Security in Internet of Things: Challenges, Solutions and Future Directions

Sathish Alampalayam Kumar [1] Tyler Vealey[1] Harshit Srivastava [2]
Coastal Carolina University, Conway, SC, USA[1] Guru Gobind Singh Indraprastha University, New Delhi, India[2]
Email: skumar@coastal.edu; tsvealey@g.coastal.edu and harshit.ndl@gmail.com

***Abstract*—Internet of Things (IoT) is an enabler for the intelligence appended to many central features of the modern world, such as hospitals, cities, grids, organizations, and buildings. The security and privacy are some of the major issues that prevent the wide adoption of Internet of Things. In this paper, with example scenarios, we are presenting review of security attacks from the perspective of layers that comprises IoT. In addition, a review of methods that provide solutions to these issues is presented along with their limitations. To overcome these limitations, we have provided future work recommendations with a framework. Further research and implementation of the framework and our recommendations will further enhance the robustness and reliability of the IoT and their applications against a variety of known attacks.**

Keywords*—*Internet of Things, security, privacy, reliability, attacks, protection methods, framework, threats

I. Introduction and Background

Internet of Things (IoT) enables various devices that we use on a daily basis can interact with each other via Internet. This ensures the devices to be smart and send the information to a centralized system, which will then monitor and take actions according to the task given to it. IoT can be used in wide range of domains including healthcare, transportation, entertainment, power grids and smart buildings [20, 22]. IoT is expected to act as a catalyst for the future technological innovations and its use is expected to rise exponentially over the coming years.

With a massive amount of devices connected to the Internet and the huge data associated with it, there remain concerns about the security [18]. By security we mean the degree of resistance to, or protection of the IoT infrastructure and applications. Many of these devices are easy targets for intrusion because they rely on very few outside resources and are often left unattended. Once the network layer is compromised, it is very easy for a hacker to gain control and maliciously use a device as well as attack other devices nearby through the original compromised node. In particular, appliances that maintain an online presence are easy to attack. These devices that do not have any virus protection or malware protection are highly susceptible to being used as "bots" to forward malicious code to infect other devices [18]. The International Data Corporation predicts that more than 200 million devices will be connected to the Internet by the year 2020, with a good amount of these being appliances; there will be a large opportunity for hackers to use these devices to their advantage through "denial of service" attacks, malicious email, and other harmful worms or Trojans. A recent HP study reveals that 70% of Internet of Things devices are vulnerable to attacks [33].

As per recent test conducted by HP, about 90 percent of tested devices collected at least one piece of personal information via the product itself, the cloud or its mobile application [33]. This personal information might easily get compromised due to a cyber-attack or unauthorized access. This will reduce confidentiality, integrity and security of the data and evidently users will be reluctant to adopt this technology [19]. Therefore, a major concern in adopting and implementing this new technology is security and privacy. Security for the users should be ensured by preventing unauthorized identification and access. By Privacy we mean that the data of the user is under his or her own control and no one else's. With a very high dependence on the data and devices based on IoT, another issue that arises is reliability. By reliability we mean that the devices need to work effectively, as intended at all times without failure. In addition to the IoT, the data transmitted between the devices and the Internet should be reliable, since giving false information or providing unreliable data is a grave concern as this might lead to taking unnecessary or wrong consequences.

Section 2 describes the protocols and standardization efforts that are being carried out to make the secure IoT feasible. Section 3 summarizes the key layers that make up IoT and Section 4, with examples of attack scenarios, provides an overview of practical security attacks classified by IoT layers. Section 5 provides an

1530-1605/16 $31.00 © 2016 IEEE
DOI 10.1109/HICSS.2016.714

IEEE computer society

overview of current security methods to protect IoT with their limitations. Section 6 provides future work recommendations to overcome the limitations with a model framework. Finally we present our summary and conclusion in Section 7.

II. Secure Protocols for IoT

Building interconnected and interoperable smart objects requires the adoption of standard communication protocols. International organizations such as the Internet Engineering Task Force (IETF) and the IPSO Alliance, promote the use of the Internet Protocol (IP) as the standard for interoperability of smart objects. Due to billions of objects expected to be connected and IPv4 addresses have almost reached depletion, IPv6 is identified as a possible solution for smart-object communication [24]. The protocol stack that smart-objects will implement will try to match classical Internet hosts in order to make it feasible to create the so-called Extended Internet, that is, the aggregation of the Internet with the IoT. Since the protocol architecture of smart objects should adhere to the standard IP architecture (for obvious integration reasons), many of the security mechanisms already defined and currently used for the Internet can be reused in IoT scenarios [28].

