International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 32-43 | Cosmos Impact Factor (Germany): 5.195
Received: 01.02.2018 Published : 07.02.2018

PRIVACY OF USER DATA AND SECURITY RISKS IN IOT

Sunanda Dixit
Associate Professor, Information Science and Engineering Department, Dayananda Sagar college of Engineering, Bangalore, India, e-mail: sunanda.bms@gmail.com
Shwetha
UG Scholar, Department of Information Science and Engineering, Dayananda Sagar college of Engineering, Bangalore, India, e-mail: shwetha.sd08@gmail.com
Mahesh B V
Tata Consultancy Services, United Kingdom, India, e-mail: mahesh_ait@hotmail.com

Abstract

As IoT is melding physical world with the virtual world, today billions of devices are connected to internet and to each other thus allowing consumers remotely control and sense the objects , resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. But IoT also has disadvantages where consumers privacy, security, safety are compromised. Data brokers are collecting users personal information through internet without their knowledge and selling it to interested parties. This paper focuses on privacy of user data and some existing privacy enhancing technologies and gives a overview of security risks in IoT.

Keywords: IoT, privacy, personal data, privacy enhancing technologies.

1. Introduction :

IOT is not a new concept, in the early 2000's, Kevin Ashton did the groundwork for what would become the Internet of Things (IOT) at MIT's Auto ID Lab. Ashton was one of the pioneers who conceived this notion as he searched for ways that Proctor & Gamble Co could improve its business by linking RFID (Radio Frequency Identification) information to the Internet. If all objects in daily life were equipped with identifiers , sensors and wireless connectivity, these objects could be communicate with each other and be managed by computers. In a 1999 article for the RFID Journal Kevin Ashton wrote: "If we had computers that knew everything there was to know about things -- using data they gathered without any help from us -- we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory RFID and sensor technology enable computers to observe , identify and understand the world -- without the limitations of human entered data[1]" . This vision required major technology improvements , one at a time. How the internetworking of the things on the planet can be achieved was a big question in 1999. Today all the obstacles are solved. The size and cost of sensor devices are reduced tremendously. IPv6 allows us to assign communications address to billions of devices. Electronics companies are building Wi-Fi and cellular wireless connectivity into a wide range of devices. Cisco's Internet of Things Group (IOTG) predicts there will be over 50 billion connected devices by 2020.

Definition: The Internet of things (IoT) is the inter-networking of physical devices,vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. Applications of IoT

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 26-31 | Cosmos Impact Factor (Germany): 5.195
Received: 01.02.2018 Published : 07.02.2018

include - Media, Environmental monitoring, Infrastructure management, Manufacturing, Energy management, Medical and healthcare, Building and homeautomation, Transportation Metropolitan scale deployments, Consumer application[2].

Advantages of IoT:-

- Data:The more the information, the easier it is to make the right decision. Knowing what to get from the grocery while you are out, without having to check on your own, not only saves time but is convenient as well.
- Tracking:The computers keep a track both on the quality and the viability of things at home. Knowing the expiration date of products before one consumes them improves safety and quality of life. Also, you will never run out of anything when you need it at the last moment.
- Time:internetworking of things reduces the amount of time spent in monitoring the things and number of trips done to a great extent.
- Money:The financial aspect is the best advantage. This technology could replace humans who are in charge of monitoring and maintaining supplies.

Disadvantages of IoT:

- Compatibility:As of now, there is no standard for tagging and monitoring with sensors. A uniform concept like the USB or Bluetooth is required which should not be that difficult to do.
- Complexity:There are several opportunities for failure with complex systems. For example, both you and your spouse may receive messages that the milk is over and both of you may end up buying the same. That leaves you with double the quantity required. Or there is a software bug causing the printer to order ink multiple times when it requires a single cartridge.
- Privacy/security: Privacy is a big issue with IoT. Internet Service providers may take users personal information and make use of it for profiling and then targeting users for selling stuffs. data security is also a big problem.
- Safety: There is a chance that the software can be hacked and users personal information misused. Users prescription being changed or account details being hacked could put them at risk. Hence, all the safety risks become the consumer's responsibility[3].

As privacy and security are big concerns in iot rest of the paper concentrates on it.

