International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 11 (November 2014), PP.73-83

Security and Privacy Consideration for Internet of Things in Smart Home Environments

Drushti Desai[1], Hardik Upadhyay[2]
[1]*GTU PG School, Research Scholar, Ahmedabad, India.*
[2]*GPERI, Assistant Professor, Ahmedabad, India.*

Abstract:-Internet Of Things(IOT) has emerged as a trustworthy technology to improve the quality of life in smart homes through offering various automated, interactive and comfortable services. Sensors integrated at different places in homes, offices, and even in clothes, equipment, and utilities are used to sense and monitor owners' positions, movements, required signs, valuable usage, temperature and humidity levels of rooms, etc. Along with sensing and monitoring capabilities, sensors cooperate and communicate with themselves to deliver; share and process sensed information and help real-time decision making procedures through activate suitable alerts and actions. However, ensuring privacy and providing enough security in these required services provided by IOTs is a major issue in smart home environments. In this paper, we examine the privacy and security challenges of IOTs and survey its possibilities for smart home environments. We discuss the unique characteristics that differentiate a smart environment from the rest, elaborate on security and privacy issues and their respective solution measures. A number of challenges and interesting research issues appearing from this study have been reported for further analysis.

Keywords:-Internet of Things, smart home, privacy, security, cryptography, Public Key Infrastructure

I. INTRODUCTION

A smart home environment is meant to be a small physical world consisting of a number of devices including sensors, actuators, displays and computational elements interacting and exchanging information with users to provide them with automated, customized, secured and comfortable services. Such environments are designed to help make life better and secure through information processing, automation and by providing personalized services. On the one hand, the potential of smart home environments is huge; for example, smart homes designed for elderly people, capable of sensing, processing and relaying their important health information and communicating the data through numerous integrated devices and their networks to protectors. They can help them live an independent and better life. The need for such automated and digital environments to provide facilities for an improved life style is increasing as the number of elderly people is on the rise. Stegelal.[18] point out that improving the quality of life for disabled and the increasing proportion of elderly people is becoming a more and more essential task for today's European societies, where the percentage of people over 65 years of age is due to rise to 20 percent by the year 2020. One way to improve the quality of life is by making the home environment a more comfortable place to live in by turning it into a smart home environment.

It aims to satisfy the experience of individuals from every environment, by replacing the hazardous work, physical labour, and repetitive tasks with automated agents. This has been made possible with the availability of flexible wearable important signs sensors and location tags that can track people's health status, etc. On the other hand, as more and more personal information is collected and communicated in the wireless network security and privacy issues become more pronounced that must be seriously taken into account in order to exploit the full benefits of smart home environments. Generally, security deals with the cryptographic techniques used to secure communication channels by ensuring message integrity, confidentiality, authenticity; while privacy studies the issues involved in trust and risk associated in the collection, storing, distribution and association of personal data [19].

In a typical smart home environment setting, Internet of Things formed by the integration of these electronic elements are expected to sense, process, and transmit data collected from mixture of different devices, users, and computers connected in the environment with a view to responding with personalized services to users. Sensors may be placed in various locations in offices, apartments and homes to collect users' locations, medical data, e.g., blood pressure, heart rate, and sugar levels, etc., and use them to make appropriate responses based on the information collected. The network is responsible for collecting, distributing and processing vast amounts of private data with other networks, domains or systems (such as the Internet), which will eventually lead to growing concerns of security, privacy and trustworthiness of the network.

Although mainstream research is driven to realize such a dream as envisioned by Marc Weiser [20] of achieving seamless integration of these intelligent sensing and processing elements and their networks into the activities of our life to provide automated and real-time lifesaving support, the equally important issues of handling privacy and security in smart home environments have not been addressed in depth. Security and privacy questions are universal in the wireless network context and unique characteristics of smart environments enable us to identify the ways of how to best solve the problems. Here are some few properties that make smart home environments uniquely different from others:

- **Ubiquity:** The technology or theinfrastructure will be present everywhere affecting most aspects of our life, i.e., the human-computer interaction or the engagement of computational devices and systems is simultaneous and information processing has been thoroughly integrated into everyday objects and activities.
- **Invisibility:** The infrastructure will bephysically invisible to users making them unaware of whether they are using the facility or not. With the ever shrinking size of computing and sensing devices and the widespread use of wireless communications and networks, the existence of the infrastructure of the systems can be made to disappear from view.
- **Sensing:** With the rapid advancement ofmini and multi-purpose digital devices, the functionalities of sensors have been augmented to cover a wide range of activities: monitoring temperature, light, humidity, noise, pressure; measuring blood pressure, sugar levels; sensing the presence of foreign bodies, and so on. Our activities including motions, locations and speeches are sensed by sensors irrespective of our awareness to the system. With sensors embedded in our clothing and our environment, the concept of sensing can go as far as sensing emotional aspects of life, such as stress, fear or excitement, with high accuracy.

