Issues and Challenges in Security and Privacy of Internet of Things (IOT)

Ugwuabonyi E.C[1] and Orji E.Z[2]

[1]*Computer Science Department, Enugu State University of Science and Technology (ESUT) Nigeria*
[2]*Computer Engineering Department, Enugu State University of Science and Technology (ESUT) Nigeria*

Abstract **- Internet of things (IoT) is becoming an integral part of our daily lives with more data being generated about our daily activities both humans and things than ever before. If we look at the data as the raw materials of our digital age, it is easy to see why the organization, government and industries value it highly than other areas of application. Data sharing needs to be voluntary with the individual agents having a thorough understanding of what is being shared with whom and for what purpose. It follows naturally that protection of these data is very crucial as data collected with a good intent can cause harm if it gets to the wrong hands.**

The paper presents the protocol architecture, the technologies and applications of IoT in different areas, the security challenges in internet of things (IoT), the vulnerabilities and proffer appropriate measure to counter the security threats and attack.

Keywords: **Data, Architecture, Technologies, Vulnerability, IoT, Security**

I. INTRODUCTION

The IoT is a technological innovation that represents the future of computing and communications, and its development depends on dynamic technical innovation in a number of important fields, from wireless sensors to nanotechnology (D.K, 2017). Smaller devices, things and even humans are allowed to be connected to interact.

It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies (Nunberg, 2012). IoT evolved from peer-to-peer connection to the connection of devices to internet to web and to connection of people and thing over the network. This causes a drastic growth rate of internet.

In January 2014, Forbes listed many Internet-connected appliances like televisions, kitchen appliances, cameras, and thermostats that can “spy on people in their own homes” (Steinberg, 2014)

The phrase “Internet of Things” was coined about 19 years ago by the founders of the original MIT Auto-ID Center, Kevin Ashton in 1999 and David L. Brock in 2001 (Sundmaeker, et, al 2010) who predicted “a world in which all electronic devices are networked and every object, whether it is physical or electronic, is electronically tagged with information pertinent to that object.”

The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service (Perera, et, al 2013).

Internet of Things means a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols (Bassi & Horn, 2008).

IoT can also be defined as An open and comprehensive network of intelligent objects that has the capacity to auto-organize, share information, data and resources, reacting and acting in the face of situations and changes in the environment. (Somayya, Ramaswamy, & SiddharthTripathi, 2015)

The IoT is criticized for being developed rapidly without appropriate consideration of the profound security challenges involved and the necessary regulatory changes (Clearfield, 2014). The security concern and challenges in IoT must be clearly stated and solution mechanism is adapted to form secure, robust and resilient data across the network.

II. PHASES OF INTERNET OF THINGS SYSTEM

(Hu, 2016), described the phases of the internet of thing undergo five stages from Collection to delivery of the information to the end users. The phases include the collection, storage, processing, transmission and delivery.

Phase I: Data Collection, Acquisition and Perception

The first phase in every IoT application be it precision agriculture, smart cities, logistics, connected cars, etc., is data collection or acquisition from the devices or things. Sensor networks are the key to gathering the information needed by smart environments, whether in buildings, utilities, industrial, home, shipboard, transportation systems automation, or elsewhere (Lewis, 2004). It has thousands of millions of small devices each with sensing, communication, processing capabilities to perceive the real world environment. Sensor networks are used to gather dynamic data while RFID is used to gather static data.

Phase II: Storage

The information gathered by sensors and RFID in phase 1 has to be stored. Generally, the internet of things components has to be installed with low memory and low processing capabilities. Hence, because of the billions of things being connected to the internet the cloud takes care of the storage.

Phase III: Processing

The IoT analyzes the data stored in the cloud data centers and provides intelligent services for work and life in hard real time. As well as analyzing and responding to queries, the IoT also controls things. The IoT offers intelligent processing and control services to all things equally hence makes use of network neutrality where no bit of information is given a priority over another in the network.

Phase IV: Transmission

Transmission occurs in every phase of IoT system ranging from data collection to information delivery. First, data is transferred from Sensors, RFIDs or chips to Data Centers. Secondly, the data is being transferred from Data Centers to Processors for processing and finally from processors to end devices or end users.

Phase V: Delivery

This is the last phase in IoT systems. It involves delivery of processed data to things on time without errors or alteration is a sensitive task that must always be carried out.

