Internet Of Things: Review On Security Of Novel Technology

Akshat Grover[1], B.M.Sahoo[2]
Amity School of Engineering and Technology,
Amity University, Uttar Pradesh
Noida – India

Abstract- The IOT hues a premonition of a world where all gadgets are between associated and unendingly keep on sharing our most viable data with each other. This data, thus empowers these items to convey indemonstrated usefulness and proficiency to its clients, by extraordinarily altering the gadgets in light of their prerequisites. How-ever, there are grave dangers associated with this sort of a world where the gadgets interminably share clients information among each other. With this exponential ascent in the generation and us-period of IoT gadgets, one of the greatest worry that this tech fixated society faces is security. With more of our family unit apparatuses and things being associated with the web, these offices makes these gadgets defenseless against assaults. Ordinary items equipped for interfacing with the web are coming into the market and with them, they bring considerably higher security concerns. Web of Things which is increasing more footing each day will soon be synonymous with human presence, however its limits are not yet settled nor is it secure[13]. There win plenitude of security challenges with the present models and the advancements which make the foundation of the Internet of Things. Security ruptures won't just influence organizations yet buyers too and in this manner the difficulties are monstrous. The paper centers around directing an efficient writing survey to discover security challenges looked in IoT and to give a prospective security structure to alleviate the possibly dangerous relationship with IoT.

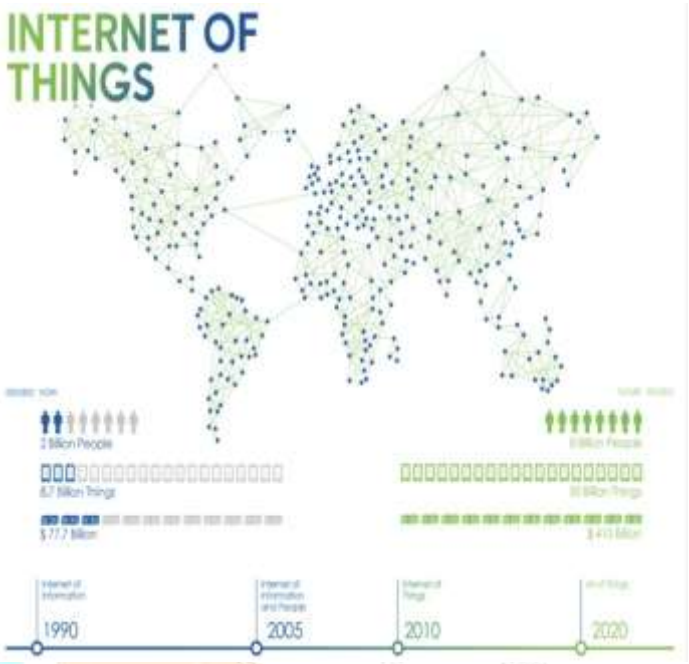
Keywords *- Internet of things (IoT), networks, security, devices/hardware, challenges, attacks*

I. INTRODUCTION

The Internet of Things signifies that each and every device in the world will have a unique digital identity in the form of a digital address (like an IP) of some kind. Using this digital identity the devices would connect and communicate to each other. It seems like every day some company announces some new IoT enabled product. And with it some prediction of where the market is going. Some of the IoT applications are: smart homes, wearable, smart city, smart grid, industrial inter-net, connected cars, connected health, smart retail, smart supply chain, smart farming and a lot more. IoT is developing for very nearly 10 years now, where different physical items would be interconnected by the utilisation of different existing innovations, such as sensors and Wireless technologies like GSM, UMTS, Wi-Fi, Bluetooth and ZigBee, etc. Although IoT brings with it a lot of benefits which will make human life a lot more easier and efficient but like every coin has two sides IoT also bring with it a lot of security vulnerabilities.