The above characteristics define how a smart environment will affect the life of people, their behaviour and interaction, and impact societal change. With its far reaching implications, the smart environment will take this involvement of computer technology and society one step further; where in a populated world of smart and intelligent but invisible Communication and computation devices, no single part of our lives will be free from digitization. Everything we say, do, or even feel, could be digitized, stored, and retrieved at a later date.

II. IOT OVERVIEW AND BACKGROUND

A. What is the Internet of Things?

The Internet of Things (IoT) is a network of globally identifiable physical objects (or things), their integration with the Internet, and their representation in the virtual or digital world. As shown in Fig. 1, the IoTs allow people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service. They are “Material objects connected to material objects in the Internet”. [1]

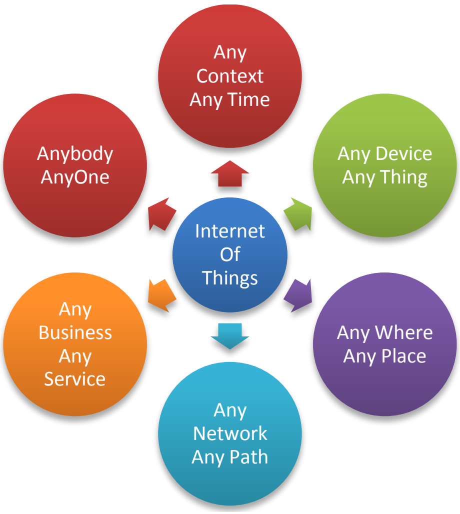

Fig. 1 Definition of Internet of Things

In order to build the IoT, a wide range of technologies are involved. For example, RFID for location and device identification, improved personal and wide area networking protocols, web technologies, etc.

These technologies help to build a virtual world of things on top of the physical world where things through Machine-to-Machine (M2M) communication talk to each other, through humans-to-machine interactions provide information to humans or take actions on human inputs, or act as passive entities to provide data to intelligent entities.

III. SMART HOME CONCEPT

A. What is Smart Home?

There is no general accepted definition of what a **'smart home'** is. The definition of this term varies based on the technology or the functionality the home provides. **'smart home'** can be defined as residences that include telecommunications networks that interconnect essential electrical appliances and services, and enables them to be controlled, monitored, or accessed from a distance. [2]

Today's homes are evolving into a place for e-health, entertainment, communication, work, commerce and learning. They are becoming intelligent living environments that provide their residents with proactive services, such as medical care and monitoring of light, temperature, humidity, heating, and energy consumption. This means homes are becoming smart-agents able to perceive the state of the house and its inhabitants through sensor technology. The aim is to increase the comfort, quality of life, productivity of residents, reduce operating costs, and to encourage occupants to use resources more effectively as well as optimize the energy consumption in order to become an environmentally friendly society. Home automation is the use of one or more computers to control basic home functions and features automatically and sometimes remotely. An automated home is sometimes called as Smart Home. Figure 3.Shows the sample of Smart Home System.

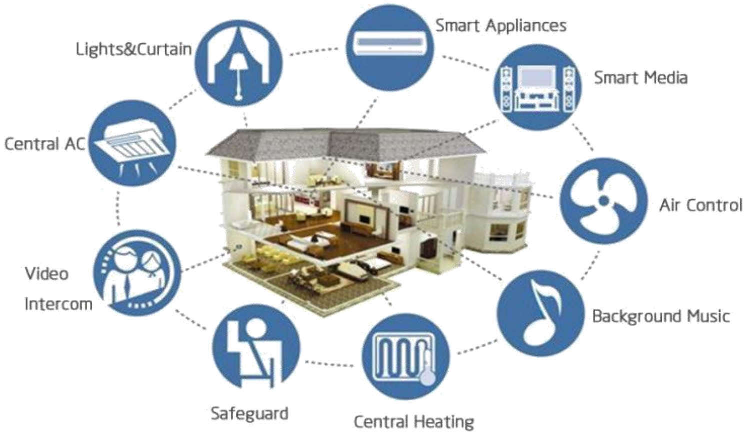

Fig.3. IoT Smart Home.

B. Applications of Internet Of Things

The IoT can find its applications in almost every aspect of our daily life. Below are some of the examples.