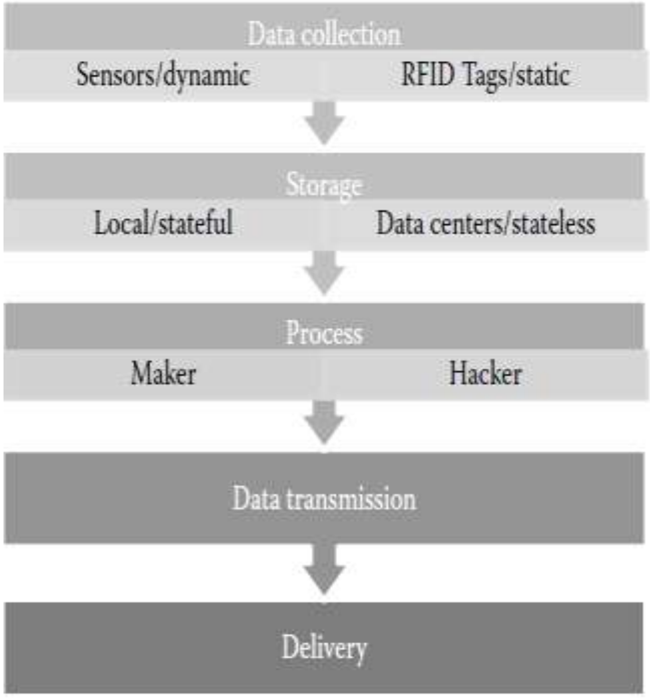

Fig 1:Phases of IoT system

III. ARCHITECTURES OF IOT

IoT is vast in nature and in such a broad concept there is no proposed uniform architecture which is the main problem of IoT. In order for the idea of IoT to work, it must consist of an assortment of sensor, network, communications and computing technologies, amongst others (Gigli, 2011).

Generally, the composite operation of an internet system can be organized into three layers: perceptual layer, network and transport layer, and application layer.

The Perceptual Layer of IoT perceives the physical properties of things around us that are part of the IoT. This process of perception is based on several sensing technologies (e.g. RFID, WSN, GPS, NFC, etc.). In addition, this layer is in charge of converting the information to digital signals, which are more convenient for network transmission.

The Network Layer of IoT it is the responsibility of the Network layer to process data received from the Perception Layer. Also, it is responsible in transmitting data to the application layer through various network technologies, such as wireless, wired networks and Local Area Networks (LAN). The Network layer uses 3G, 4G, Wi-Fi, Bluetooth, Zigbee, FTTx, UMB, and infrared technology as its main media of data transmission. Huge quantities of data will be carried by the network. Hence, it is crucial to provide a sound middleware to store and process this massive amount of data. To reach this goal, cloud computing is the primary technology in this layer.

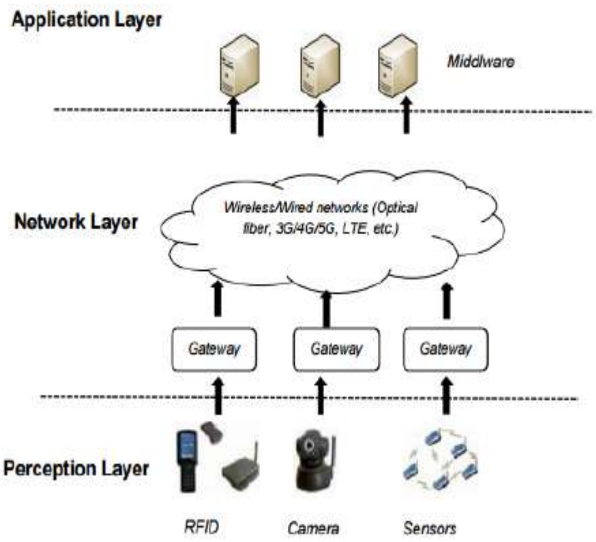

Fig 2: Architecture of IoT

The Application Layer of IoT uses the processed data by the Network Layer. This Application Layer is composed of the front end of IoT through which its potentials harnessed.

Moreover, this layer provides the required tools (e.g. actuating devices) for developers to realize the IoT vision.

IV. VULNERABLE FEATURES OF INTERNET OF THING

Security and privacy challenges poses a great threat in IoT since more and more things are being connected by the day. (Misra & Hashmi, 2017), proposed some of the challenges that can affect security and privacy in Internet of things are show in the figure 3 below.