2. Privacy:

Human beings value their privacy and the protection of their personal sphere of life. They value some control over who knows what about them. In recent years there have been numerous incidents where personal data has been stolen, lost or subject to unauthorised access.They certainly do not want their personal information to be accessible to just anyone at any time. But recent advances in information technology threaten privacy and have reduced the amount of control over personal data and open up the possibility of a range of negative consequences as a result of access to personal data. The 21st century has become the century of Big Data and advanced Information Technology allows for the storage and processing of exabytes of data. There are companies out there that collect users information,they're called data brokers and they have names like Spokeo, Whitepages.com, PeopleFinder, as well as plenty of others. They collect data from everything we do online and then sell that data to interested parties, mostly in order to more specifically advertise to user and sell more stuff. user could search for herself on these sites and then deal with each site individually to get her name removed. Problem is, the procedure for opting out from each site is different and sometimes involves sending faxes and filling out actual physical paperwork. First, companies should build security into their devices at the outset, rather than as an afterthought. As part of the security by design process, companies should consider[4]:

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 26-31 | Cosmos Impact Factor (Germany): 5.195
Received: 01.02.2018 Published : 07.02.2018

- conducting a privacy or security risk assessment.
- minimizing the data they collect and retain.
- testing their security measures before launching their products.

3. Personal Data:

Personal information or data is information or data that is linked or can be linked to individual persons. Examples include date of birth, sexual preference, whereabouts, religion, but also the IP address of your computer or metadata pertaining to these kinds of information. Personal data can be contrasted with data that is considered sensitive, valuable or important for other reasons, such as secret recipes, financial data, or military intelligence.

Moral reasons for protecting personal data[5]:

The following types of moral reasons for the protection of personal data and for providing direct or indirect control over access to those data by others can be distinguished (van den Hoven 2008):

- Prevention of harm: Unrestricted access by others to one's passwords, characteristics, and whereabouts can be used to harm the data subject in a variety of ways.
- Informational inequality: Personal data have become commodities. Individuals are usually not in a good position to negotiate contracts about the use of their data and do not have the means to check whether partners live up to the terms of the contract.
- Informational injustice and discrimination: Personal information provided in one sphere or context (for example, health care) may change its meaning when used in another sphere or context (such as commercial transactions) and may lead to discrimination and disadvantages for the individual.
- Encroachment on moral autonomy: Lack of privacy may expose individuals to outside forces that influence their choices.

4. Privacy Enhancing Technologies:

More than a decade ago, the Dutch and Ontario Data Protection Authorities recognised the role of technology in protecting privacy and coined the term Privacy Enhancing Technologies (PET). Today, European Data Protection Authorities routinely refer to PET as an approach to help achieve compliance with data protection legislation[6].

Definition: "Privacy-enhancing technologies are protocols, standards and tools that directly assist in protecting privacy, minimizing the collection of personally identifiable information, and when possible, eliminating the collection of personally identifiable information".

PETs aim at allowing users to take one or more of the following actions related to their personal data sent to, and used by, online service providers, merchants or other users:

- increase control over their personal data sent to, and used by, online service providers and merchants (or other online users).
- data minimisation : minimise the personal data collected and used by service providers.
- degree of anonymity : choose the degree of anonymity by pseudonyms, anonymisers or anonymous data credentials.
- degree of linkability : choose the amount of linkability by using multiple virtual identities.
- achieve informed consent about giving their personal data to online service providers and merchants

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 26-31 | Cosmos Impact Factor (Germany): 5.195
Received: 01.02.2018 Published : 07.02.2018

- provide the possibility to negotiate the terms and conditions of giving their personal data to online service providers and merchant.
- provide the possibility to have these negotiated terms and conditions technically enforced by the infrastructures of online service providers and merchants.
- provide the possibility to remotely audit the enforcement of these terms and conditions at the online service providers and merchants (assurance)
- data tracking: allow users to log, archive and look up past transfers of their personal data, including what data has been transferred, when, to whom and under what conditions facilitate the use of their legal rights of data inspection, correction and deletion.