At network layer, an IoT node can secure data exchange in a standard way by using the Internet Protocol Security (IPsec) [27]. IPSec, which was initially developed for IPv6, found widespread adoption even in IPv4 where it was back-engineered. IPSec was an integral part of IPv6. IPSec can be used to protect data-flow between terminals (host-to-host communication), pair of security gateways (network-to-network communication) or between security gateway and a terminal (network-to-host communication). IPSec can provide confidentiality, integrity, data-origin authentication and protection against replay attacks, for each IP packet (it works at network layer). These security services are implemented via two IPSec protocols: Authentication Header (AH) and Encapsulated Security Payload (ESP). The AH is responsible for providing integrity, data-origin authentication and anti-replay capabilities, while ESP is responsible for providing confidentiality, authentication and integrity.

In the current IP architecture, data exchange between nodes is secured at the transport level via Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS). TLS provides completely secure communications through: peer-entity authentication and key exchange (using asymmetric cryptography); data authentication, integrity, and anti-replay (through message authentication code) and confidentiality (using symmetric encryption). The peer-entity authentication and key exchange is performed by TLS handshake phase, which is done at the beginning of the communication. Probably the biggest issue that exists in IPSec and transport layer approaches is that they are dependent on intermediate nodes, in order to assure complete end-to-end security. However, end-to-end security can still be provided but only in the presence of very trusted intermediate systems.

A different approach that aims at addressing these issues is to provide complete end-to-end security at the application level. This, in turn, simplifies the complexities of deployment of security in underlying layers and reduces the cost, in terms of packet-size and data processing, because only application have to be secured and only per-data overhead will be introduced. Moreover, multicast communications, and in-network data aggregation in encrypted domains (for example through homomorphic cryptography) is easier to be implemented at application level. The disadvantage that this approach has is that by providing security at application level, complications are introduced in the application development and the overall code size due to poor reuse of software codes. This is mainly due to the lack of well- defined and adopted secure protocols at application level.

III. Key Layers of IoT

As shown in Figure 1, following are the key layers for accomplishing an objective of creating IoT [22, 31]:

- Application Layer: Consists of the various applications and services that the IoT provides. Applications include smart cities, smart home, transportation, utilities and healthcare
- Perception Layer: This layer consists of various forms of sensory technologies, including temperature sensors, vibration sensors, pressure sensors, and RFID sensors that allow devices to sense other objects
- Network Layer: This layer consists of network communications software as well as physical components such as topologies, servers, network nodes, and network components that allow the devices to communicate. Its main purpose is to transmit data between devices and from the devices to receivers
- Physical Layer: The physical layer consists of the basic hardware such as physical components, smart appliances and power supplies that acts as backbone for networking the smart objects.