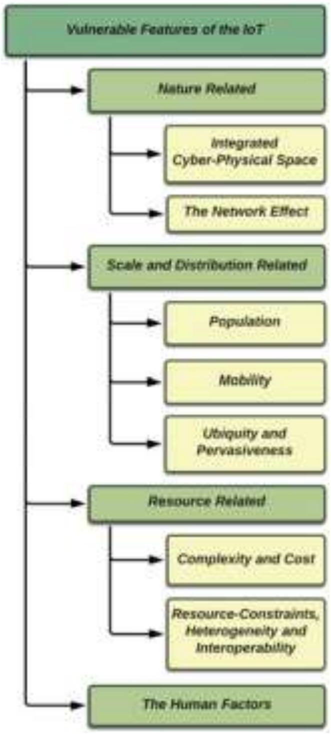
Vulnerable Features of the IoT
Nature Related
Integrated Cyber-Physical Space
The Network Effect
Scale and Distribution Related
Population
Mobility
Ubiquity and Pervasiveness
Resource Related
Complexity and Cost
Resource-Constraints, Heterogeneity and Interoperability
The Human Factors

Fig 3: Vulnerable features of IoT *(Misra & Hashmi, 2017)*

Integrated Cyber-Physical space - The most significant feature of the IoT is its ability to integrate computing and communication capabilities with monitoring and control of entities in the physical world. This feature has enabled the actions of real, physical entities, or events in real environment to influence the events in the virtual world, and vice versa. Many of such associations are safety-critical: their failure can cause irreparable harm to the associated physical systems or people (Greenberg, 2007). For instance Sensors and RFIDs are used to perform data acquisition and collection, disruption of these services will lead to severe problem in public health, safety and economic place.

Network Effect - Human-to-Human (H2H, Human-to-Things (H2T), Things-to-Things (T2T) connection in IoT has made IoT the largest network. This has worsen the challenges of maintain the security and privacy in the Internet of Things. Most IoT services are realized through high degree of intercommunication among the multiple component devices since there is increase in interaction between connected systems as it grows.

Population (Data Volumes) - Although some IoT applications use brief and infrequent communication channels, there are considerable number of IoT system such as sensor-based, logistics and large scale system that have potentials to entail huge volume of data on central network or servers (Mattern & Floerkemeier, 2010). There is high growth rate of things being connected to the internet. In 2003, 500 million things were connected to the internet. In 2010, 12.5 Billion things where connected to the internet. It has been predicted that in 2020, there will be 50 billion things connected to internet. This high rate of connection pose a big challenge to management security and privacy of connected things.

Mobility/Privacy Protection - Since a great number of RFID systems are short of suitable authentication mechanism, anyone can tracks tags and find the identity of the objects carrying them. Intruders can not only read the data, but can also modify or even delete data as well.

However, due to the mobile devices such as the smartphones, laptops and tablet, personal computers, cars, wearable technologies like smartwatches and Google Glass, mobile sensors, and even connected livestock which are connected to the internet, there is minimum or no guarantee that all these devices will be secured. Hence there is no assurance of privacy.

Ubiquity and pervasiveness - Generally IoT is Anything, Anyone connection in Anywhere, Anyplace using Anypath, Anyservice. Its architecture is low-constrained in nature with low memory, low processing power and low CPU compared to the traditional internet. The inexpensiveness of the enabling technologies, has led to much widespread physical distribution of IoT systems. The ubiquity, pervasiveness, and the increasing invisibility of the IoT element worsen the identity management, monitoring, security, as well as privacy protection concerns.

Complexity and Cost - Device complexity is determined by the device’s processing capability, storage capacity, and other available resources. The higher the resources, the higher the complexity. The IoT comprises a variety of connected devices with diverse complexities, ranging from high complexity systems like servers and personal computers, to low complexity, specialized devices like sensors, to highly constrained devices like RFIDs.

Interoperability, Resource-constrained - The resource-constrained members of the IoT are a major vulnerability. Achieving interoperability among the resource-constrained networks and other network forms like the Internet is a challenge, as the resulting heterogeneity complicates protocol design and system operations (Roman, Najera, & Lopez, 2011).

Human factor **-** One of the most vulnerable features in internet of things is user or the manufacturer's action. A manufacturer can cause harm or turn malicious to system by trying to exploit the system or his irresponsible or ignorant actions can affect the system. For instance he may clone the device for his selfish reasons probably to make more gains.

