because existing Internet protocols are not normally built for embedded devices, these traits have made the transition to networked IoT controllers more difficult. To address these issues, the Internet Engineering Task Force (IETF) has formed many working groups. The IETF's IoTstandardisation effort has been crucial in developing the requisite light-weight communication protocols for limited contexts over the existing IP network. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN: RFC 6282) (Thubert, P, 2011), IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL: RFC 6550) (Brandt, A, et al 2012), and Constrained Application Protocol (CoAP: RFC 7252) are a few examples (Shelby, Z, et al 2014). The IETF IoT and TCP/IP protocol stacks are compared in Figure 3. Once devices are connected to the Internet, any Internet-based security concerns could undermine IoT security and privacy. We'll go over the current security implementations for these basic IoT protocols in the sections below.



	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	

Figure 3:The comparison of the IETF Internet of Things and the TCPIP protocol stacks

6.1 6LoWPAN and Security

The 802.15.4 standard for wireless personal area networks was developed by the Institute of Electrical and Electronics Engineers (IEEE) (WPANs). IEEE 802.15.4 specifies how the physical and media access control layers should function in these networks' low-bandwidth, low-cost, low-speed, and low-energy environments. As a result, 6LoWPAN (Shelby, Z, et al 2011) is a lightweight protocol developed by the Internet Engineering Task Force to allow IPv6 packets to be sent across IEEE 802.15.4 wireless networks.

To provide data integrity, secrecy, origin authentication, and anti-replay protection for IPv6 packets, the Internet Protocol Security (IPsec) suite has specified Authentication Headers (AH) and Encapsulating Security Payloads (ESP). To implement IPsec and allow end-to-end secure communications between wireless devices, the authors proposed compressed AH and ESP features for 6LoWPAN.

6.2 RPL and Security

Routing protocols are an important part of traditional networks, and the same is true for 6LoWPAN networks. RPL is an IPv6 routing protocol optimised by the Internet Engineering Task Force (IETF) for Low Power and Lossy Networks (LLNs), and is largely used by 6LoWPAN networks. The mapping topology of RPL is based on a Destination-Oriented Directed Acyclic Graph (DODAG) structure, and it is a distance-vector routing protocol. In Trust Anchor Interconnection Loop (TRAIL), a generic topology authentication scheme for

Corresponding author: **Vineet Kumar Kathuria and Dr.Prerna Pareek**
Submitted: 27 Aug 2020, Revised: 09 Sep 2020, Accepted: 12 Oct 2020, Published; 30 Nov 2020

RPL has been presented (Perrey, H, et al 2013). By detecting and isolating forged nodes, TRAIL can prevent topological inconsistency attacks from spurious nodes. TRAIL uses a round-trip

message to verify upward path fidelity to the root node and to assist nodes in the tree in receiving real rank information. TRAIL distinguishes itself by allowing each node in the tree to confirm its upward journey to the root and detect any phoney rank attacks.

Because every node except the root must have a parent node, it is critical for nodes in the DODAG tree to select the correct parent nodes. The RPL rank is used to define the position of a node in a tree topology. The authors provide a safe selection strategy to assist a child node in selecting a genuine parent node. To prevent spoofing nodes from becoming its parent, the selection method calculates a node's threshold value based on the average and maximum rank values of its neighbour nodes. As a result, existing technologies can assure the secure construction of routing tables in Smart Home networks.