Some of the PETs are:

4.1 EPID :

Enhanced Privacy ID (EPID) is a cryptographic scheme that enables the remote authentication of a hardware device while preserving the privacy of the device. EPID can be viewed as a direct anonymous attestation scheme with enhanced revocation capabilities. In EPID, a device can be revoked if the private key embedded in the hardware device has been extracted and published widely so that the revocation manager finds the corrupted private key. In addition, the revocation manager can revoke a device based on the signatures the device has signed, if the private key of the device is not known.

Why EPID :

Consider the problem: a hardware device (e.g., a graphics chip, a trusted platform module, a mobile device, or a processor) wants to authenticate to a service provider that it is a genuine hardware device , so that the service provider can send a protected resource (e.g., high definition media) to the device. One possible solution is that the hardware manufacturer assigns each device a unique device certificate. The device can authenticate to the service provider by showing the device certificate. However, such solution raises a privacy concern as the device certificate can uniquely identify the device. Brickell, Camenisch, and Chen introduced a cryptographic scheme called Direct Anonymous Attestation (DAA) that can solve the above problem. In a DAA scheme, a hardware device can be revoked only if the private key embedded in the hardware device has been extracted and published widely so that the revocation manager finds the corrupted private key. However, if an attacker corrupts a hardware device and obtains the device's private key, but he never publishes it, then there is no way to revoke the key in DAA. If the named base option in DAA is used, it can allow revocation based on signatures for all uses of the same named base, but it has the unfortunate property of removing the anonymity for all uses with the same named base. To get around the problem of the limited revocation properties of DAA, Brickell and Li introduced the notion of Enhanced Privacy ID (EPID).

In an EPID scheme, there are four types of entities: an issuer, a revocation manager, platforms, and verifiers. The issuer could be the same entity as the revocation manager. The issuer is in charge of issuing membership to platforms, i.e., each platform obtains a unique private key from the issuer through a join process. A platform can prove membership to a verifier by signing a signature using its private key. The verifier can verify membership of the platform by verifying the signature, but he cannot learn the identity of the platform.

One important feature of EPID is that nobody besides the platform knows the platform's private key and nobody can trace the signatures created by the platform. Yet an EPID scheme has to be able to revoke a platform if the platform's private key has been corrupted. There are two types of revocations in EPID:

- private-key based revocation in which the revocation manager revokes a platform based on the platform's private key

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 26-31 | Cosmos Impact Factor (Germany): 5.195
Received: 01.02.2018 Published : 07.02.2018

- signature based revocation in which the revocation manager revokes a platform based on the signatures created by the platform[7].

4.2 Anonymyzers :

An anonymyzer is a tool that attempts to make activity on the internet untraceable. It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. Anonymyzer sites access the internet on our behalf, protecting our personal information from disclosure. it protects all of our computer's identifying information while it surfs for us.
Two basic types of Internet anonymizers

- Single point design
- Networked design

Single point anonymyzers :

This type of anonymizer passes our surfing through a single website to protect our identity, and often offers an encrypted communications channel for passing passage of results back to the user. Single-point anonymizers offer less resistance to sophisticated traffic analysis. But they pose simplicity, organizational familiarity, and apparent trustworthiness. Many single-point anonymizers create an anonymized URL by appending the name of the site user wish to access to their URL.

With single-point anonymizers, our IP address and related identifying information are protected by the arms-length communications and not transferred to the sites we visit. If we are using a secure channel to the anonymizer, then our communications to the anonymizer site are also confidential to any local eavesdroppers tapping our Internet line connection.

Networked anonymyzers :

This type of anonymizer transfers our communications through a network of computers between us and the destination. For example, a request to visit a web page might first go through computers A, B, and C before going to the website, with the resulting page transferred back through C, B, and A then to us. Example of networked anoymyzers are- zero knowledge systems , EFF's TOR(currently existing).

The main advantage of the networked anonymizer design is that it makes traffic analysis (a vulnerability of single-point anonymizers) much more difficult. For example, analysis of the incoming and outgoing traffic of a single-point anonymizer could note that communications with our machine, even though the contents are encrypted, are closely synchronized in time with the anonymizer site's unencrypted communications with some particular website. If ten times in a row our communication with the anonymizer is followed milliseconds later by a request from the anonymizer to a particular site, and that site's response to the anonymizer is followed milliseconds later by an encrypted communication to us, then it is clear that we made a visit to that site.