V. SECURITY THREATS AND ATTACKS

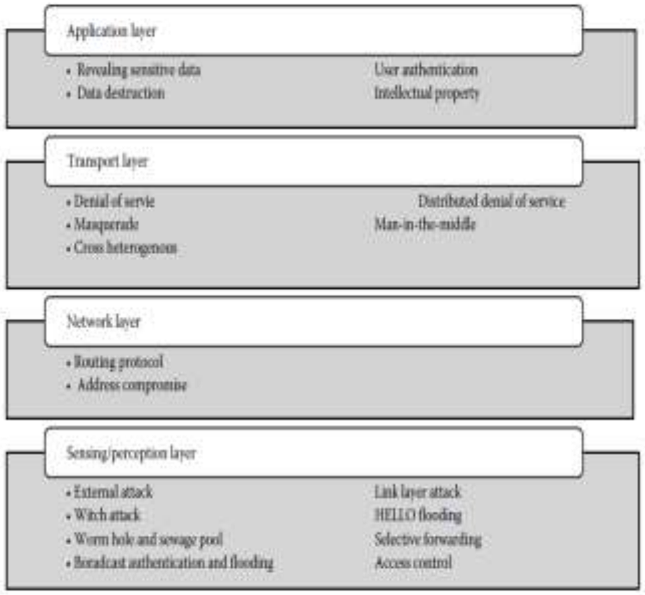

Fig 4: Security threats and attacks

Application Layer Attack

Data destruction: An attacker can gain access to a data stored in disks or other electronic media and cause misuse or destroy the sensitive information thereby rendering them completely unreadable and cannot be accessed by the authorized user. An attacker can also cause a packet on transit to be dropped. For instance, a poorly performed student can gain access to student grade record sheet and manipulate the result either on his favour or at the detriment of others.

User Authentication: A node or device can be impersonated when an unauthorized user gain access as a legitimate user. It will start to carry out attacks which will involve false readings and reporting of the data, offers bad control messages and also affects the traffic flow of the network. Authentication can be done by mutual authentication of routing peers before they can share information. This can be done by identifying each user, monitor connections through the firewall and restricting policies through the user name.

Transport Layer Attack

These are attacks that affect the transport layer of IoT. It includes but not limited to Denial of service (DoS), Distributed Denial of Service (DDoS), man-in-the-middle, cross heterogeneity, masquerade, etc.

Denial of Service (DoS) attack: Denial of Service (DoS): (Ojha, 2012), (Blackert, et al., 2003), is created by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In IoT, different types of DoS attacks in different layers might be performed. Jamming and tempering in common in physical layer, collision, exhaustion, unfairness exist at link layer, at network layer, neglect and greed, homing, misdirection, black holes while malicious flooding and desynchronization can be found at the transport layer. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

Man-in-the-Middle Attack: This attack is described as a form of eavesdropping in which the unauthorized party can monitor or control all the private communications between the two parties hideously. The illicit user can even fake the identity of one authorized user and communicate normally to gain more information in the system.

Network Layer Attack

Network attacks are the attacks that cause disruption of service and affect the routing of the packet from source to the destination. They attack the routing protocol and compromise the IP address of the device. Such attacks are sinkhole, Sybil, spoofed routing information, Ack. Flooding, etc.

Spoofed routing information: the most direct attack against a routing protocol is to target the routing information in the network. Disruption in the network may occur when the attacker spoof, modify, or replay routing information.

Sinkhole: (Sen, 2009), (Ojha, 2012), in a sinkhole attack, an attacker makes a compromised node look more attractive to its neighbors by forging the routing information. The result is that the neighbor nodes choose the compromised node as the next-hop node to route their data through. Sinhole attack aid in selective forwarding attack, where all traffic in a big network from different nodes will prefer to send their data through the compromised node.

This type of attack makes a compromised node to draw all the sensor network traffic to itself.

Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been able to insert itself between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them

Sybil attack: it is an attack where one node presents more than one identity in a network. It was originally described as an attack intended to defeat the objective of redundancy mechanisms in distributed data storage systems in peer-to-peer networks (Sen, 2009). Voting, routing algorithms, data aggregation, fair resource allocation, and foiling misbehaviour detection can all be attributed to Sybil attack.

Eavesdropping and passive monitoring: This is most common and easiest form of attack on data privacy. If the messages are not protected by cryptographic mechanisms, the adversary could easily understand the contents. Packets containing control information in a WSN convey more information than accessible through the location server, Eavesdropping on these messages prove more effective for an adversary.