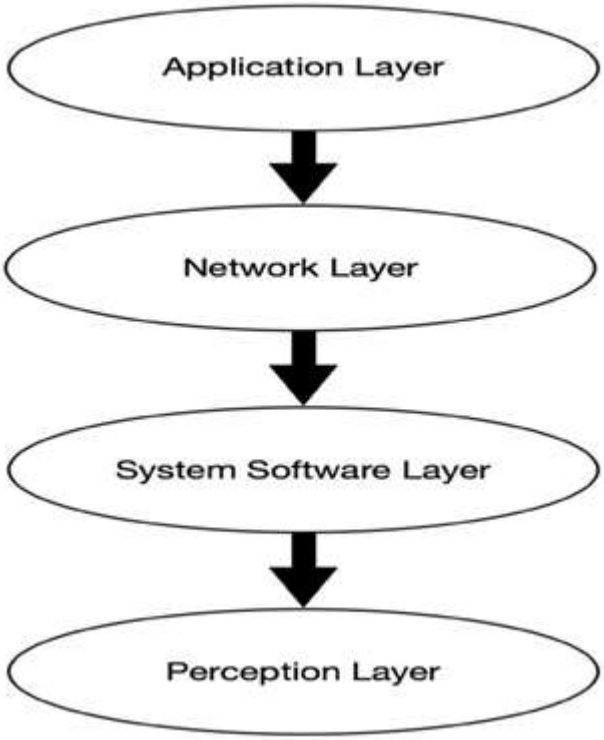
The onslaught of the Internet of Things raises questions. Are IT professionals aware of all the connected devices in their organisations? Should consumers feel confident that their in-formation is safe on their IoT devices? Are new security stan-dards needed? The objective of this research is to present a literature review of existing IoT reference architecture with a comparative study of their corresponding security concerns and solutions while proposing a security framework so as to mitigate the dangers. This, as a result should yield a strong foundation for researchers who intend to understand the archi-tecture of IoT devices and their security protocols.

IoT lacks a well defined architecture which makes it vulnera-ble. It is impossible to condense over two decades of security evolution into modern IoT devices and there exists no magic potion that can potentially alleviate threats. Small size restric-tions and insubstantial processing capabilities of many inter-connected devices could impede encryption and other power-ful security measures. IoT chips won't be very profitable since they are very small in size and typically based on outdated architectures so there is no incentive for the manufacturers to add in extensive security features. Leading cell phone compa-nies don't upgrade their software on 2-3 year old phones, so the state of substantially cheaper IoT devices that may stay on your network for years can be imagined.



Generic Architecture:-

1. **Perception Layer:** The Perceptual layer is the most basic layer also known as recognition layer, collecting informa-tion and identifying the physical world through various types of information sensors like RFID, Barcodes, Wi-Fi, ZigBee or whatever other sensor system . This layer often forms a root of trust in modern computing systems.



Layers of Architecture

2. **System Software Layer:** The system software layer con-sists of firm ware, operating system code, and any privi-leged system applications or programming frameworks. This layer builds on hardware mechanisms for establishing trust and isolation.

3. **Network Layer:** The network layer is also known as wire-less sensor networks, which are responsible for the trans-mission of information, initial processing of information, classification and polymerisation through existing corre-spondence systems like Internet, Mobile Network or what-ever other dependable system.
4. **Application Layer:** The application layer in IoT is no dif-ferent from other computing paradigms it runs customised code for end-user scenarios. The application layer provides services for all industries and is handy in taking into ac-count the requirements of clients, for example, Smart Home, Smart Environment, Smart Transportation and Smart Hospital and so on.

II. LITERATURE REVIEW

The documentation presented in this paper was obtained from different search engines and online databases including Google, Scopus, Arxiv, Yahoo and Google Scholar. Keywords and idioms were identified before hand and used for the search in concomitance with each other and independently to identify all related papers as well as tech-articles. The publications which were printed in english language including papers fea-turing in prominent journals, books and reports were scruti-nised to distinguish those that met a criteria of presenting in-formation accredited to the purpose of this review.

- A new proposal from the IEEE, published in the current "Proceedings of the IEEE" journal, suggests a model which combines the capabilities of IoT enabled devices with a con-trol system gateways using real-time response to potential threats[15]. Both terminal and edge devices would utilise a mixture of signal/image processing, biometric, digital signa-tures, cryptography. These devices would also have com-munication capabilities for validation of functions. The new model proposed is considered to be more potent against po-tential threats while having the ability to scale to a large network and since it comes with real-time performance it is resilient as well as compared to traditional IT security solu-tions.