- **Industry applications:** The IoT canfindapplications in industry e.g., managing a fleet of cars for an organization. The IoT helps to monitor their environmental performance and process the data to determine and pick the one that need maintenance.
- **Design of smart homes:** The IoT can helpin the design of smart homes e.g., energy consumption management, interaction with appliances, detecting emergencies, home safety and finding things easily, home security etc.
- **Medical applications:** The IoT can alsofind applications in medical sector for saving lives or improving the quality of life e.g., monitoring health parameters, monitoring activities, support for independent living, monitoring medicines intake etc.
- **Agriculture application:** A network ofdifferent sensors can sense data, perform data processing and inform the farmer through communication infrastructure e.g., mobile phone text message about the portion of land that need particular attention. This may include smart packaging of seeds, fertilizer and pest control mechanisms that respond to specific local conditions and indicate actions.
- **Intelligent transport system design:** TheIntelligent transportation system will provide efficient transportation control and management using advanced technology of sensors, information and network. The intelligent transportation can have many interesting features such as non-stop electronic highway toll, mobile emergency command and scheduling, transportation law enforcement, vehicle rules violation monitoring, reducing environmental pollution, anti-theft system, avoiding traffic jams, reporting traffic incidents, smart beaconing, minimizing arrival delays etc
- **Design of smart cities:** The IoT can help to design smart cities e.g., monitoring air quality, discovering

emergency routes, efficient lighting up of the city, watering gardens etc.

- **Smart Security:** The IoT can also find applications in the field of security and surveillance e.g., surveillance of spaces, tracking of people and assets, infrastructure and equipment maintenance, alarming etc.

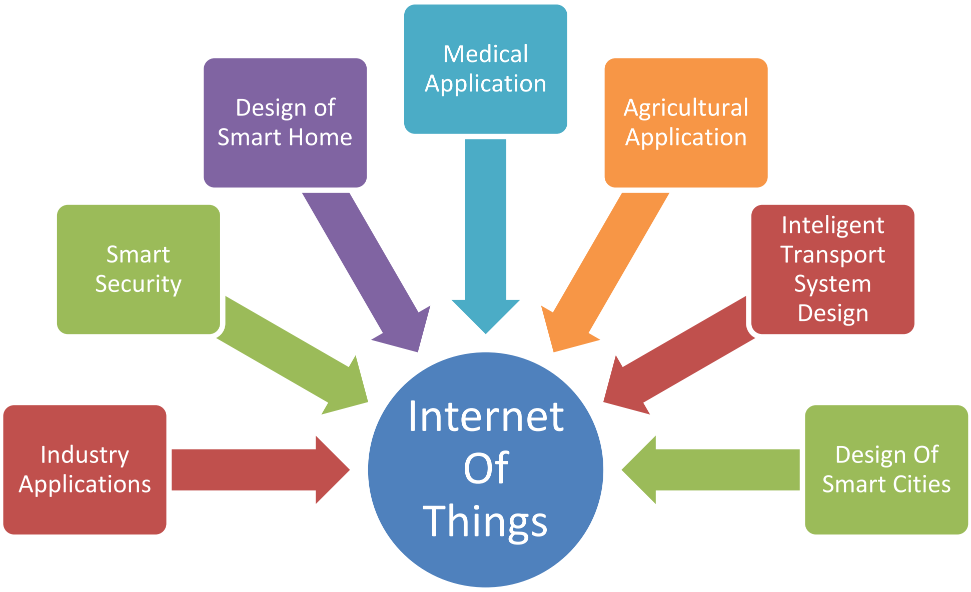

Fig. 4. Applications of IOT.

C. Pros and Cons of the Internet of Things

The Pros of IoT

1. **Information:** In my opinion, it is obviousthat having more information helps making better decisions. Whether it is mundane decisions as needing to know what to buy at the grocery store or if your company has enough widgets and supplies, knowledge is power and more knowledge is better.

2. **Monitor:** The second most obviousadvantage of IoT is monitoring. Knowing the exact quantity of supplies or the air quality in your home, can further provide more information that could not have previously been collected easily. For instance, knowing that you are low on milk or printer ink could save you another trip to the store in the near future. Furthermore, monitoring the expiration of products can and will improve safety.

3. **Time:** As hinted in the previous examples,the amount of time saved because of IoT could be quite large. And in today’s modern life, we all could use more time.

4. **Money:** In my opinion, the biggestadvantage of IoT is saving money. If the price of the tagging and monitoring equipment is less than the amount of money saved, then the Internet of Things will be very widely adopted.

The Cons of IoT

1. **Compatibility:** Currently, there is nointernational standard of compatibility for the tagging and monitoring equipment. I believe this disadvantage is the most easy to overcome. The manufacturing companies of this equipment just need to agree to a standard, such as Bluetooth, USB, etc. This is nothing new or innovative needed.
2. **Complexity:** As with all complex systems,there are more opportunities of failure. With the Internet of Things, failures could sky rocket. For instance, let’s say that both you and your spouse each get a message saying that your milk has expired, and both of you stop at a store on your way home, and you both purchase milk. As a result, you and your spouse have purchased twice the amount that you both need. Or maybe a bug in the software ends up automatically ordering a new ink cartridge for your printer each and every hour for a few days, or at least after each power failure, when you only need a single replacement.
3. **Privacy/Security:** With all of this IoT databeing transmitted, the risk of losing privacy increases. For instance, how well encrypted will the data be kept and transmitted with? Do you want your neighbours or employers to know what medications that you are taking or your financial situation?
4. **Safety:** Imagine if a notorious hackerchanges your prescription. Or if a store automatically ships you an equivalent product that you are allergic to, or a flavour that you do not like, or a product that is already expired. As a result, safety is ultimately in the hands of the consumer to verify any and all automation.