Sensor/Perception Layer Attack

Link layer is responsible for multiplexing of data streams, data frame detection, medium access control, and error control. Attacks at this layer include purposefully created collisions, resource exhaustion, and unfairness in allocation (Sen, 2009). When two packets are transmitted over a network, a collision may occur which can lead to either packet loss or packet retransmission. During packet retransmission, an attacker can constantly send packet over the network to cause collision and thereby creating an Exponential back-off attack.

Wormhole: (Sen, 2009), (Ojha, 2012), a wormhole is low latency link between two portions of a network over which an attacker replays network messages. This link may be established either by a single node forwarding messages between two adjacent but otherwise non-neighbouring nodes or by a pair of nodes in different parts of the network communicating with each other. This sort of attack does not require compromising a sensor in the network rather; it could be performed even at the initial phase when the sensors start to discover the neighbouring information

Selective forwarding: In this type of attack, a compromised node in a network selectively forwards some messages and drops others. This is common in a multi-hop network like a WSN where all nodes in the network need to forward messages accurately for communication to take place.

Hello Flooding: (Sen, 2009), (Ojha, 2012), this attack uses HELLO packets as a weapon to convince the sensors in IoT. Here, an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within an IoT. The sensors are thus convinced that the adversary is their neighbor. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.

External attack: As internet keep growing and things get connected to internet where it is being stored in the cloud, trustworthiness of the cloud service provider is the key concern. Organizations may deliberately offload both sensitive and insensitive data to obtain the services. But they are unaware of the location where their data will be processed or stored. It is possible that the provider may share this information with others, or the provider itself may use it for malicious actions (Hu, 2016).

Witch attack: this type of attack occur when a genuine node fails and a malicious node takes advantage of such failure. Making the factual link takes a diversion through the malicious node for all its future communication, resulting in data loss (Hu, 2016).

Spoofed routing information: the most direct attack against a routing protocol is to target the routing information in the network. The attacker may disrupt the network traffic by spoofing, altering, or replaying routing information. Generating fake error messages, increasing end-to-end latency, causing network partitioning, creation of routing loops, and attracting or repelling network traffic from selected nodes may occur as a result of the network disruption.

Traffic analysis: Through an effective analysis of network traffic, an adversary can identify some sensor nodes with special roles and activities in a network. For example, a rapid increase in message communication between certain nodes indicates that those nodes have some precise activities and events to monitor in the network. By identifying such node, the attacker can disrupt the network by attacking those special nodes.

Node replication attack: In a node replication attack, an attacker attempts to add anode to an existing WSN by replication (i.e. copying) the node identifier of an already existing node in the network. A node replicated and joined in the network in this manner can potentially cause severe disruption in message communication in the WSN by corrupting and forwarding the packets in wrong routes. This may also lead to network partitioning, communication of false sensor readings.

Broadcast Authentication and Flooding: Whenever a protocol is required to maintain state at either end of a connection, it becomes vulnerable to memory exhaustion through flooding. An attacker may repeatedly make multiple connection requests until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored or the node becomes unreachable as a result of power exhaustion.

Acknowledgment spoofing: data transmission acknowledgment is required in some routing algorithms for WSNs. Attacking node eavesdropping may hear packet transmissions from its neighbors and spoof the acknowledgments thereby providing false information about the data transmission. In this way, the attacker is able to disseminate wrong information about the status of the nodes and the data.

VI. SECURITY MEASURES IN IOT

As things are getting connected to the internet, appropriate measure to secure the devices and things should be guaranteed. (Roman, Najera, & Lopez, 2011), opined that in order to avoid attacks and threats in IoT, it must have a strong security foundation built on a holistic view for all IoT elements at all phases, ranging from data collection to the delivery of the information, from data acquisition to the governance of the whole IoT infrastructure. (Misra & Hashmi, 2017), recognizes four key fields in the IoT to make it more secure, resilience, reliable, robust and efficient against different vulnerabilities. They include the following:

- Making the IoT more secure and private
- Standardization
- Governance
- Social Awareness

Making the IoT more Secure and Private

(Misra & Hashmi, 2017), (Roman, Najera, & Lopez, 2011), Summarized the security and privacy in IoT in five stages.