6.3 CoAP and Security

CoAP is an HTTP-like application layer protocol for device networks with limited resources. CoAP provides multicast functionality, which HTTP lacks, because some unique requirements, such as group communications in IoT networks, necessitate it. CoAP uses the User Datagram Protocol (UDP) protocol to better suit low-bandwidth connections and low-computational-power device situations. When compared to its counterpart Transmission Control Protocol, UDP is a simpler, low-latency, and connectionless transport layer protocol (TCP). CoAP is a stateless protocol that employs a client-server architecture. It exchanges messages between the client and server via request/response operations. CoAP, like HTTP, is based on a representational state transfer (REST) model, in which each server resource has its own Uniform Resource Identifier (URI), and a client can access a resource by sending a request to the server using one of four methods: GET, POST, PUT, or DELETE. Transport Layer Security (TLS: RFC 5246) (Dierks, T.; Rescorla, E. 2008) is the most widely used encryption protocol for HTTP nowadays, but TLS implementation is overly difficult for resource-constrained IoT devices. CoAP uses the Datagram Transport Layer Security (DTLS: RFC 6347) security protocol to protect communications. TLS and DTLS both provide the same level of security. TLS and DTLS are distinguished by the fact that TLS is based on the TCP protocol whereas DTLS is based on the UDP protocol. There are four different security modes defined in the CoAP specification. NoSec, PreSharedKey, RawPublicKey, and Certificate are the four security modes that a device can use. Within restricted networks, IETF standards enable secure means for secure web-based communications.

6.4 Future IoT Security Directions

As the three examples above show, there is already a lot of work being done to secure mission-critical IoT applications. IP-compatible secure communications networks that are suited for resource-constrained devices and use state-of-the-art security mechanisms have taken a lot of time and effort to build. However, to create and maintain a secure IoT system, many of these solutions necessitate thorough, unified, system-wide architecture and expert network engineers. Our focus is on the system management side of Smart Home security, i.e., how to correctly install and maintain the protection afforded by these powerful technologies, rather than on this sort of "technical" security.

7. REQUIREMENTS OF SECURITY IN SMART HOME

The security needs for a Smart Home environment are determined after presenting the concept of a Smart Home and describing the networking technologies utilised to implement its systems. Confidentiality, Integrity, Authentication, Authorization, Non-repudiation, and Availability are the primary security criteria that a Smart Home ecosystem must meet.

Confidentiality refers to the protection of sensitive information from unauthorised access. In order to enable indirect monitoring of residents' actions in a Smart Home setting, an adversary may exploit services giving information about the Smart Home's status as part of a confidentiality assault (Komninos et al., 2007a; Komninos et al., 2007c). Using symmetric cryptographic cyphers, confidentiality can be accomplished (i.e. block or stream ciphers).

Integrity is a type of security service that guards against unwanted data change. During any operation, such as transfer, storage, or retrieval, integrity assures that data is not modified, damaged, or lost. Integrity, in other terms, ensures that data is consistent and correct. A malicious attacker who eavesdrops on communications to or from a Smart Home's internal network and tampers data can endanger its integrity. A Message Authentication Code can be used to provide integrity (MAC).

Authentication is a type of security service that involves verifying an entity using a password or a shared secret key between communication parties. Authentication is the process of one entity confirming the identity of another. Entity authentication and message authentication are the two types of authentication. Entity authentication ensures that each entity's declared identity is genuine. Entity authentication, in other words, verifies the identity of communicating parties. Message authentication, on the other hand, ensures that a message comes from the stated entity. User-to-device, user-to-internal network, device-to-device, device-to-internal network, and user-to-service provider authentications all require a variety of authentication procedures in a Smart Home context. In order to get essential information about home users or access Smart Home environment services, an adversary may pose as another genuine user or company (Jeong et al., 2006; Komninos& Mantas, 2009).

Authorization is the process of determining a user's access privileges to a device or network resource, as well as what a device can perform in the Smart Home context. Authorization can also provide multiple access levels to ensure that organisations can only access and operate on network resources for which they have been granted permission. There are two sorts of devices in the Smart Home internal network: home devices and foreign devices. The authorization procedure for home devices is based on the home user's access privileges to the devices. In the case of foreign devices, the device's owner delegated specific access privileges to foreign users who must pay to utilise them. In a Smart Home context, however, an adversary can utilise falsified authorizations to undertake illegal behaviours (Schwiderski-Grosche et al., 2004).