IV. PRIVACY IN SMART HOME ENVIRONMENTS

Privacy is a generic term whose great scope spans different cultures, generations, time for which there is no universally accepted definition - "no definition ... is possible, because [those] issues are fundamentally matters of values, interests, and power" [3]. In dealing with the formal understanding of privacy, Samuel Warren and Louis Brandeis wrote the influential paper "The Right to Privacy" [4] motivated mainly by the origin of modem photography and the printing press. In order to give a concise and clear idea of privacy, Brandeis defined privacy as "the right to be let alone". Although this encapsulates the essence of privacy, the sphere of privacy has been extended over time to include the protection of one's private domain, one's bodily private sphere (e.g., body temperature, behaviour etc.), privileged conversations with family members, lawyer priest, etc. the undisturbed development and exercise of one's life style and so on.

Most people today think of it more as "the right to select what personal information about me is known to what people" as mentioned in [5]. In summary, privacy focuses on protecting users' personal information, whether it be the person'sidentity, locations, movements or any information related to him/her that the person is afraid to share with others. With considerable amounts of private information being collected, transmitted and analysed by the IOT, it is no surprise that privacy concerns are critical in smart home environments. Where numerous devices and networks are constantly interacting through sharing and distributing information protecting privacy will be a tremendous challenge.

Typically, there are two kinds of private information, namely data-oriented and context-oriented that is required to be protected or preserved. In the category of data-oriented privacy, one is interested in finding techniques that would enable aggregation and transmission of the sensed data i.e. private data associated with individuals by the IOT without violating the privacy of the data.

Potential applications in the smart environment feature that need of data privacy. For example, wireless sensors may be positioned in critical places in homes, government agencies, buildings, and factories to record or measure the amounts of electricity, water and other utilities or resource usage and report them to the centre, possibly via other networks. Also, sensor readings could reveal whether there are any people, or any number of people present, their identification, the daily activities of a household, their current activities, and movements, etc. On the other hand, through in-home floor sensors, information regarding weight coupled with additional data such as whether the person is doing exercise, sitting, etc. could also be collected. Wearable sensors that take readings about important health may be ofinterest to health-care providers, and/or insurance companies to help them make timely and important decisions. Such data is certainly confidential and deserve privacy.

On the other hand, context-privacy deals with protecting mechanisms regarding location and timing, i.e., keeping secret from unwanted exposure the location and timing of the data generation of users' information. Data is often encrypted which is difficult to break and know the content. Instead of directly dealing with encrypted data, adversaries armed with knowledge of network deployment, routing patterns, algorithms and the base location can make use of the context, i.e., the surrounding environments and timing of data generation to infer about the events for which the network is deployed. This type of privacy is important especially in the moving target tracing applications of IOTs, since an adversary withtiming information and the locations of sensors generating the data packets may be able to figure out the nature and the location of the target. Required context-oriented privacy also extends to other concerns, such as the hiding of time frequency of communication between sensor nodes in IOT , because such frequency may expose information about the traffic flow in IOT.

A. Data-oriented Privacy

Data-privacy can be violated by external and internal adversaries. In an external type of attack, the adversary who is not an authorized network participant eavesdrops or listens to the data communication between sensor nodes. General measures that effectively defend against this kind of attack are cryptographic encryption and authentication. An internal adversary is a node in the network which is captured and reprogrammed by malicious entities to compromise private information. This type of attack is stronger than an external attack because traditional encryption and authentication is unable to detect it since the node is legally allowed to encrypt and decrypt messages. The main challenge for protecting data-oriented privacy is to protect data from internal adversaries.

A straight-forward approach to defend against internal adversaries is to apply end-to-end encryption between the data source and the base station. With this approach, no intermediate node, including the internal adversaries, can compromise the privacy of data being transmitted without knowing the key shared by only the two end nodes. Although it seems to be a robust defence, it may not be feasible for IOTs because a lot of extra communication overhead, incurred during the communication as intermediate nodes is not allowed to aggregate the data. One way to overcome this impediment is to use hop-by-hop encryption where each pair of neighbours shares a private key to enforce encryption and decryption.

B. Context-oriented Privacy

Context-oriented privacy protection deals with mechanisms for protecting contextual information such as the location and timing of traffic data transmitted in IOT. Location privacy has been gaining a lot of attention because of the continued development of advanced wireless devices, like PDA, GPS and with the advent of location-based services. In such a system, a user holding a wireless device queries the server to obtain the nearest restaurant or hospital to him/her. What happens in this case is that there exists a centralized trusted third party which collects the requests from users with wireless devices. Then this trusted third party, hiding the real locations of the users, sends approximate location information combined with the other users' information to the server to learn the nearest service provider's location. Privacy is achieved as the server is unable to distinguish the particular user's location because of the way information is provided to it. However, if the trusted third-party is compromised, complications may arise and privacy may be violated. The requirement of a third party can be removed with the addition of significant computation and communication overhead. Such a technique has been proposed in.