Protocol and Network Security: One of the issues in security and privacy of IoT is their resource-constrained nature. Highly constrained devices that use low-bandwidth standard such as IEE 802.15.4 must open secure communication channels with more powerful devices. Cryptographic mechanisms, Key Management Schemes and Standard security protocol are the cornerstone of IoT security.

Cryptographic Algorithm

The goal of a good cryptographic design is to reduce more complex problems to the proper management and safe-keeping of a small number of cryptographic keys, ultimately secured through trust in hardware or software by physical isolation or procedural controls (Menezes, Oorschot, & Vanstone, 1996). Cryptographic Algorithms include Symmetric Algorithms such as AES, DES, etc., Asymmetric Algorithms such as Rivest Shamir Adelman (RSA), Elliptic Curve Cryptography (ECC) and Hash Function such as SHA-1 and SHA-256.

Efficient Key Management

For securing cryptographic techniques providing confidentiality, entity authentication, data origin authentication, data integrity, and digital signatures are the basis of cryptography which Key management plays a essential role. The objective of key management is to maintain keying relationships and keying material in a manner which counters relevant threats, such as: (i) compromise of confidentiality of secret keys. (ii) Compromise of authenticity of secret or public keys. Authenticity requirements include knowledge or verifiability of the true identity of the party a key is shared or associated with. And (iii) unauthorized use of secret or public keys (Menezes, Oorschot, & Vanstone, 1996).

The key management schemes as outline by (Saxena, 2007) are network wide shared key, master keys and link keys, Public Key Cryptography, preconfigured Symmetric keys and Bootstrapping keys. Diffie-hellman (DH) is a key management Algorithm.

Standard Security Protocol

All the communication protocols in the traditional Internet and the IoT should be standardized to ensure consistent communication standards and to avoid usage of communication and security protocols, which are not optimal for some resource-constrained members of the system, or to avoid any intermediate protocol translation which endangers end-to-end security. The standardized communication and security protocols are required to not only fulfil the IoT’s performance goals but also provide the protocol’s original security properties in the context of the Internet architecture (Garcia-Morchon, et, al, 2014). Some network Protocols list are Internet key Exchange (IKEv2)/IPsec and the Host Identity protocol (HIP) perform an authenticated key exchange and set up the IPsec transforms for secure payload delivery, Transport Layer Protocol (TLS) provides security for TCP and requires a reliable transport, while it variant DTLS secures and uses datagram-oriented protocols such as UDP. Extensible Authentication Protocol (EAP) supports duplicate detection and retransmission, but does not allow for packet fragmentation. The Protocol for Carrying Authentication for Network Access (PANA) is a network-layer transport for EAP that enables network access authentication between clients and the network infrastructure.

Data and Privacy Enormous data generated with the connected things and people anytime, anyplace, anywhere have to be secured. (Roman, Najera, & Lopez, 2011), classified the Data and Privacy security as follows:

Privacy by Design: in which case the user will have the required tool to manage his own data

Transparency also forms essential part of Privacy of data since the user needs to know which entities are managing their data, how and when those entities are using it.

Data management: It is difficult to manage the huge data generated by the connection of billions of thing. Cryptographic mechanisms and protocols protect data throughout the service’s life cycle, but some entities might lack the resources to manage such mechanisms

Identity management: One of the problems facing IoT is the management of object and user identities and its relationship. Identity management supports Minimal disclosure of privacy information. To ensure security of data identities, security elements like integrity, availability, authenticity, non-repudiation are integrated in classic identity protocols.

Trust Management

Trust should be deemed to be a vital component of the IoT. Trust in the context of the IoT encompasses the following two concepts:

- Reduction of uncertainty and improvement of trustworthiness of the constituting elements of the IoT.
- User experience: How comfortable, secure and capable the users feel while interacting with the IoT.

Fault Tolerance: Fault tolerance is essential to assure service reliability, resilience in IoT but any solution must be specialized and lightweight to account for the number of constrained and easily accessible IoT devices. Fault tolerance in the IoT can be accomplished with the help of three main cooperative efforts.

The first of the efforts is to make all IoT objects secure by default.

Designing a secure mechanisms and protocols by researchers are not enough; they must work hard in improving software implementation quality. Reason is that it is not easy to proved software patch for billions of IoT devices

Secondly, it is important for all IoT objects to know the state of the network and its services which it belongs to.

Lastly, network failures and attacks should be withstood by these IoT objects.

All objects should be able to degrade its services and also its protocol should incorporate mechanisms that respond to abnormal situations on the network.