Techniques that anonymizers can use to reduce the risk of traffic analysis include:

- adding small but random delays to the passage of responses back to the user to make time matching more difficult.
- making random requests to random pages across the web to pollute the pool.
- having a large number of simultaneous users to make analysis more difficult.
- have a large cache of web pages so that not all incoming requests have outgoing requests.

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 26-31 | Cosmos Impact Factor (Germany): 5.195
Received: 01.02.2018 Published : 07.02.2018

Advantages : compilation of communication by passing our communications through a preferably random path of other computers. An eavesdropper would have to put in place the equipment and programs to watch all of the computers in the anonymizer's Internet network and then solve a much more complex analysis.

Disadvantages : at each computer in the anonymizer chain there is a risk that it has already been compromised by the owner or an intruder and the communications can be tapped.

Limitations of anonymyzers :

- HTTPs : Anonymizers cannot process secure protocols like "https:" since our browser needs to directly access the site to maintain the secure encryption.
- Plugins : If we access a site with an anonymizer that invokes a third-party plugin, then there is a possibility of direct connections from our computer to the remote site that are not anonymized.
- Logs : All anonymizer sites claim that they don't keep a log of our requests. Some Anonymizer, keep a log of the addresses accessed .
- Java : Any Java applications that we access through an anonymizer will not be able to bypass the Java security wall and access our name, email adress, or file system.
- Active X: Presumably safe, authorized Active X applications are certified with a certificate number. Active-X applications have almost unlimited access to our computer system, and once downloaded by a website they bypass the anonymizer completely. They can access and reveal our name and email address, and can access our file system to perform file creations, reads, and deletions[8].

4.3 Encryption :

Encryption is a mathematical function using a secret key which encodes data so that only users with access to that key can read the information.Encrypting data whilst it is being transferred from one device to another (eg across the internet or over a wireless connection) provides effective protection against interception of the communication by a third party whilst the data is in transfer.
There are two types of encryption in use today : symmetric and assymmetric encryption.

- Symmetric encryption:In symmetric encryption the same key is used for encryption and decryption. It is therefore required that a secure method is considered to transfer the key between sender and recipient.

- assymetric encryption:Asymmetric encryption uses the notion of a key pair: different keys are used for the encryption and decryption processes. One of the keys is known as the private key and the other is known as the public key.The private key is kept secret by the user and the public key is either shared amongst authorised recipients or made available to the public at large.Data encrypted with the public key and transmitted can only be decrypted with the corresponding private key. Data can therefore be transferred without the risk of unauthorised access[9].

4.4 Anonymous credentials :

A credential is a means to establish a claimed identity, roles, or attributes about oneself with an entity, typically as part of an access control request. So for instance an identity card can serve as a credential to establish that one is between 12 and 15 years old as might be required to access a teenage chat. Using a traditional identity card, this would also reveal to the chat side all the other information on the card. Anonymous credentials overcome this: with such credential a user can selectively reveal any of the attributes contained in the credential without revealing any of their personal information whatsoever. Thus, anonymous credentials are a key ingredient to protect one's privacy in an electronic world. Tools are existing to generate anonymous credentials for example- IBM's Identity mixer Idemix. With identity mixer, users can obtain from an issuer a credential containing all the information the issuer is ready to attest about them. When a user later wants to prove to a service provider a statement about her,

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 26-31 | Cosmos Impact Factor (Germany): 5.195
Received: 01.02.2018 Published : 07.02.2018

she employs identity mixer to securely transform the issued credential. The transformed credential will only contain the subset of the attested information that she is willing to disclose[10].

4.5 Limited disclosure technology:

It is designed to protect individuals' privacy by allowing them to share only enough personal information with service providers to complete an interaction or transaction. The technology is also designed to limit tracking and correlation of users' interactions with the third parties. Limited disclosure uses cryptographic techniques and allows users to retrieve data that is evaluated by a provider, to transmit that data to a relying party, and have these relying parties trust the authenticity and integrity of the data[11].

4.6 Shared online accounts:

One person creates an account for a site , providing bogus data for name, address, phone number, preferences, life situation etc. They then publish their user-ID and password on the Internet. Everybody can now use this account comfortably. Thereby the user is sure that there is no personal data about him in the account profile. Moreover, he is freed from the problem of having to register at the site himself giving his personal email ID, which the sites may further use for sending lots of advertisements which causes irritation to the user.