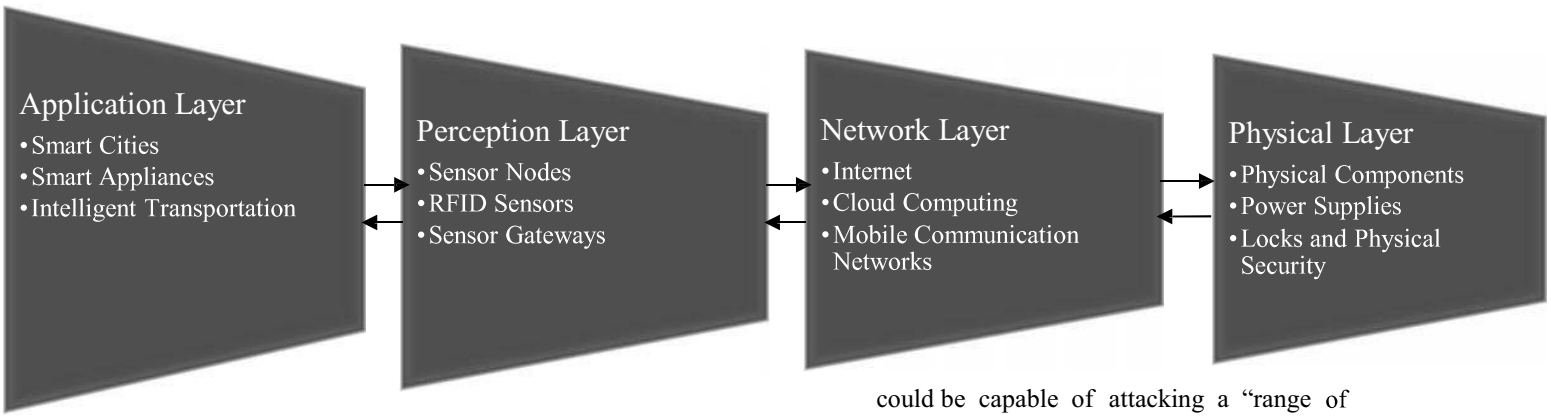

Fig 1. IoT as a Layered Approach

IV. Security Issues in IoT Layers

With the high adoption rate of Internet of Things, more and more devices are connected to the Internet. Every day, these smart objects are becoming target for information security risks; IoT has the potential to distribute these risks far more widely than the Internet has to date [17]. The four layers in IoT that we discussed earlier play the most important role in IoT and to make IoT reliable and secure, we need to make sure that these four basic layers are secured. Attacks can be carried out heavily on the devices and it is the basic elements in these layers will have to deal with them. Monitoring of these devices should also be done in such a way that no data is lost or altered.

A. Security Issues in the Application Layer

Due to security issues in the application layer, applications can be shut down and compromised easily. As a result, the applications are failed to carry out the services they are programmed to do or even carry out authenticated services in an incorrect manner. In this layer, malicious attacks can cause bugs in the application program code that triggers the application to malfunction. This is a very dangerous concern based on the numbers of devices categorized as application level entities [17, 18, 21]. Common threats to Application Layer are:

- *Malicious code attacks*: An example scenario in this type of attack could be a malicious "worm" spreading on the Internet attack embedded devices running a particular operating system for e.g. Linux. Such a worm could be capable of attacking a "range of small, Internet-enabled devices" such as home routers, set-top boxes and security cameras. The worm would use a known software vulnerability to spread. Such code attacks could break into a Car's Wi-Fi, take control of the steering wheel, and crash the car resulting in injuries to the driver and the car.
- *Tampering with node-based applications*: Hackers exploit application vulnerabilities on device nodes and install malicious root kits. The security design of devices needs to be tamper-resistant or at least tamper-evident. Protecting specific parts of a device may be insufficient. Some threats can manipulate the local environment to cause the device to malfunction and result in heating or freezing the environment. A tampered temperature sensor would just show a fixed value of temperature, while tampered camera in the smart home would relay outdated pictures.
- *Inability to receive security patches*: In areas such as nuclear reactors, if the software bug in the constantly moving node is not updated with software patches, it may result in catastrophic consequences [32, 34].
- *Hacking into the smart meter/grid*: In this scenario, a smart meter, which is responsible for sending the usage data to the utility operator for dynamic billing must be secured. If someone accesses that data transmission, one can know when then home is empty based on the power utilization, making it ideal for burglary or even worse. Attack on smart grid is much more catastrophic and cost the economy in billions of dollars.

B. Security Issues in the Perception Layer

The security threats in the Perception layer are at node level. Because the nodes are made up of sensors, they are prime targets from hackers, who wish to utilize them to replace the device software with their own. In the perception layer, majority of the threats

comes from the outside entities, mostly with respect to sensors and other data gathering utilities [17, 18, 21]. Common threats in Perception Layer are:

- *Eavesdropping*: As the mode of communication between these devices will be wireless and through the Internet, the devices will be vulnerable to eavesdropping attacks as the devices will generally be left unattended. In this attack scenario, sensors in the smart home or m-health domain that are compromised can send push notification to users and try to collect private information from the users.
- *Sniffing Attacks*: Attackers can put malicious sensors or devices close to the normal sensors of the IoT devices, in order to acquire information from the device. The profusion of smart environment IoT devices means that humans can be identified, tracked and profiled to a greater degree throughout the physical environment, without their consent. For instance, as more human-to-human and human-to-device interactions occur over shared physical networks, shared service and social spaces, it is also possible to sense smaller amounts of physical trails of these interactions with a greater degree of sensitivity and accuracy.
- *Noise in data*: Due to transmission of data over wireless networks covering large distances, there are high possibilities that the data may contain noise i.e., incomplete information or even worse, false information. Misrepresentation of data can be dangerous in such scenarios when a lot is dependent on the reliable transmission of data.