IoT Governance: Laws and Policies will help ensure security and privacy in IoT. Governance helps strengthen trust in the IoT. A common framework for security policies will support interoperability and ensure security's continuity. This can be accomplished by defining adequate enforcement mechanisms which will help in data protection

Social awareness: The manufacturers, service providers, and enterprises need to consider societal needs and legal obligations while developing IoT services. They also need to be updated about the development standards set by an established consortium. IoT device and application developers should be aware of secure development practices. Application developers should ensure stable, resilient and trustworthy coding through observing better code development standards, developer trainings, threat analysis and rigorous software testing. Vendors should update device software/firmware to fix vulnerabilities, but should avoid untrusted third parties to apply the upgrades.

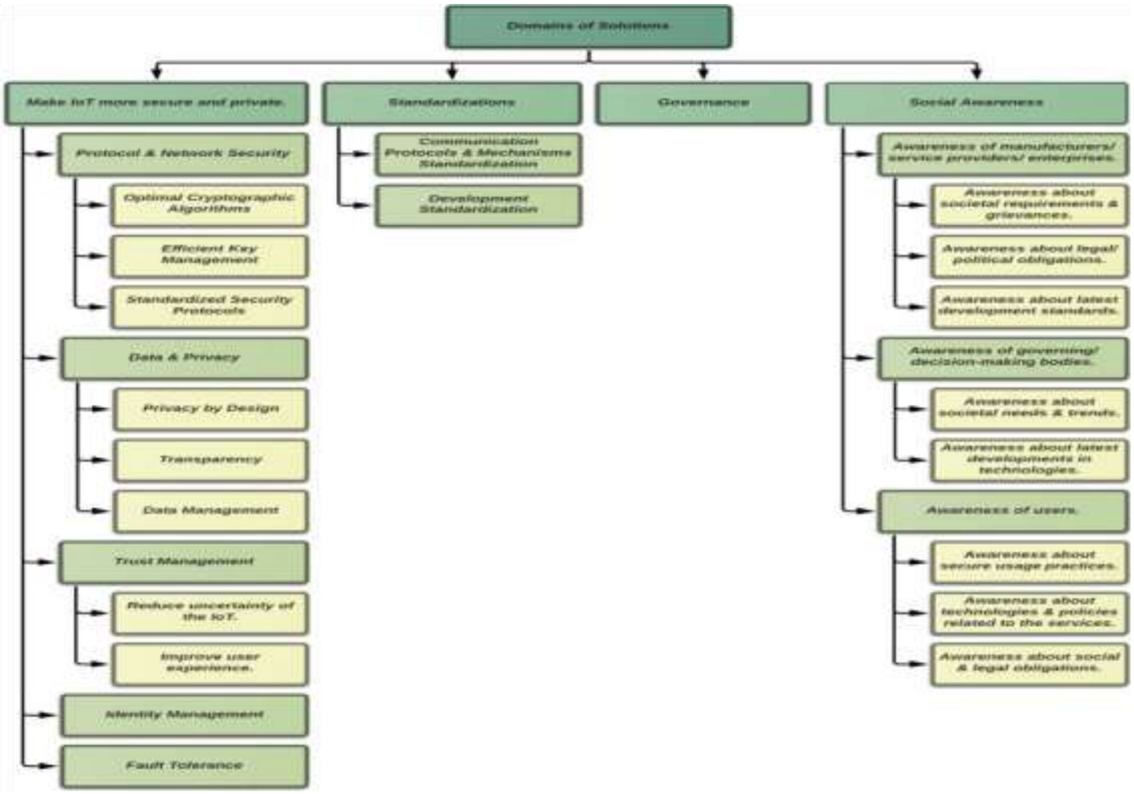
Domains of Solutions
Make IoT more secure and private.
Standardizations
Governance
Social Awareness
Protocol & Network Security
Optimal Cryptographic Algorithms
Efficient Key Management
Standardized Security Protocols
Data & Privacy
Privacy by Design
Transparency
Data Management
Trust Management
Reduce uncertainty of the IoT.
Improve user experience.
Identity Management
Fault Tolerance
Communication Protocols & Mechanisms Standardization
Development Standardization
Awareness of manufacturers/ service providers/ enterprises.
Awareness about societal requirements & grievances.
Awareness about legal/ political obligations.
Awareness about latest development standards.
Awareness of governing/ decision-making bodies.
Awareness about societal needs & trends.
Awareness about latest developments in technologies.
Awareness of users.
Awareness about secure usage practices.
Awareness about technologies & policies related to the services.
Awareness about social & legal obligations.