Non-repudiation is a security service that protects against rejection of participation in an action. Nonrepudiation, for example, precludes both the sender and the receiver from denying the transmission of a message or access to services. This service is akin to having the author or recipient of a document sign a document in person. Furthermore, this service is unable to prohibit an entity from retracting a certain activity. It can, however, provide proof (e.g., proof of commitment, resource use, obligation, and data origin) that can be maintained and utilized later by a trusted third party to resolve disputes that emerge when one of the organizations involved in the activity repudiates the action. Digital signatures based on public key encryption cryptosystems can offer non-repudiation (Stallings, 2005)

Availability ensures that network services and resources (such as bandwidth) remain available and safeguarded from network-wide events like malicious assaults. Because it is

Corresponding author: Vineet Kumar Kathuria and Dr.Prerna Pareek
Submitted: 27 Aug 2020, Revised: 09 Sep 2020, Accepted: 12 Oct 2020, Published; 30 Nov 2020

directly connected to the Internet, the Smart Home internal network is particularly vulnerable to direct denial of service assaults. Furthermore, since the internal network is vulnerable to a number of attacks that result in the loss or reduction of availability, disaster recovery solutions are incorporated in this service.

8. FACTORS AFFECTING THE SECURITY IN SMART HOME

In a Smart Home context, security is a vital concern. Many people are concerned about unwanted entry to their homes and the protection of their personal information. However, due of its heterogeneous character, dynamic nature, constant Internet connectivity, and open security back doors drawn from family members, providing security in the Smart Home environment is not an easy task (Thomas & Sandhu, 2004; Wang et al., 2005; Haque&Ahamed 2006). As we've already mentioned, the Smart Home internal network is quite heterogeneous because it comprises of a diverse set of devices, apps, and communication protocols. Many devices, such as light switches, white appliances, sensors, cameras, TVs, phones, PCs, and PDAs, communicate with each other via wired and wireless networks in a Smart Home, and have quite distinct capabilities and requirements (Ziegler et al., 2005). As a result, the deployment of security mechanisms is dependent on the capabilities and requirements of the device. In terms of memory storage, battery power, and computing performance, devices have a wide range of capabilities (Haque&Ahamed 2006). PCs, for example, can easily do complex computations while still supporting security features. However, due to their limited resources, some devices, such as the handset of a cordless phone, do not have the necessary processing capacity (i.e. memory storage, battery power and computational capability). These gadgets typically offer no protection or can only support basic security methods. Intruders can breach residential networks by abusing these devices. Furthermore, not every gadget necessitates the same amount of protection. It might range from a low to a high level. Depending on the needs of each device, different security techniques should be implemented.

Furthermore, Smart Home Systems support a wide range of applications. There are programmes that support many sorts of data, such as audio and video signals, as well as low-date-rate sensor data, each with its own set of characteristics. As a result, each application should have its own security system that is optimized for it. Security procedures that do not add latency or jitter are required for applications that enable high data rate services (e.g. multimedia applications). On the other hand, because of power consumption, applications that enable low data rate services (e.g. over a sensor network) may be forced to adopt complicated security mechanisms. Furthermore, having discussed Smart Home networking technology in the section "Smart Home Networking Technology," it is evident that a Smart Home's internal network is a completely heterogeneous network that combines a variety of communication methods. Each Smart Home networking technology has its own set of features as well as security flaws. Because of their broadcast nature, wireless technology, for example, can be easily tapped. An attacker can intercept a signal or disrupt a wireless communication's normal operation.

Wired systems, on the other hand, are designed to give higher degrees of security. There are many wireless devices in a Smart Home setting that provide a wide range of services and join and leave the internal network at will, generating a very volatile ad hoc sub-network. This ad hoc sub-network is very dynamic and changes on a regular basis. As a result, the internal network's topology is dynamic, which means that the essential security mechanisms should be dynamically reconfigured whenever the topology is altered without the interaction of the home user. The internal network, on the other hand, has a number of security flaws. However, because of its inherent dynamic character, deploying security procedures in an ad hoc network is a difficult task. As a result, in order to prevent security breaches, ad hoc networking security solutions should be built on dynamic security mechanisms with appropriate intelligence.