C. Security Issues in the Network Layer

The network layer is highly susceptible to attacks because of the large amount of data that it carries, this causes a large amount of "network congestion". In this layer, the prominent security issues are with respect to the integrity and authentication of the data that is being transported in the network. An attack from hackers and malicious nodes that compromises devices in the network is a serious issue. Common threats to Network layer are:

- *DoS attack*: The devices or server are bombarded so that they are unable to service those users, who need their services. DoS attacks that shut down the transfer of data between the devices and their source. An overflow of information is sent to the device that shuts down its processes. For example, seizure of the health information systems and services implemented in the lower bandwidth IoT networks mean risks of life-threatening situations and loss of business [16].
- *Gateway Attacks*: These attacks cut off connection between the sensors and the Internet infrastructure. Gateway attack could include DoS attack or routing attacks launched in the gateway that results in no or wrong information being transmitted from the Internet to the sensors/nodes/actuators, thereby jeopardizing the functioning of the sub-domains, such as vehicular networks or smart cities [19].
- *Unauthorized Access*: Devices may be left unsecured either because their owners expect that they will remain under their physical control. However, if they don't, they are open to use by anyone. Embedded micro devices and macro devices may need to be left unattended for long periods, in relatively inaccessible environments, e.g., pace-makers that are implanted in the human body and remote sensors left in uninhabited physical environments. These unattended embedded devices, that are used for control, e.g., pace-maker implants, require stable timing to deliver control signals at set times, over time are very risky for the users. As the devices will be designed to communicate with other devices in order to transmit and receive data, some malicious nodes may try to disguise themselves as "authenticated" and access these devices without possessing the authority and compromise the devices.
- *Storage Attacks*: Huge chunks of data containing vital information of the user will need to be stored on storage devices or on cloud, both of which can be attacked and the data may be compromised or changed to incorrect details. The replication of the data coupled with the access of data to different types of people results in the increased surface area for the attacks.
- *Injecting fake information*: Outside attackers can inject false data causing the system to react inappropriately or dangerously. This may also be a precursor to a physical attack and may be used to mask such threats.

D. Security Issues in the Physical Layer

There are many security issues at the physical layer of IoT system as well. There is great need for new technology to safeguard power sources and physical security mechanisms. Devices need to be secured against physical attacks, both from weather

and individuals perspective. They also need to be power efficient and capable of relying on battery power in the event of a city grid blackout or power interrupt. Batteries need to hold charge for a sufficient amount of time and recharge quickly so as to keep the device running. [17, 18, 21]. Common issues in Physical Layer are:

- *Physical Damage*: An example scenario in this type of attack is physical devices such as sensors, nodes and actuators that are physically damaged by the malicious entities. This could cause the sensor, nodes and actuators to lose its expected functionality and become vulnerable to other risks.
- *Environmental attacks*: An example scenario in this type of attack is sensors that are bombarded with the environmental hazards like abnormal rain/snow/ wind. This could cause the sensor to lose its expected functionality and vulnerable for the other risks.
- *Loss of Power*: Devices that run out of power essentially cannot operate normally and this results in a denial of service. For example, a common strategy to conserve power is for devices to enter various power-saving modes, e.g., various sleep and hibernation modes. A sleep deprivation attack makes just enough legitimate requests to prevent a device from entering its energy-saving mode.
- *Hardware Failure*: The devices act as a lifeline to the user and he/she will be very much dependent on these devices. So, it is important that no hardware failures occur which result in the condition that the device stops working or even worse, starts sending incorrect data. Cyber-attack on smart cities would result in an inadequate supply of electricity/water and result in chaos.
- *Physical tampering*: In the factory floor automation, deeply embedded programmable logic controllers (PLCs) that operate robotic systems are integrated into the typical enterprise IT infrastructure. It is important to shield those PLCs from human interference and at the same time protect the investment in the IT infrastructure and leverage the existing security controls.

V. Security Methods to Protect IoT

Following are prominent security methods that have been proposed in the literature for IoT. These security methods were identified from the leading journals and conferences as well as reviewing the citations for these articles. Table 2 summarizes the existing methods and their limitations from providing security and reliability for IoT.

The Identity Framework Management Methods proposed by A. Sardana and S.Horrow solves issues regarding the authentication of data and processes between the cloud and sub-sequential communication devices. It suggests having an Identity manager that authenticates the data and then forward it to a Service Manager to validate the instructions of the service to be performed [1].

Another proposed security method is the Game Theory based Adaptive Security for Smart IoT method by Cox that involves simulated use of strategies in which computers make decisions to develop strategies to prevent, detect, and avoid attacks. It introduces reliability and risk analysis in the face of threats [9].