- IEEE members and Intel executives have come up with the proposal, which will create an additional level of security beyond initial machine authentication. Being referred to as Real-Time Identity Monitoring can monitor the behaviours of connection for a specific client device and it can also re-peatedly request extra validation of information.

- Increasingly, control systems are becoming networked, and controlling access to the devices becomes existential. A 2013 study by Trend Micro found that the highest number of attempts to hack the device against a control system con-stantly monitored were classified as unauthorised entrance.

- **Security controls:** Security controls have evolved over the years from first packet-filtering firewalls to more complex application-aware firewalls, intrusion detection and preven-tion systems and security incident and event management (SIEM) solutions. These controls prevented and detected any malicious activity on corporate networks. If malware managed to breach a firewall, certain antivirus techniques based on signature matching and blacklisting would prevent the any further breach. The blacklisting techniques got re-placed by whitelisting techniques as the malware advanced to the extent where current techniques were not sufficient to control security[2,13]. As more devices were added to the corporate networks, various access control systems were developed to authenticate both devices and users. The con-cerns over data privacy gave rise to controls such as virtual private networks (VPN) or physical media encryption, such as 802.11i (WPA2) or 802.1AE (MACsec).

- **Object identification and location in IoT:** Distinguishing an object is the first key security issue that needs to be ad-dressed[9]. An explicit identification function is the anchor of securing IoT infrastructure. For example Domain Name System has the responsibility to identify a host on the inter-net uniquely. Due to huge success of DNS, a new system was proposed by the name of Object name Service (ONS)by EPC global board . The task of this function was identify the position of services and metadata affiliated with an issued Electronic Product Code. A structure built on the same lines could be proposed that will be applicable to identifying an
- object in IoT. Few systems have been proposed such as Named data Networking (NDN), they combine name and address where routing of a packet is based directly on object names.

- **API management-key to Internet of things:** API manage-ment is like an umbrella which encompasses a collection of solutions such as gateways, security and access management. Developing patches for IoT devices may not be as easy or even possible, to update. What makes IoT so impor-tant is its ability to connect applications to devices. There-fore, API management is essential for an IoT device to func-tion, grant the developers who enable the connecting of things to APIs the authority and at the same time, retaining the right to revoke that access[11]. As said by the data man-agement firm, Axway, API's provide a control point which can be monitored to create an audit trail and where controls can be enforced according to the requirements.

- **Identity management:** For most internet services, especial-ly the free ones, there is no confirmed identity of a user. For example, one internet service provider, enables individuals to use their Facebook account as identity for signing-in for the various services provided. There is a glaring threat visi-ble to us here which is that the user's account can easily be compromised if a hacker somehow obtains the credentials of a user's account. If this account is connected to user's home security system, he could come to his or her house that has been vandalised. For identity management, Public Key In-frastructure is used to set up trusted connections between the device and provider for patches, software upgrades and in-formation exchange.

Security Challenges in Internet of Things:-

1. **Unsanctioned Intercession Between Communicating Parties**[1]: This challenge refers to a situation where in an unauthorised party maybe causing interference between two legal entities engaged in a communication.
2. **Eavesdropping Attack:** This security challenge refers to a situation where an entity with a malicious intent may gather information without causing interference.

3. **Trust Management**[1,10]: Trust management provides behaviour based analysis of entities, using their past be-haviour, reputation in the network or recommendation. A trustworthy system is needed to prevent from unwanted activities conducted by malicious devices. The implemen-tation of effective Trust Management is a challenge

4. **Physical Attack on Non-Volatile Memories**[5,7]: Protect-ing non volatile memory from physical attack by hackers is a big concern especially in IoT since they are made at ex-tensively low cost.

5. **Availability, Integrity and Confidentiality of Data**[12]: Maintaining confidentiality, integrity and availability is a huge challenge from security point of view as it involves extensive secure framework.

6. **Identification Of Various Devices:** With 50 billion IoT devices said to be in circulation within next two years giv-ing unique identity to every IoT enabled device will be a challenge[10].