Timing privacy concerns the time when sensitive information is sensed, processed and transmitted to the base station [6]. Time plays a vital role in many applications such as tracking a person's movement, where an adversary with knowledge of the timing could possibly figure out the location of the person. Also, communication traffic can fall into timing privacy because identifying frequent communication at some particular period of time between a person's sensor sensing the heart rate or blood pressure and its neighbours may indicate the person is having health problem, which is definitely a violation of privacy.

As mentioned above, an adversary can derive vital information observing the traffic pattern between sensors generating data and the base station. One way to protect the network, in particular the locations of such data sources, is to hide the real traffic. In order to do so the simplest approach is to insert some fake packets into the network to produce different routing paths that may confuse the adversary in their effort to track or learn about the original traffic pattern. There are four existing techniques to achieve this: flooding, random walk, dummy injection, and fake data sources against the disclosure of the data source.

V. SMART HOME ENVIRONMENT SECURITY ISSUES

A. Requirement for Security for the Smart Home Environment

People living in the smart home environment are increasingly relying on information from wireless networks that are monitoring, collecting and analysing important data about themselves, their vital signs, locations, motions, appliance and utility usage, and sending them to caregivers or other authenticated agencies for decision making.

Such private and sensitive data generated by the IOT and the interactions between various intelligent devices and sensors are communicated to the outside world via other existing network technologies, and possibly the Interment for further processing, analysis and database storage. The integration of such a wide range of devices, networks and different technologies, together with the Internet, leaves no room for neglecting state-of-the art security issues, architectures, protection and defence mechanisms in IOTs. Moreover, the sensing devices are deployed or positioned in accessible areas increasing security vulnerabilities. The dynamic nature of sensor networks i.e. node and link failures combined with consideration of prioritizing critical data, location and context awareness, and coordination of heterogeneous devices and sensors add to the security challenges. The traditional security threats, attacks and defence mechanisms that exist for wired and other computer and communications networks and even for the Internet also equally apply for wireless networks.

In order to provide complete security to IOTs, security must be integrated into every node of the system otherwise an insecure component in the network could be a point of attack and can make the whole system vulnerable. That is why security must succeed in every aspect of the design of IOT application that will require a high level of security. It is obvious that without any protective mechanism, the network could suffer from attacks or malfunctions that disrupt the services provided by the network [7]. Care should be exercised in identifying possible threats and attacks such as eavesdropping, injection and/or modification of data packets that can lead to unwanted situations and cause disruption in the network and applying the standard methods of protection against them.

B. Security Goals

The security objectives of electronic information are determined based on the kinds of threats and vulnerabilities that can be inflicted upon it. While vulnerability deals with the opportunity to cause damage because of a logical design or implementation flaw, a threat arises from an attacker trying to find and exploit the vulnerability in order to inflict damage. When dealing with security in IOTs, the following are some essential security requirements that are often the measures to compare the performance of various secured systems:

- **Confidentiality:**

It refers to preventing disclosure of information to unauthorized persons, parties or systems. Confidentiality secures the network by preventing unauthorized parties from accessing the data generated, e.g., domain specific information, such as the user identity, positions and other related information transmitted in the network. In other words, an eavesdropper should not be able to extract the content of a confidential message [8].

- **Integrity:**

It refers to preventing falsification, modification of data transmitted in the network by unauthorized persons or systems. More specifically in the automation system, this applies to information such as sensor values, or control commands. This objective includes defence against information modification via message injection, message replay, and message delay on the network. Violation of integrity may interfere with safety issues, i.e., modified or false data can malfunction and damage control systems and facilities such as communications and security systems, lighting, heating and hydro systems. [8]

- **Freshness:**

It could mean data freshness and key freshness. It is concerned with whether the data produced or measured in the system is recent and ensures no adversary generated old messages. This is very important in the context of the smart home environment since sensors often sense and transmit time-critical data such as someone's blood-pressure and heart-rates at certain times which bear more significance than other times and should be handled in real-time for ensuring the safety of lives.

- **Availability:**

It refers to ensuring that unauthorized persons or systems cannot deny access system resources to authorized users. For automation systems, this refers to all the IT elements of the home environment including control, safety, utility and entertainment systems as well as the communication systems between these elements and to the outside world. Simply, it means that the availability of services ensures that only authorized entities can access data, services and other available resources when requested. Violation of availability, also known as denial-of-service (DoS), may not only cause economic damages but may also affect safety issues and jeopardize the life of individuals since there might be situations (e.g., heart attacks, respiratory malfunctions of individuals) when urgent and timely actions are crucial. [8]

- **Authenticity:**

It is related to confining the true identity of a system user or entity and mapping of this identity to a system-internal principal (e.g., valid user account) by which this user is known to the system. In other words, authentication distinguishes between legitimate and illegitimate users in a system [8].