Furthermore, the expansion of the Smart Home internal network to the outside world via the Internet causes numerous network security issues, as it is vulnerable to a range of cyber threats such as DoS attacks, malicious malware, and eavesdropping, among others (Kim et al., 2007). Smart Home high-speed connections, in contrast to dial-up Internet connections, give constant Internet connectivity, implying a static IP address. Because the IP address does not vary, attackers have a lot of time to guess the IP address and hack the linked devices, making the internal network easy to infiltrate (Herzog et al., 2001). Furthermore, because it is accessible via the Internet, the internal network is vulnerable to all of the traditional security threats that an open network faces. First and foremost, malevolent intruders can wreck havoc in a Smart Home environment by intercepting and modifying remotely transmitted communications of networks (e.g., Powerline, Phoneline, and wireless networks) that make up the Smart Home's internal network. Furthermore, malevolent attackers may obtain access to the internal network and use it to launch attacks against other networks, so obscuring their presence. Adversaries can also exploit the hacked internal network's computing power and resources to launch Denial of Service attacks against other Internet nodes. Furthermore, by eavesdropping on the Internet traffic of household members, enemies may obtain access to confidential information. Adversaries can obtain credit card numbers or learn about household members' behaviour by sniffing messages from e-banking transactions, for example. They can also obtain the home's locking mechanism password in order to break in.

As a result of the heterogeneity of devices, applications, and communication technologies in a Smart Home environment, as well as the dynamic nature of the Smart Home internal network and the fast permanent connection to the outside world, no single security solution is capable of providing all required security services in order to reduce the risk of security attacks. As a result, a variety of security methods, protocols, and services that should be integrated and controlled in the Smart Home internal network can be used to handle the difficulties of security insurance.

Finally, the members of the family play a role in making a Smart Home environment vulnerable to a wide range of security threats. The majority of household members are non-professionals in the field of networking and network security. However, they frequently construct internal networks without the involvement of security experts. As a result, there are always security flaws in the internal network that intruders can exploit. Furthermore, family members frequently abuse their privileges, posing several security concerns. Furthermore, many home users believe that suitable security measures are difficult to implement and are unwilling to do so due to low usability. Furthermore, there are instances where residents do not employ security protection or follow security policies because they either do not care about security or do not fully comprehend the hazards they face.

9. FUTURE SMART HOME SECURITY CHALLENGES

In order for a gateway-based Smart Home design to be sufficiently secure for general adoption; our study is now looking into two enhancements. Because our research is still in its infancy, we describe the difficulties and general system architectures as a first step toward solutions.

9.1 Auto-Configuration Support

Smart Home networks are projected to connect an increasing number of smart household appliances. The most significant problem in the home environment is a lack of technical

Corresponding author: **Vineet Kumar Kathuria and Dr.Prerna Pareek**
Submitted: 27 Aug 2020, Revised: 09 Sep 2020, Accepted: 12 Oct 2020, Published; 30 Nov 2020

help. Households will be saddled with time-consuming, repetitive, and error-prone manual chores for adding and administering smart devices to their home networks, which could constitute a significant security risk. As a result, a safe auto-configuration approach should be investigated further for the effective implementation of a Smart Home, not only to simplify Smart Home device installation and maintenance, but also to improve the security of the auto-configuration process. Our strategy necessitates gateway and cloud-based service capability. When a new device is connected to the network, the gateway will utilise the device ID to query a trusted web service for information on the device, including its capabilities, commands, encryption and networking protocols, and any critical firmware upgrades that are now available. Most auto-configuration approaches require a lot of this information to be saved on the devices themselves, as well as the ability for the devices to already implement a deep protocol stack. A simple device ID and a web service ensure that this information is easily accessible and up-to-date using our approach. Figure 4 depicts a typical network design as well as the procedures required to start the auto-configuration process. (Ruckebusch, P, et al 2016)