5. Access to the personal data :

The service provider's infrastructure should allow users to inspect, correct or delete all their data stored at the service provider. Policies should be made that Data brokers must notify user before collecting their data and they should also allow the user to remove his data from their database whenever he wants. User can delete his personal information captured and stored in any site by deleting his account for example, social network accounts (eg,face book), online shopping accounts (eg,amazon account).

6. Privacy policy:

As the Internet of Things becomes more widespread, consumers must demand better security and privacy protections that don't leave them vulnerable to corporate surveillance and data breaches. But before consumers can demand change, they must be informed — which requires companies to be more transparent. The most dangerous part of IoT is that consumers are surrendering their privacy, bit by bit, without realizing it, because they are unaware of what data is being collected and how it is being used.
Most people do not read privacy policies for every device they buy or every app they download, and even if they attempted to do so, most would be written in legal language unintelligible to the average consumer. Those same devices also typically come with similarly unintelligible terms of use, which include mandatory arbitration clauses forcing them to give up their right to be heard in court if they are harmed by the product. As a result, the privacy of consumers can be compromised, and they are left without any real remedy.Increased corporate transparency is desperately needed, and will be the foundation of any successful solution to increased privacy in the IoT. This transparency could be accomplished either by industry self-regulation or governmental regulation requiring companies to receive informed and meaningful consent from consumers before collecting data. Layered privacy policies should be a best practice adopted by many industries, and Creative Commons licenses could serve as useful models. Those licenses have a three-layer design: the "legal code" layer, the "human-readable" layer and the "machine-readable" layer.The "legal code" layer would be the actual policy, written by lawyers and interpreted by judges. The "human-readable" layer would be a concise and simplified summary of the privacy policy in plain language that an average consumer could read. The "machine-readable" layer would be the code that software, search engines and other kinds of technology can understand, and would only allow the technology to have access to information permitted by the consumer[12].

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 26-31 | Cosmos Impact Factor (Germany): 5.195
Received: 01.02.2018 Published : 07.02.2018

6.1 Privacy policy in India:

Currently, India's most comprehensive legal provisions that speak to privacy on the internet can be found in the Information Technology Act (ITA) 2000. The ITA contains a number of provisions that can, in some cases, safeguard online privacy, or in other cases, dilute online privacy. Provisions that clearly protect user privacy include: penalizing child pornography, penalizing, hacking and fraud and defining data protection standards for body corporate. Provisions that serve to dilute user privacy speak to access by law enforcement to user's personal information stored by body corporate collection and monitoring of internet traffic data and real time monitoring, interception, and decryption of online communication.

Future frameworks for privacy in India:

The report of group of experts on privacy – In October 2012 the Report of the Group of Experts on Privacy was published by a committee of experts chaired by Justice A.P. Shah. The report creates a set of recommendations for a privacy framework and legislation in India.+++ Most importantly, the Report recognizes privacy as a fundamental right and defines nine National Privacy Principles that would apply to all data controllers both in the private sector and the public sector. This would work to ensure that businesses and governments are held accountable to protecting privacy and that legislation and practices found across sectors, states/governments, organizations, and governmental bodies are harmonized. The privacy principles are in line with global standards including the EU, OECD, and APEC principles on privacy, and include: notice, choice & consent, collection limitation, purpose limitation, access and correction, accountability, openness, disclosure of information, security[13].

7. Security Concerns:

Internet of things interconnects billions of devices and benifits us to a greater extent .However, against a wider backdrop of increasing cyber fraud and online crime, our growing reliance on interconnected devices is raising serious concerns about security. The gateways that connect IoT devices to company and manufacturer networks need to be secured as well as the devices themselves. IoT devices are always connected and always on. In contrast to human-controlled devices, they go through a one-time authentication process, which can make them perfect sources of infiltration into company networks. Therefore, more security needs to be implemented on these gateways to improve the overall security of the system[14]. Also of concern are huge repositories where IoT data is being stored, which can become attractive targets for corporate hackers and industrial spies who rely on big data to make profits. In the wake of massive data breaches and data theft cases we've seen in recent years, more effort needs to be made to secure IoT-related data to ensure the privacy of consumers and the functionality of businesses and corporations. The security requirements of Internet of Things(IoT) system are complex,they include-confidentiality,integrity,availability,authentication,authorization,nonrepudiation,freshness of data and backward secracy.Based on these requirements security attacks can be broadly categorized as physical, network, software or encryption attacks[15].