Z. Li's propose a PKI-Like Protocol that involves encrypting the routes of nodes to their destinations and using a key for decryption and security. The data is sent along the way to and "offspring node", that then transmits the key when the node reaches the destination node [3].

R. Aggarwal also proposes another method of security not protecting the data but the devices using Radio Frequency Identification, that are embedded in devices to allow the devices to communicate with one another and communicate with humans [4].

Another method is the use of cyber sensors, or sensors that detect real time data such as temperature and speed for use in real time events and for immediate actions [8]. Another security method is called the "preference based Privacy model" which uses a third party to identify what security level should be used for a device based on the set preferences [5].

Intelligent Transportation Systems (ITS) use another security method called risk analysis in which a public key infrastructure is used in the Certificate Authorities (CA's) are used for managing and monitoring security credentials for the network nodes on ITS to devices to prevent data from being interrupted [7]. The use of middleware as a security method is also growing in popularity. Middleware can be used to secure communication by devices though encryption [6].

Lui et al., has proposed authentication and access control in the IoT that fixes loopholes in device security and data integrity. In this method, an user requests authentication to access a device and asks for permission from a "Registration Authority" (RA). RA in turn send user a question, if response is OK, the user is authenticated to access the device [2].

A.Dohr et al. has proposed an innovative framework called Ambient Assisted Living (AAL), which allows elderly people to lead a safe and independent lifestyle as long as possible by encompassing IoT based technical systems. Although the proposed method is quite practical and can be helpful, the main drawback of this approach is that it only tries to address the connectivity issues but there is no mention of the privacy and security features. However, they mention that security, privacy and reliability are main needs of the elderly, who would be the prime users of the AAL method [10]. The two methods proposed for implementing the connectivity technology are:

- *Keep In Touch (KIT)*: It uses smart objects and technologies such as Near Field Communication (NFC) and Radio Frequency Identification (RFID) to facilitate tele-monitoring process.
- *Closed Loop Hierarchy*: This service uses KIT and is capable of processing relevant data and establishing communications between elderly people and care-givers such as physicians and relatives.

Sventek, J., et al. propose a method of Self-Managed cells (SMC). SMC model is composed of policy, discovery and role services, which allow for easy management and measurement of resources. The main drawback of this approach is that the architecture proposes policy services, which vaguely touch upon the authorization and authentication and does not address any other security and privacy issues [11].

In their Domain Specific Metrics (DSM) approach Jafari et al. discuss security metrics for eHealth information systems. They propose security metrics development based on five elements: technology maturity analysis, threat analysis and modelling, requirements establishment, policies & mechanisms and system behavior. However, their discussion does not provide any methods for the identification, collection, computation or the application of the security metrics to address the security issues and objectives [12].

Weiß et al. propose comparative and comprehensive metric (CCM) approach for providing security functionality built on risk management approach. In their approach, security is quantified in terms of incidents as a result of asset loss. The model is based on the assumption that the good incident knowledge would be able to offer evidence, especially for the security effectiveness. However, the availability and attainability of the data related to incidents is often a challenge in security measurement [13].

Pierre de Leusse et al. propose Self-Managed Security Cells (SMSC) model, which is an improvement of Self-Managed cell model that also takes into account the security aspects. It proposes a scalable security enhancement system for distributed resources. The method has several components, which aims at providing interoperability, decentralization, automation and contextualization in addition to security [14].

There is another common approach discussed in many papers in regards to adaptive learning. Abie H. et al. propose an Adaptive Security and Trust Management (ASTM) solution with the main idea that the system learns and adapts to changing environment dynamically and anticipates unknown threats by making dynamic changes in the security architecture and parameters of the system. The limitation of this method is that, it is a more abstract concept rather than validated and applied for IoT environment [15, 23, 24].

As for sensor protection R. Savola has proposed an idea: Adaptive Security Management that involves the gathering of sensory data from within and around the system and its environment to analyze information and respond to changes by adjusting internal parameters like encryption schemes, access controls, and security protocols and procedures and making dynamic changes in the structure of the security system to protect the device [16]. This method is based on adaptive learning. The main contribution of their work is identification of the security objectives and the adaptive security management needs in the eHealth IoT environment. Though they have proposed high level adaptive security management mechanism that utilizes security metrics, details of the implementation is missing. Their adaptive security management mechanism comprises of the following four steps:

- *Continuous Monitoring*: Regular and continuous collection of data is implemented to know about every little change.
- *Analytics and predictive function*: These functions are executed on the collected data. Analytics function analyses the data stored and notes down all the changes and reactions to certain phenomenon and the predictive function then tries to predict future events based on the analysis.
- *Decision making*: The next step is carried out by the decision making device which decides on whether to carry out the changes or not
- *Metrics-based adaptive security models*: This final step is carried out to evaluate and validate the capacity to adapt to the challenges in the changing environments and rising threat situation.