7. **Controlling Access**[1]: With ubiquitous connectivity present today and plethora of IoT devices giving access to number of devices and controlling them without failing the device is a big challenge.

8. **Insurance of Security and Requirements of Privacy in Disparate Abode:** When an IoT device will be in your network for a long amount of time it is only logical to have some sort of insurance to protect your data[10].

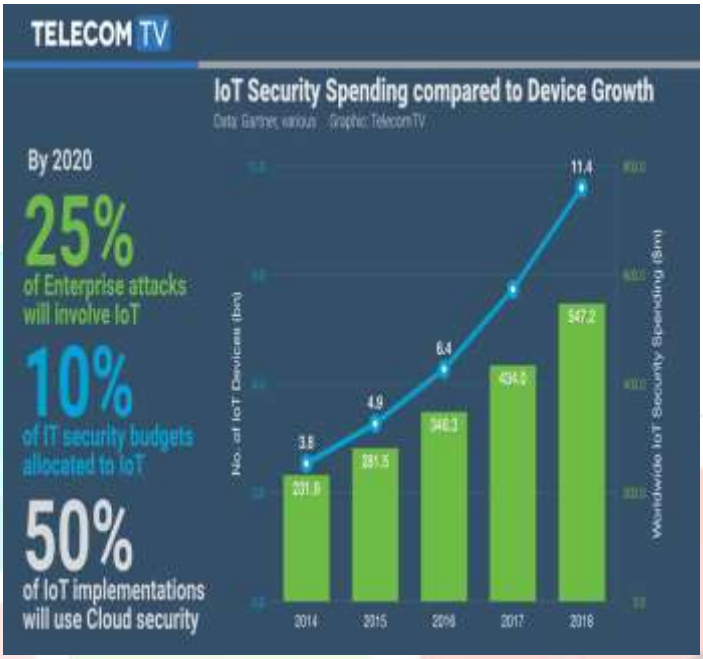
9. **Storage and Transmission of Crucial Data**[12]: Not only securing software and hardware is important in IoT archi-tecture but also transmitting across the spectrum and storing it securely is a challenge.

10.**Network Security:** Securing the network through various cryptography techniques and key management.

11.**Secure Routing**[6]: During routing data is most critical in the sense that an attacker can create a fake path to access critical information about the architecture.

Solutions available to us for the afore mentioned chal-lenges:-

1. We need regular authentication to solve our problem of maintaining integrity of data while ensuring device valida-tion[12,13] . A secure transit channel needs to be set be-tween both the communicating objects in a preset time-frame . In order to that we will require Security protocols at various layers, symmetric/asymmetric cryptographic algo-rithms and hashing functions[10].
2. On-demand routing protocols and Multi-path routing can be integrated in the disparate sensing networks[6].
3. One method of ensuring management of critical user data and traffic analysis is to have less overhead information for information security during the transmission. Another is to build a mode based on the concept of trust between devices and systems to store user information in cloud database, however there must be a backup available of the critical data at a number places isolated from each other[2,14].



Limitations on the above mentioned solutions:-

1. IoT devices are very small compared to traditional IT de-vices so in them even if cryptographic algorithms are im-plemented the limited resources on these devices would be tied up in them which would make key management and storage critically unsafe[1].

2. Providing a User Interface and a Storage Capacity will se-verely limit the efficacious solutions designed for numerous security challenges thrown by IoT devices[1,10,13].

3. Many manufactures will give their gadgets their own inno-vation or technology that will not be present in others to expand their market share, this is a potential threat.

III. PROPOSED WORK

We propose that in order to have a truly secure device where the consumers mind can be at peace the manufactures of IoT systems should make use of micro-kernel approach. Micro-kernel approach would be utilising minimal kernel and enforc-ing hardware separation[4]. Also only kernel runs in CPU privileged mode. In this approach there is no restrictions on component software while ensuring that we can reuse legacy software. If every aspect is separate there would be no existen-tial threat even if one device or a part of O.S gets compromised[4].