C. ATTRIBUTES OF ATTACKS AND COUNTERMEASURES IN IOT

Although the security objectives mentioned earlier are generic in the sense that they can be applied to both wired and wireless solutions, the wireless nature of the communication between sensors and devices makes these objectives more vulnerable, as there is no apparent physical boundary of the transmission medium [9]. However, based on a specific need and function, the smart home can select the possible security objectives that need to be ensured. Among the attacks that can be mounted on such wireless systems, we have briefly elaborated on a few of them. In the following, we discuss potential attacks and their general defence mechanisms, which is in fact applicable in any WSN application whether it be home and environment monitoring, medical and health, military battle-field, and so on.

Attacks are mainly categorized by two types - outside and inside attacks. In an outside attack, an outsider adversary or attacker is not a participant of the network while an inside attack consists of attacking nodes by running malicious code in them [9].

1. Eavesdropping:

Eavesdropping is an outside attack where an adversary can choose to passively eavesdrop on the network communication and steal the data. Through passive eavesdropping adversaries apparently eliminate their presence in the network and make such attacks difficult to detect. The goal of such an attack is to violate the confidentiality of the communications by intercepting the network and sniffing or listening to the routing packets.

In some cases, instead of completely being passive an eavesdropper can use advanced techniques to send queries to see what is going on in the network or try to determine the content of the packets in order to gain more information [10]. Moreover, an adversary can actively influence the communication channel by disrupting, jamming or modifying the network packets and/or insertingfalse packets into the network. Jamming happens at the physical layer which may cause interference at different frequencies in an intermittent or constant manner that can make communication impossible.

Observations & Avoidances:

Using a sufficiently strong encryption and decryption technique one can obtain sound Protection against eavesdropping. Proper authentication and integrity mechanisms can ward off such active eavesdropping. On the other hand, a standard defence against jamming includes various forms of spread-spectrum (e.g., direct sequence spread-spectrum and frequency-hopping spread spectrum) and frequency-hopping communications and maintaining a low-duty cycle, locating a jamming area, and rerouting transmissions.

2. Denial of Service:

WSNs can suffer from the Denial of Service(DoS) attacks [11] which occur when attackers use PC or laptops to transmit signals in order to interfere with the radio frequencies being used by the network. This kind of DoS can also be visible at the data link layer where, in order to disrupt the communication protocols whether they are industry standards such as IEEE 802.15.4 or ZigBee, attacks are committed by transmitting a continuous stream of messages with a view to generating collisions. These collisions lead sensors to retransmit messages indefinitely and render them inoperative by exhausting battery power. As a result, the sensors consume their valuable computational resources, such as bandwidth and processor time. Other problems include disruption of configuration information, such as routing information, and obstruction of the communication media between the intended users so that they can no longer communicate adequately.

Observations & Avoidances:

A probabilistic measure to counter collisions is to rely on random back-offs which decrease the rate of collisions. As reported in, one of the most promising solutions for reducing collisions is rate limiting in MAC and using small frame sizes. Some researchers proposed several mechanisms that identify such malfunctioned and misbehaving nodes based on the rating of how well they are performing services as requested and help routing protocols avoid them. Virtual currency systems use currency to pay nodes (payment is made by
the sender) who forward the messages of sender nodes. The advantage of this method is that it discourages nodes from flooding packets in the systems.

3. Node Compromise:

Node compromise is one of the major problems **in** IOTs that lead to inside attacks. It is a kind of act by which a legitimate node in the network is captured and compromised, that is, reprogrammed by an adversary. In situations where it is not feasible for an adversary to physically capture and reprogram nodes in the network, he can use a laptop, which is more powerful in terms of computing and radio power to communicate with sensors and insert malicious code without moving to their locations or physically touching them. With this, a compromised node running malicious code disguised as a legitimate node continuously seeks to find ways to disrupt communication and paralyze the network. However, node compromise attack is severe when the base node is compromised.

The malicious activities commonly done by a compromised node include: stealing secrets from the encrypted data, reporting wrong and misleading information to the network, reporting other legitimate nodes as compromised nodes, launching different routing attacks. All these attacks are very difficult to detect and encryption methods have little effect on countering them. This is because these compromised nodes still hold at least some legitimate secret cryptographic keys used in the network..

Observations & Avoidances:

The best way to counter node compromise is to utilize code testing schemes whichemploy an optimal program verification process to verify the memory of a sensor node by calculating the hash values of randomly selected memory regions. Another method suggested in detects node compromise by comparing the previous position of nodes with their current positions, assuming that node compromise must be done by physically capturing a node, reprogramming and then redeploying it in the network.