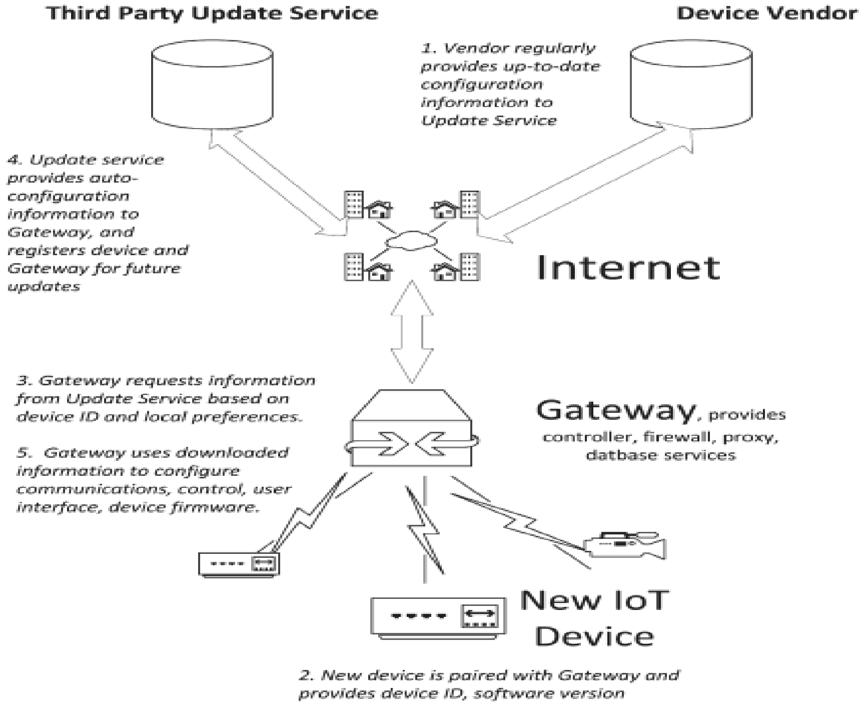

Third Party Update Service
Device Vendor
1. Vendor regularly provides up-to-date configuration information to Update Service
4. Update service provides auto-configuration information to Gateway, and registers device and Gateway for future updates
Internet
3. Gateway requests information from Update Service based on device ID and local preferences.
5. Gateway uses downloaded information to configure communications, control, user interface, device firmware.
Gateway, provides controller, firewall, proxy, datbase services
New IoT Device
2. New device is paired with Gateway and provides device ID, software version

Figure 4:Architecture of Auto-configuration

9.2 IoT Software and Firmware Updates

As security vulnerabilities are discovered and patched, desktop operating systems are updated on a regular and automatic basis. Mobile devices, such as smart phones, receive regular software updates as well, which include measures to check the changes' legitimacy. Because the number of operating system versions and operating system makers is limited, and the number of deployed devices is in the millions, such systems are economically viable. For the hundreds of various IoT devices, there is no such frequent updating service available. An Internet of Things (IoT) device is a set of hardware and software that performs specific, dedicated activities. Firmware is a sort of software that is stored in a smart device's non-volatile memory. Firmware is the programme that directly communicates with the hardware, regulating the system's operations and functions, from initializing the device to interacting with users, processing requests, and doing activities. It is a crucial aspect of any IoT system. As a result, it's critical to keep smart device firmware up to date in order to address security

Corresponding author: **Vineet Kumar Kathuria and Dr.Prerna Pareek**
Submitted: 27 Aug 2020, Revised: 09 Sep 2020, Accepted: 12 Oct 2020, Published; 30 Nov 2020

flaws, improve functionality, add new features, and cure other faults. Unlike an enterprise-scale system, which has its own specialized IT department or technical team to maintain and deliver software upgrades, the Smart Home environment typically does not. Smart Home IoT devices should have systems in place to automatically apply safe and secure firmware updates with little or no user engagement. The home gateway can control this feature. (L. Atzori et al., 2010)