7.1 Physical Attacks

Physical attacks target the hardware of an IoT system and include breaches at the sensor layer. They typically require physical proximity to the system but can also involve actions that limit the efficacy of IoT hardware. Attackers can tamper with nodes to gain control over sensor nodes or devices in an IoT environment and use that control to extract materials, data and code. With malicious node injection, attackers can physically deploy malicious nodes between legitimate nodes in an IoT network. Also known as a man-in-the-middle (MitM) attack, the malicious nodes can then control operations and the data flowing between linked nodes.This enables the malicious actor to monitor, eavesdrop on and control communications between the two legitimate nodes.Attackers might target the routing protocol in IoT networks to alter the traffic flow through a compromised node, reconfigure the network topology, create routing loops, generate false errors or modify source routes. In a Sybil attack, for

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 26-31 | Cosmos Impact Factor (Germany): 5.195
Received: 01.02.2018 Published : 07.02.2018

example, fraudsters create fake node identities or mimic legitimate ones. These are then used to generate false and malicious information to compromise an IoT system. Injecting malicious code enables attackers to access IoT systems, for example by plugging a USB key into a device on the network. An attacker can compromise a node by physically injecting it with malicious code that would grant access to the IoT system.Attackers can physically damage IoT devices to disrupt the availability of service. Also at risk are areas controlled by IoT systems or facilities that host them, such as data centers. Cybercriminals could also conduct distributed denial-of-service (DDoS) attacks through signal interference on radio-frequency identification (RFID) systems and radio frequency interference on wireless sensor networks.Using social engineering, attackers can control users of an IoT system to serve their own ends. They can also launch sleep deprivation attacks, which target the vulnerability of battery drainage in devices and sensors in an IoT system. Most devices have a sleep mode to extend battery life, but sleep deprivation attacks maximize the power consumption of nodes to ultimately shut them down.

7.2 Network Attacks

Network attacks target the IoT system network layer and can be conducted remotely. DDoS attacks are perhaps the most widely known network IoT security risk. Typically, they involve overflowing network devices with more requests than they can handle, thus preventing the server from answering legitimate requests. Using sniffing applications, attackers can perform traffic analysis to infer information based on communication patterns between devices in an IoT network. Even encrypted information can be deduced from this data without decryption.

7.3 Software Attacks

The biggest IoT security risks involve software. Software attacks can exploit entire systems, steal information, alter data, deny service and compromise or damage devices.In a phishing attack, for example, fraudsters gain access by impersonating a legitimate entity to trick users into providing access or credentials. Attackers also use malware, such as viruses, worms and Trojans, to damage or delete data, steal information, monitor users and disrupt key system functions. Attackers can also target software at the application layer to execute DDoS attacks. In addition to shutting down access to legitimate users, application layer attacks expose databases and sensitive data.

7.4 Encryption Attacks

IoT security risks also include attacks that target encryption schemes. Instead of targeting the cryptographic algorithms themselves, side-channel attacks target the implementation of those algorithms.Attackers can infer the encryption key by analyzing physical measurements during computation and the internal state of the physical device during processing. Cryptanalysis attacks attempt to deduce encryption keys by searching for weaknesses in the cryptographic algorithm. Depending on the information available to the attacker, cryptanalysis attacks can take following forms: ciphertext-only, chosen-plaintext, adaptive-chosen-plaintext, chosen-ciphertext and adaptive-chosen-ciphertext. Encryption schemes are also vulnerable to MitM attacks in which a malicious actor intercepts communication between two users and decrypts data using keys shared with both of them. As in other MitM attacks, users continue assume they are communicating only with each other.