While Micro-Kernel approach would be useful in isolating various different parts of architecture, we need to make sure that at no point end user's critical data is compromised. We make sure that does not happen through a multi-layered ap-proach to security that starts at the initialisation of the device when it is embedded into the network and is given power, es-tablishes a trusted and uses that trust to make something that cannot be tampered with. Security is not an add-on feature, throughout our research we have come to realise that not only manufacturers but the end consumers also view security as a luxury when it should be a corner stone of any device. In order to truly secure a device we need to address it throughout the life cycle from the device design to operational environment[3]. The vulnerabilities concerning the security of IoT devices are endless and at the crux of the matter is lack of a concrete architecture to safeguard consumer and business interests[8,12]. The first step to help secure our future is a comprehensive security framework. We propose a chassis to secure the vulnerabilities of fledgling IoT devices.

Framework for IoT Security:-

1. **Secure Start:** When device is initialised through electricity, device's software should be verified for its authenticity and integrity using cryptographically generated digital signa-tures . The process should be as follows a digital signature which is attached to the device's software should be validat-ed by the said device .This will ensure that only the soft-ware that has been sanctioned to run on that device, and signed by the entity that authorised it, will be loaded [3]. This establishes foundation of trust(Trust Management), however the device still needs protection from various threats such as malicious scripts being loaded at run time.

2. **Controlling Access:** Next, various types of access and re-source control should be employed in the architecture itself. Mandatory access controls built into the operating system will peg the privileges of various applications and compo-nents on the device[14] .This will ensure that the access be only given to the resources they need to do their respective jobs . In situation of attack if even one of the device's com-ponent is compromised, access control will ensure that the infiltrator has as nominal access to other parts of the operat-ing system. Access control mechanism built into the device are analogous to access control system employed in the network[3] . The principle of minimal privilege tells us that only the limited amount of access required to execute an operation should be validated in order to minimise the effi-cacy of any security breach.

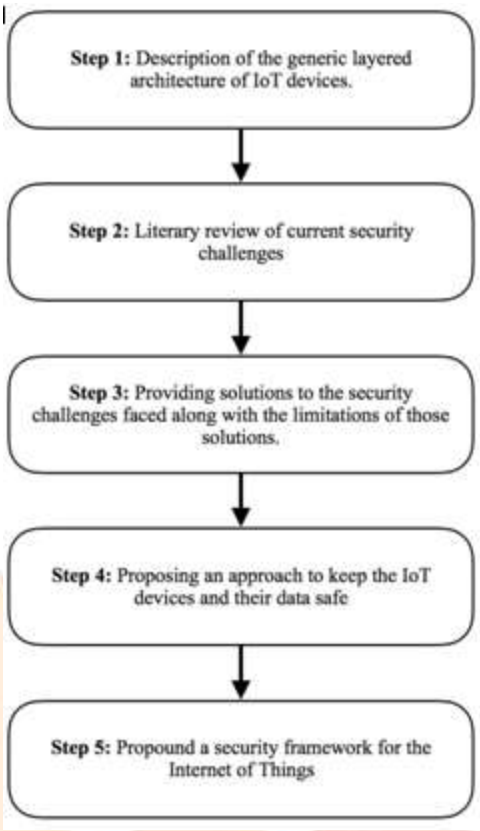
3. **Authentication of Device:** When the device is initially embedded into the network, it should authenticate itself before receiving or transmitting any sort of data . Generally users are not sitting on their keyboards to validate IoT de-vices which are embedded deep into the network so that they can gain access into the said network [3].To make sure that those devices which are correctly identified prior to authorisation we can use machine authentication, biomet-rics, two-factor authentication [12]. Authentication may require some additional time but it will in turn allow us to manage more devices in a synchronous way.

4. **IoT API Security:** One of the responsibility of the network is the ability to certify and countenance data movement between various applications, IoT devices embedded in the network and the back-end systems using technologies such as REST-based APIs. In order to protect the coherence of data travelling between the devices in the network and back-end systems, securing the API's is very crucial, this is because we need to validate all the devices , developer as well as the apps communicating with the API's so that we are better prepared against potential threats and attacks[11].

5. **Encryption:** Encrypting data at storage and in transit be-tween IoT devices embedded into the network and back-end systems using cryptographic algorithms such as AES-256, which would help maintain data integrity and it will also prevent the data being sniffed by potential attackers. Silicon Physically Unclonable Function (PUF)is emerging as a so-lution to keeping key safe as an attacker with physical ac-cess will not be able to get the desired outcome[5,7].