Certificate-based digital signatures should be used for updates to assure their integrity and authenticity, as well as to prevent possible firmware tampering, such as malware infiltration. Each update must be confirmed against its digital signature, and the digital certificate must be examined to ensure it is legitimate and provided by the vendor or a trusted third party before being installed. The methods for downloading new updates must also be carefully considered. A hacker could prevent fresh updates from being installed and launch an attack on unpatched firmware if the update-checking mechanisms are exploited. Attackers might even pass off an older version of firmware with security flaws as the most recent version, causing the firmware to revert to a faulty version. As a result, the device manufacturer or vendor should encrypt and digitally sign the updated release information to prevent cybercriminals from interfering with the update version maintenance process. Delta updates, which only contain the data that has changed, considerably enhance efficiency and reduce installation job time due to the low bandwidth and resource-limited nature of many smart devices. This reduces the risk of update failure, which is especially important for battery-operated devices due to battery power exhaustion during the lengthy firmware upgrading procedure.

Generic extension for Internet-of-Things Architectures (GITAR) is a new software update mechanism for resource-constrained IoT devices that may be applied to existing IoT operating systems. According to the authors, this architecture can apply partial code updates (delta updates) for protocols and programmes during run-time using conventional file formats, tools, and techniques. There are three levels to this architecture: the static system level, dynamic component level, and kernel level. At the system level, the main operating system components and hardware drivers are implemented. The system level is divided into a hardware abstraction (HAL) and a hardware interface (HIL) layer to improve programme portability. Only the entire firmware can be updated to update the static code at the system level. The apps and network protocol components run at the component level, not at the system level, and the code at the component level is flexible, which means it can be upgraded dynamically rather than changing the entire firmware. The interface between the system and component levels is the kernel level. It connects dynamic components as well as system functions. The authors showed their approach with Contiki, a popular open-source IoT operating system, without requiring major changes to existing network protocols and applications' source code.

10. CONCLUSIONS

In this paper, we have introduced the concept of the Smart Home as well as its systems, and we have also looked at the dangers that aim to compromise the security needs. Finally, existing security mechanisms were discussed, including those that provide security features in a Smart Home context. For example, Gartner projects that the number of connected devices will increase from 5 billion in 2015 to 25 billion by 2020, representing a rapid expansion of the Internet of Things computing paradigm. The availability of reasonably priced Internet-linked household equipment, such as light bulbs, cameras, televisions, thermostats, and locks, is spurring the development of what we refer to as "smart connected houses," which are homes that are connected to the Internet. The Internet of Things does not consist of a single application domain, and the security measures employed in a domestic Smart Home application are significantly different from those employed in mission-critical applications in business or utilities. One particular problem is that the security of the network is dependent on the installation and configuration of the network by a large number of inexperienced individuals. Effective security rules and methods become much more difficult to establish, implement, enforce, and maintain as a result of this, unless they can be done on an automated basis. Our preferred solution to resolving these issues is to use a Smart Home gateway architecture supported by web-services for automatic device and network configuration, as well as automatic system updates.