4. Sinkhole and Wormhole Attacks:

A Sinkhole Attack [12] is a type of attack where a malicious node attracts network packets towards it by spreading false routing information to its neighbours in order to make selective forwarding of packets which, in turn, reshapes the network's routing behaviour. The adversary lures traffic by advertising the existence of a high quality routing path to its neighbours. To do this, a laptop with a powerful antenna can be used to send a strong signal to reach the base station possibly in one hop. As nodes are lured to send their packets through the malicious node, it can suppress or modify packets as it wishes. Since packets are destined for the base station, a compromised node just has to convince its neighbours with a high quality routing path to the base.

In a Wormhole Attack [12], an attacker receives packets at one point in the network, funnels them to another point in the network, and then replays them into the network from that point creating confusion in routing, aggregation and other important decisions made by the nodes. In this attack, an adversary acts as a forwarding node between two legitimate nodes which may be far away and gives them the impression that they are neighbours, leading them to quickly dissipate their valuable energy.

Observations & Avoidances:

One possible solution to overcome Wormhole and Sinkhole attacks is to have every node use a unique symmetric shared key with the base. Wormhole and Sinkhole attacks are more stringent than the Sybil attack (and selective forwarding) and finding a strong countermeasure for them is difficult. Designing good routing protocols such as multi-path routing can be helpful to minimize the effect of such attacks.

5. Physical Attack:

Last but not the least type of attack is the physical attack of the node itself. It deals with the ability of the attacker to gain physical access to sensors. This physical access opens up a number of attacks including destroying or stealing the nodes, removing them from their original locations, inserting malicious code and retrieving secret information such as cryptographic keys. Tamper proof hardware is sometimes seen as a viable option to protect the sensors, but this is expensive and may not be very effective against an attacker.

D. CRYPTOGRAPHIC TECHNIQUES

Cryptographic methods are the key to ensuring **most** of the security objectives such as confidentiality, integrity, authentication, and non-reputability. Cryptographic algorithms are employed for secure data storage and secure transmission. For secure data transmissionsecurity measures need to be incorporated in each participating node in the network. For comprehensive overviews of cryptographic algorithms and protocols, see [13] and [14]. This section provides a brief review of some existing cryptographic algorithms used in wireless networking systems. Cryptography is the basic encryption method used in security implementation in data and information communication. There are two types of cryptographic methods, namely, symmetric and asymmetric. Symmetric encryption algorithms are characterized by the fact that the decryption key is identical to the encryption key or the keys can be transformed to one another via simple functions.

Asymmetric or public key cryptography on the other hand, uses different keys to encrypt and decrypt messages. Asymmetric key cryptographic approaches such as RSA, and Elliptic Curve Cryptography (ECC), require more computation power and memory than the symmetric key cryptographic approaches like AES block cipher, DES, and RC4 [15]. Symmetric key cryptography is difficult for key deployment and management. However, in the context of WSNs, symmetric key cryptography seems to be the best choice because sensors cannot afford to dedicate their limited energy to implement complex and resource-oriented public key cryptography.

In symmetric key cryptography, the key must be exchanged in advance between the sender and receiver in a secure manner and must be kept secret. Considering security, key management is very important especially in the symmetric cryptography structure and is the basis for establishing secure communications between sensors. However, sensor network dynamic structure, easy node compromise, and the self-organization property add to the difficulty of key management and bring about broad research issues in this area. Most symmetric schemes use key pre-distribution to ease the difficulty of key management. There is a plethora of literature discussing the relative merits and demerits of different key management schemes in the wireless network.

Symmetric-key algorithms can be divided into stream ciphers and block ciphers. Stream ciphers combine input data bit-or byte-wise with a key stream, while block ciphers transform input data block-wise in a key-dependent way. There exist a wide range of symmetric algorithms with different characteristics. Some examples of popular and well respectedsymmetric algorithms include RC4, DES, and AES. RC4 is a popular stream cipher with byte-wise processing [15] that can be easily implemented on weak processors such as 8- bit processors. DES is a block cipher defined as U.S. standard for encryption in 1977 [16], however, it is not very stable and is breakable due to the relatively short key length (56 bits). A later version of DES was developed, called the triple DES to make the scheme stronger with the introduction of a longer key (three times the size of the DES key). The Advanced Encryption Standard (AES) is the current U.S. standard for encryption [17] which is at least as secure as Triple DES. It has gained popularity in sensor networks because it is much faster, consumes less resource and is suitable for different processor word lengths. AES comes with 128-bit blocks and its key size is 128, 192, or 256 bit. Today, a key size of 128 bit is considered strong enough.

On top of these general security and solution measures, we need to consider other issues which are unique to smart environments, such as users being able to freely move in environments wearing sensors and be considered as roaming entities. They can leave any given smart environment and appear in any unknown domain, and along with that there can be mobile devices, such as robots, in a smart environment. Such mobility can cause several problems. First, tracking malicious users or devices becomes more difficult because a legal roaming node at one place may be working as a good node and then can be compromised and reprogrammed somewhere in its trajectory by a malicious user and can act maliciously. Second, security concerns arise, both for the security of wireless networks against attack from roaming devices and the security of the roaming devices against a wireless network capable of malicious behaviour.