6. **Fire-walling and IoT Security Analytics:** A secure device also needs a deep packet inspection which has the capabili-ty to control traffic that is destined to terminate at the de-
vice[8].There is a pertinent need for host-based firewall even if network-based appliances are in place because deeply embedded devices have unique protocols, very dis-tinct from commonly used IT protocols. Protocols designed specifically for an Industry should filter along with having the ability for deep packet inspection to identify malicious payloads hiding in protocols[3]. While the network appli-ance take care of filtering and traffic management, the de-vice's job should be to filter specific data which is destined to terminate on that device while making efficient use of all the resources available to it. Accumulating and monitoring comprehensive data from IoT devices embedded into the network to provide a detailed report so that action can be taken on potentially dangerous activities should be done at regular interval[3]. The afore mentioned solutions need complex technologies such as artificial intelligence, ma-chine learning and big data techniques to provide effective predictive modelling and anomaly detection. These capabil-ities are still emerging but in future would be synonymous with IoT security[9].

7. **Patches and Updates:** As soon as the device is embedded into the network and working in it location, it should start receiving software updates and patches . Manufacturers and Operators should be mandated to roll out patches, and de-vices will then need to validate them, in a way that does not diminish the functional safety of the device[3] . The updates of firmware running on the device should be rolled out and delivered in such a way that it does not waste the limited bandwidth of the device while maintaining the intermittent connectivity of the embedded device[8]. The patches should in no way compromise the functional safety of the device and or the network.



Work Flow Step By Step Process

IV. CONCLUSION

As the euphoria of the potential of the Internet of Things dwindle down we are faced with practical reality where in-tegrity and confidentiality of information of a consumer is ever so easily available by executing relatively simple attacks. Unlike the smartphone revolution, IoT devices will, in the main, be relatively cheap low-cost items, and they'll be manu-factured and sold by a huge range of vendors. Easy then, to cut corners and overlook important security aspects. If IoT is to play a lead role in the Industrial Internet and Industry 4.0, then a better framework for standards in security is needed.

V. REFERENCES

1. Khadija Fazal, Hassan Shehzad, Ayesha Tasneem, Aisha Dawood, Zohaib Ahmed - "A Systematic Literature Review On The Security Challenges Of Internet Of Things And Their Classification"

2. Earlence Fernandes, Amir Rahmati, Kevin Eykholt, Atul Prakash - "Internet Of Things Security Research: A Rehash Of Old Ideas Or New Intellectual Challenges?"

3. Wind - "Security In The Internet Of Things: Lessons From The Past For The Connected Future"

4. Jim Huang, Louie Lu - "Secure Microkernel For Deeply Embedded Devices"

5. Srini Devadas, Dwaine Clarke, Blaise Gassend, Daihyun Lim, Jaewook Lee, Marten Van Dijk - "Physical Unclon-able Functions And Applications"

6. David Airehrour, Jairo Gutierrez, Sayan Kumar Ray - "Se-cure Routing For Internet Of Things"

7. William Enck, Kevin Butler, Thomas Richardson, And Patrick Mcdaniel - "Securing Non-Volatile Main Memory"

8. Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan - "Internet Of Things (Iot) Security: Current Status, Challenges And Countermeasures"

9. Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh - "Iot Security: Ongoing Challenges & Research Opportunities"

10. Chris Folk, Dan C. Hurley, Wesley K. Kaplow, James F.
X. Payne - “The Security Implications Of The Internet Of Things”

11.John Thielens - “Without Api Management, The Internet Of Things Is Just A Big Thing”

12.Dave Raggett - “Tackling Data Security And Privacy Challenges For The Internet Of Things”

13.Manik Lal Das - “Privacy And Security Challenges In In-ternet Of Things”

14. Ericsson - “Iot Security: Protecting The Networked Soci-ety”

15. Michael W. Condry, Catherine Blackadar Nelson- "Using Smart Edge Iot Devices For Safer, Rapid Response With Industry Iot Control Operations", Proceedings Of The Ieee, 2016