8. Denial of Service Attack(DoS):

Denial of Service attack is an attack on network availability.This attack is the process of preventing the accessibility of information to legitimate users by unknown third party intruders[16]. This can take place on different layers of a network:-

1) DoS attack on the physical layer:

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 26-31 | Cosmos Impact Factor (Germany): 5.195
Received: 01.02.2018 Published : 07.02.2018

The physical layer of a wireless sensor network carries out the function of selection and generation of carrier frequency, modulation and demodulation,encryption and decryption, transmission and reception of data. This layer of the wireless sensor network is attacked mainly through-

A)Jamming: In this type of DoS attack occupies the communication channel between the nodes thus preventing them from communicating with each other.
B)Node tampering: Physical tampering of the node to extract sensitive information is known as node tampering.

2) DoS attack on the link layer:

The link layer of WSN multiplexes the various data streams, provides detection of data frame, MAC and error control. Moreover the link layer ensures point-point or point-multipoint reliability [17].

The DoS attacks taking place in this layer are:

A) Collision: This type of DoS attack can be initiated when two nodes simultaneously transmit packets of data on the same frequency channel. The collision of data packets results in small changes in the packet results in identification of the packet as a mismatch at the receiving end. This leads to discard of the affected data packet for re-transmission [18].

B) Unfairness: As described in [18], unfairness is a repeated collision based attack. It can also be referred to as exhaustion based attacks.

C) Battery Exhaustion: This type of DoS attack causes unusually high traffic in a channel making its accessibility very limited to the nodes. Such a disruption in the channel is caused by a large number of requests (Request To Send) and transmissions over the channel.

3) DoS attack on the network layer :

The main function of the network layer of wireless sensor network is routing. The specific DoS attacks taking place in this layer are:

A) Spoofing, replaying and misdirection of traffic.
B) Selective forwarding: As the name suggests, in a selective forwarding, a compromised node only sends a selected few nodes instead of all the nodes. This selection of the nodes is done on the basis of the requirement of the attacker to achieve his malicious objective and thus such nodes does not forward packets of data.
C) Sybil: In a Sybil attack, the attacker replicates a single node and presents it with multiple identities to the other nodes.
D) Wormhole: This DoS attack causes relocation of bits of data from its original position in the network.This relocation of data packet is carried out through tunnelling of bits of data over a link of low latency.
E) Acknowledgement flooding: Acknowledgements are required at times in sensor networks when routing algorithms are used. In this DoS attack, a malicious node spoofs the Acknowledgements providing false information to the destined neighboring nodes[16].
4) DoS attack on the transport layer :
This layer of the WSN architecture provides reliability of data transmission and avoids congestion resulting from high traffic in the routers. The DoS attacks in this layer are:
A)Flooding: It refers to deliberate congestion of communication channels through relay of unnecessary messages and high traffic.
B)De-synchronization: In de-synchronization attack, fake messages are created at one or both endpoints requesting retransmissions for correction of non-existent error. This results in loss of energy in one or both the end-points in carrying out the spoofed instructions.

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 26-31 | Cosmos Impact Factor (Germany): 5.195
Received: 01.02.2018 Published : 07.02.2018

5)DoS attack on the application layer:
The application layer of WSN carries out the responsibility of traffic management. It also acts as the provider of software for different applications which carries out the translation of data into a comprehensible form or helps in collection of information by sending queries [17]. In this layer, a path-based DoS attack is initiated by stimulating the sensor nodes to create a huge traffic in the route towards the base station [18].

9. Security risks in RFID Technology:

In context to IoT, RFID technology is mainly used as RFID tags for automated exchange of information without any manual involvement. But the RFID tags are prone to various attacks from outside due to the flawed security status of the RFID technology. The four most common types of attacks and security issues of RFID tags [16] are shown in Figure 3 which are as follows:

A) Unauthorized tag disabling (Attack on authenticity):The DoS attacks in the RFID technology leads to incapacitation of the RFID tags temporarily or permanently. Such attacks render a RFID tag to malfunction and misbehave under the scan of a tag reader, its EPC giving misinformation against the unique numerical combination identity assigned to it. These DoS attacks can be done remotely, allowing the attacker to manipulate the tag behavior from a distance.

B) Unauthorized tag cloning (Attack on integrity): The capturing of the identification information (like its EPC) esp. through the manipulation of the tags by rogue readers falls under this category. Once the identification information of a tag is compromised, replication of the tag (cloning) is made possible which can be used to bypass counterfeit security measures as well as introducing new vulnerabilities in any industry using RFID tags automatic verification steps.