VI. RESEARCH CHALLENGES

Ensuring adequate security in IOTs is an ongoing challenge due to the sensors' severe resource constraints and their demanding deployment environments based on applications. The unique properties of IOTs present a number of important trades-offs in terms of the sensor's energy consumption and maintaining sufficient security measures. We need to analyse and determine the exact security requirements of the home environment considering its distinctive characteristics, which are different from the environments and security needs of a military battle-field, manufacturing shop floors, shopping centres or malls. At the basic level, considering the physical security of the networks and their components, some research efforts should be driven to figure out protective measures to make the nodes tamper proof without much overhead.

Another important issue is to consider the robustness and resilience of IOTs which are concerned with the strength of the network to provide an acceptable level of security if some nodes are compromised and the ability of the network to operate despite attacks. Efficient mechanisms should be sought to quickly determine whether certain nodes are compromised and if so, they should be identified and taken care of without seriously affecting the normal functioning of the network. Secure routing protocols, in general, provide little or no security features and are susceptible to many types of attacks that target routing disruption. Existing secure routing protocols in traditional networks can be investigated to see whether they can fit to WSNs. Care should be taken to prevent adversaries from knowing about the topology of the network. Adopting multi-path routing only when the regular routing path is corrupted by the presence of compromised nodes is a good way to circumvent malicious nodes, otherwise frequent and unnecessary dependence on multi-path routing can affect the energy consumption of the sensors.

The privacy issue in IOTs is wider than mere data protection since it encompasses the protection of a private sphere including bodily characteristics such as body temperature, behaviour, privileged conversations, positional gestures and other important and sensitive data of an individual. These features must be taken into account in order to develop strong privacy protection mechanisms. Encryption keys used to protect such personal data need to be sufficiently strong but computationally feasible enough to be used by sensors limited by their computation power. There are also other avenues of research concerning issues for the rectification of incorrect data, enabling checking the accuracy of private data, unauthorized copying and destruction data that are no longer needed etc.

VII. CONCLUSION

In this paper, we made an attempt to provide a survey on the issues of privacy and security of IOTs in smart home environments. We have discussed several security problems and privacy issues that are present in IOTs considering the smart home's conditions including process management, workflow, interference, appliance placement and movement. A number of existing standard solutions have been studied along with their mechanisms to deal with various attacks and threats. Although the existing security paradigms as outlined by the standards (for example, ZigBee) seem to be sufficient to counter against major attacks, they leave the design and implementation details to the users. Also there are still interesting problems left for future investigation, specially to handle privacy issues and other legal considerations regarding personal data. On the other hand, traditional complex cryptographic algorithms (e.g., public key cryptography) that seem effective to handle most security issues may not be suitable for sensors because of their lesser power and processing capabilities. Thus, future research in this direction would be to develop new protocols which will be able to effectively solve most of the security and privacy problems.

REFERENCES

[1]. J. S. Kumar, “A Survey on Internet of Things: Security and Privacy Issues,” International Journal of Computer Applications, vol. 90, pp. 1-7, 2014.

[2]. A. J. M., “Privacy in the context of Smart Home Environments,” 2014.

[3]. R. Gellman, “Does privacy law work? In Agre and Rotenberg,” pp. Chapter-7 pp.193-218.

[4]. S. W. a. L. Brandeis, “The right to privacy, Harvard Law,” pp. vol. 4, pp. 193-220.

[5]. A. F. Westin, “Privacy and Freedom, Atheneum”.

[6]. W. X. W. T. P. Kamat, “Temporal privacy in wireless sensor network,” InternationalConference on Distributed Computing Systems, p. 23, 2007.

[7]. R. H. S. M. J. Deng, “Countermeasures against traffic analysis,” in Proc. of Securityand Privacy for Emerging Areas in Communications Networks, 2005, pp. 113-126.

[8]. S. V. N. K. a. J. S. Khaleel Ahmad1, “Classification of Internet,” NationalConference, 2011.

[9]. P. M. a. M. H. D. Christin, “Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives,” NationalConference, 2010.

[10]. E. C. M. S. M. B. Z. I. a. I. L. M. Anand, “Sensor Network Security: More Interesting Than You Think,” USENIX HotSec, 2007.

[11]. L. Z. GAN Gang, “Internet of Things Security Analysis”.

[12]. T. N. E. L. M. Healy, “Security for wireless sensor networks: A survey,” SAS IEEESensors Applications Symposium, 2009.

[13]. W. Mao, “Modem Cryptography: Theory and Practice”.

[14]. B. Schneier, Applied Cryptography, 1996.

[15]. R. Rivest, “The RC4 encryption algorithm (proprietary),” RSA Data Security Inc., 1992.

[16]. Data Encryption Standard, 1997.

[17]. Specification of the Advanced Encryption Standard (AES), 2001