Fig 5: IoT security domain. (Misra & Hashmi, 2017)

VII. CONCLUSION

Anything, anywhere, anyplace internet of things has actually made internet a buzzword today. The paper presents the protocol architecture, the technologies and applications of IoT in different areas, the security challenges in internet of things, the vulnerabilities and proffer appropriate measure to counter the security threats and attack.

Protocol and Security, Communication protocol, Cryptographic encryptions, among others are the some of the security measures suggested to be the cornerstone of IoT security.

This is because of its low energy consumption, low processing power and low memory storage requirements.

REFERENCES

[1]. (n.d.). Retrieved from https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_E
[2]. Bassi, A., & Horn, G. (2008). *Internet of Things in 2020: A Roadmap for the Future.* Information Society and Media, European Commission.
[3]. Blackert, W., Gregg, D. M., Castner, A. K., Kyle, E., Hom, R., & Jokerst, R. (2003). Analyzing interaction between distributed denial of service attacks and mitigation technologies. *Proc. DARPA Information Survivability Conference and Exposition.*
[4]. Clearfield, C. (2014). *Why the FTC can't regulate the Internet of Things.* Retrieved from http://www.forbes.com/sites/chrisclearfield/2013/09/18/why-the-ftc-cant-regulate-the-internet-of-things/.
[5]. D.K, A. S. (2017). Internet of Things (IoT): A Literaturer Review. *International journal of Research in Advent Technology (IJRAT)*.
[6]. Garcia-Morchon, O., Kumar, S., Keoh, S., Hummen, R., & Struik, R. (2014). Security considerationsin the IP-based Internet of Things. draft-garcia-core-security-06. *CoRE: Internet Draft*.
[7]. Gigli, M. a. (2011). Internet of Things, Services and Applications Categorization. *Advances in Internet of things: Scientific Researcg*.
[8]. Greenberg, A. (2007). *Americas Hackable Backbone* . Retrieved from Forbes.
[9]. Hu, F. (2016). Security and Privacy in Internet of Things (IoTs): Models, Algorithms and Implementations. In N. Jeyanthi, *Internet of Things (IoT) as interconnection of threats (IoT).* CRC Press, Taylor and Francis group.
[10]. Lewis, F. (2004). Wireless sensor network.
[11]. Mattern, F., & Floerkemeier, C. (2010). From the Internet of Computer to the Internet of Things. *Springer*.
[12]. Menezes, A. J., Oorschot, P., & Vanstone, S. (1996). *A handbook of applied cryptography.*
[13]. Misra, S. M., & Hashmi, S. (2017). Security Challenges and Approaches in Internet of Things. *Springer Briefs in Electrical and Computer engineering*.
[14]. Nunberg, G. (2012). The advent of the Internet: 12th April courses. *International Journal of Innovation and Research in Technology*.
[15]. Ojha, D. (2012). SECURITY PROBLEMS AND VARIOUS SECURITY: SCHEMES IN WIRELESS SENSOR NETWORKS. *International Journal of Research in Science And Technology*.
[16]. Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2013). Context Aware Computing for The Internet of Things: A Survey. *IEEE Communications Surveys & Tutorials*.
[17]. Roman, R., Najera, P., & Lopez, J. (2011). Securing the Internet of Things. *IEEE Computer*.
[18]. Saxena, M. (2007). *SECURITY IN WIRELESS SENSOR NETWORKS - A LAYER BASED CLASSIFICATION.* Purdue University, West Lafayette: Center for Education and Research in Information Assurance and Security.
[19]. Sen, J. (2009). A Survey of Wireless Sensor Network Security. *International Journal of Computer Networks and Information Security*.
[20]. Somayya, M., Ramaswamy, R., & SiddharthTripathi. (2015). Internet of Things (IoT): A Literature. *Journal of Computer and Communications*.
[21]. Steinberg, J. (2014, Jan 27). *Steinberg, J.: These devices may be spying on you (Even In Your Own Home) (2014).* Retrieved from https://www.forbes.com/sites/josephsteinberg/2014/01/27/these-devices-may-be-spying-on-you-even-in-your-own-home/#13e4c615b859.
[22]. Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the Internet of Things. *EUR-OP*.