C) Unauthorized tag tracking (Attack on confidentiality): A tag can be traced through rogue readers, which may result in giving up of sensitive information like a person's address.Thus from a consumer's viewpoint, buying a product having an RFID tag guarantees them no confidentiality regarding the purchase of their chase and infact endangers their privacy.

D) Replay attacks (Attack on availability): In this type of impersonation attacks the attacker uses a tag's response to a rogue reader's challenge to impersonate the tag. In replay attacks, the communicating signal between the reader and the tag is intercepted, recorded and replayed upon the receipt of any query from the reader at a later time, thus faking the availability of the tag.

10. Conclusion :

The IoT presents numerous benefits to consumers, and has the potential to change the ways that consumers interact with technology in fundamental ways. In the future, the Internet of Things is likely to meld the virtual and physical worlds together. From a security and privacy perspective,it poses many difficulties to consumers. Users personal data will be collected and used without their control over it. Even though there are many privacy enhancing technologies, data protection laws ,privacy policies existing ,users personal data are still at risk. Its better if organizations, companies and internet service providers itself take measures to protect users personal data and to minimize the amount of the personal data collection. At the same time users also should be careful while providing their information online, as it may cause misuse of the data by selling it to third parties. Government should enforce laws so that data brokers stop steeling users personal data. There are a lot of security risks affecting devices and thereby users in IoT, but no strong solution that can effectively mitigate the threats, so large amount of research and focus is very much required to overcome these risks.

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 26-31 | Cosmos Impact Factor (Germany): 5.195
Received: 01.02.2018 Published : 07.02.2018

References :

[1] Lopez research "An introduction to the internet of things".
[2] "internet of things"- iwww.wikipedia.com/iot
[3]Prateek saxena- Jun 15,2016 - "The Advantages and Disadvantages of Internet of Things"- https://e27.co/advantages-disadvantages-internet-things-20160615/
[4] https://www.ftc.gov/system/files/documents/...staff...privacy/150127iotrpt.pdf
[5] " Privacy and Information Technology"- Nov 20,2014 - https://plato.stanford.edu/entries/it-privacy/#PerDat
[6]Steve Kenny- "An Introduction to Privacy Enhancing Technologies"- May 1,2008-https://iapp.org/news/a/2008-05-introduction-to-privacy-enhancing-technologies/
[7] Ernie Brickell and Jiangtao Li -Feb 25,2009- "Enhanced Privacy ID from Bilinear Pairing"- http://eprint.iacr.org/2009/095
[8] Lance Cottrell - "Internet Anonymizers"- http://www.livinginternet.com/i/is_anon.htm
[9] https://ico.org.uk/for-organisations/guide-to-dataprotection/encryption/
[10]Identity Mixer - https://idemix.wordpress.com/
[11]Gartner IT Glossary - "Limited Disclosure Technology"- http://www.gartner.com/it-glossary/limited-disclosure-technology/
[12]Christine Bannan - Aug 14,2016 - "The IoT Threat to Privacy" - www.techcrunch.com
[13]The Centre for Internet and Society -"Internet Privacy in india"- http://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india
[14]Ben Dickson - Oct 24 , 2015 - "Why IoT Security is so critical" - https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical.
[15]Tristan O'Gorman - Feb 8,2017 - "A Primer on IoT Security Risks" - www.secu
A Primer on IoT Security Risks , February 8, 2017 - By Tristan O'Gorman - www.securityintelligence.com
[16]Tuhin Borgohain, Uday Kumar, Sugata Sanyal - "Survey of Security and Privacy Issues of Internet of Things"- pageno:2-4. https://arxiv.org/ftp/arxiv/papers/1501/1501.02211.pdf
[17]Ahmad Abed Alhameed Alkhatib, and Gurvinder Singh Baicher. "Wireless sensor network architecture."International conference on computer networks and communication systems (CNCS 2012) IPCSIT. Vol. 35. 2012, pp. 11-15.
[18]Sunil Ghildiyal, Amit Kumar Mishra, Ashish Gupta, Neha Garg- "Analysis of Denial of Service (DoS) Attacks in Wireless Sensor Networks" IJRET: International Journal of Research in Engineering and Technology;eISSN: 2319-1163 | pISSN: 2321-7308.