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
2. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. Comput. Netw. 2010, 54, 2787–2805.
3. Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Vasseur, J.P.; Alexander, R. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks; RFC 6550; Winter, T., Thubert, P., Eds.; Internet Engineering Task Force: Fremont, CA, USA, 2012.
4. Dierks, T.; Rescorla, E. The Transport Layer Security (Tls) Protocol Version 1.2; RFC 5246; Internet Engineering Task Force: Fremont, CA, USA, 2008
5. Haque, M., &Ahamed, S. I. (2006). Security in Pervasive Computing: Current Status and Open Issues. International Journal of Network Security, 3(3), 203–214.
6. Haque, M., &Ahamed, S. I. (2006). Security in Pervasive Computing: Current Status and Open Issues. International Journal of Network Security, 3(3), 203–214
7. Jeong, J., Chung, M., & Choo, H. (2006). Secure User Authentication Mechanism in Digital Home Network Environments. In Sha, E., Han, S.-K., Xu, C.-Z., Kim, M. H., Yang, L. T., & Xiao, B. (Eds.), Embedded and Ubiquitous Computing (pp. 345–354). Springer
8. Kim, G. W., Lee, D. G., Han, J. W., & Kim, S. W. (2007). Security Technologies Based on Home Gateway for Making Smart Home Secure. In Denko, M. (Eds.), Emerging Directions in Embedded and Ubiquitous Computing (pp. 124–135). Springer.
9. Komninos, N., &Douligeris, C. (2009). LIDF: Layered intrusion detection framework for adhoc networks. Journal in Ad Hoc Networks, 7(1), 171–182.
10. Komninos, N., Vergados, D., &Douligeris, C. (2007a). Authentication in a Layered Security Approach for Mobile Ad Hoc Networks. Journal in Computers & Security, 26(5), 373–380
11. Komninos, N., Vergados, D., &Douligeris, C. (2007c). Multifold Authentication in Mobile Ad-Hoc Networks. International Journal of Communication Systems, 20(12), 1391–1406
12. Perrey, H.; Landsmann, M.; Ugus, O.; Schmidt, T.C.; Wahlisch, M. Trail: Topology Authentication in RPL. 2013, arXiv:1312.0984v2.
13. Ricquebourg, V.; Menga, D.; Durand, D.; Marhic, B.; Delahoche, L.; Loge, C. The Smart Home Concept: Our Immediate Future. In Proceedings of the 2006 1st IEEE International Conference on E-Learning in Industrial Electronics, Hammamet, Tunisia, 18–20 December 2006; pp. 23–28. 17.
14. Ruckebusch, P.; de Poorter, E.; Fortuna, C.; Moerman, I. Gitar: Generic extension for internet-of-things architectures enabling dynamic updates of network and application modules. Ad Hoc Netw. 2016, 36, 127–151.

Submitted: 27 Aug 2020, Revised: 09 Sep 2020, Accepted: 12 Oct 2020, Published; 30 Nov 2020

15. Schwiderski-Grosche, S., Tomlinson, A., Goo, S. K., & Irvine, J. M. (2004). Security Challenges in the Personal Distributed Environment. In Proceedings of IEEE 60th Vehicular Technology Conference. Los Angeles.
16. Shelby, Z.; Bormann, C. 6lowpan: The Wireless Embedded Internet; John Wiley & Sons: New York, NY, USA, 2011; Volume 43.
17. Shelby, Z.; Hartke, K.; Bormann, C. The Constrained Application Protocol (Coap); RFC 7252; Internet Engineering Task Force: Fremont, CA, USA, 2014
18. Stallings, W. (2005). Cryptography and Network Security Principles and Practices. Upper Saddle River, NJ: Prentice Hall.
19. Thomas, R. K., & Sandhu, R. (2004). Models, Protocols, and Architectures for Secure Pervasive Computing: Challenges and Research Directions. In Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops.
20. Thubert, P. Compression Format for Ipv6 Datagrams over IEEE 802.15.4-Based Networks; RFC 6282; Hui, J., Ed.; Internet Engineering Task Force: Fremont, CA, USA, 2011.
21. Wang, J., Yang, Y., &Yurcik, W. (2005). Secure Smart Environments: Security Requirements, Challenges and Experiences in Pervasive Computing. In Proceedings of NSF Pervasive Computing Infrastructure Experience Workshop
22. Ziegler, M., Mueller, W., Schaefer, R., &Loeser, C. (2005). Secure Profile Management in Smart Home Networks. In Proceedings of the 16th International Workshop on Database and Expert Systems Applications. Copenhagen, Denmark

Corresponding author: **Vineet Kumar Kathuria and Dr.Prerna Pareek**
Submitted: 27 Aug 2020, Revised: 09 Sep 2020, Accepted: 12 Oct 2020, Published; 30 Nov 2020