TABLE 2: EXISTING METHODS AND THEIR LIMITATIONS FROM PROVIDING SECURITY AND RELIABILITY FOR IOT

Method/Author /Layer	Issues it addresses	Solution	Limitations
RFID Tags (Radio Frequency ID) / Aggarwal et al., [4] (Physical Layer)	Not being able to connect devices	RFID tags can be installed/embedded into smart objects to allow fast communication between devices	While RFID tags are useful for providing security, they are also very prone to hacking as more and more RFID banking applications are becoming susceptible to" RFID hacking"
Identity Management Framework Method /Horrow et al., [1] (Network Layer)	Authenticating data that travels between the device and the cloud	Place an Identity Manager and Service Manager on the devices	The protocols to develop the method have not yet been implemented
ITS Security Methods and Standards for Efficiency – Risk Analysis /Zhao et al., [7] (Network Layer)	Address threats to the ITS or Intelligent TransportationSystem(i.e. smart transportation)	A public key infrastructure is used in that certificate authenticating (CA's) are used for managing and monitoring security credentials for the network nodes on ITS to devices to prevent data from being interrupted	Technology is still being developed
Authentication and Access Control / Lui et al., [2] (Network Layer)	Fixes loopholes in device security and data integrity	A user requests authentication to access a device, things ask for permission to do so from a "Registration Authority", RA approves device to send user a question, if response is OK, user is authenticated access to the device	Systems are still very vulnerable to Man in the Middle attacks and Eavesdropping attacks
Security Middleware /You-guo and Ming-fu [6] (Network Layer)	Provides security to Intelligent home systems and communication devices	Uses Entity identification, Secure Storage, Security Audit, Data encryption / decryption, digital signature / verification to secure communication between devices	Middleware is an upcoming trend, it's not yet widely integrated or used
AAL / A. Dohr et al. [10] (Perception Layer)	Safe lifestyle for the elderly people	Keep In Touch (KIT) through smart objects and technologies such as NFC, RFID and Closed Loop Hierarchy	Fails to address the security and privacy issues, though they identify security, privacy and reliability as the main needs of the intended users of AAL.
Cyber Sensors / Liu et. al., [8] (Perception Layer)	Lack of data output from physical objects/lack of real time data	Cyber sensors that capture data from physical objects can later be used to perform actions or real – time event response	Some of the technology for the sensors does not yet exist
PKI – Product Key Infrastructure / Li et al., [3] (Perception Layer)	Threats involving node security	Nodes are authenticated by an "offspring node" that sends a decryption key when the node is safely transmitted. Offspring node still continues to be improved and developed.	Encryption is not fast
SMC/Sventek [11] (Perception Layer)	Management and measurement of resources in a ubiquitous computing environment	An SMC (Self-Managed Cells) model which is composed of policy, discovery and role services	Policy services vaguely touch upon the authorization and authentication issues but do not address any other security and privacy issues
ASM/ Reijo M. Savola et al. [16] (Perception Layer)	Identifies security objectives and threats in data integrity and adapts to environmental and censored changes that it detects utilizing the security metrics.	ASM comprises of four steps: continuous monitoring, analytics and predictive function, decision making, and metrics based adaptive security models. Sensors are analysed to gather information about the devices surroundings & environment. Very successful in hospitals	The high level security management mechanism does not provide details on the security metrics and the security objectives it tries to solve. Sensors can fall subject to interference from other electronic devices.
DSM/Jafari et al. [12] (Application Layer)	Security metrics for eHealth information systems	For the development of security metrics, they propose five elements that deal with security analysis and policies in general	Fail to address the methods for the identification, collection, computation or the application of the security metrics to address the security issues and objectives.

Game Theory /Cox and Balasingham [9] (Application Layer)	The attack of various varying complex systems	Method of attacking systems to develop better security strategies.	Prototyping is not yet complete. So not clear how the system will handle varying complex systems.
Preference Based Privacy Protection Method /Tao and Peiran [5] (Application Layer)	Issues in data privacy	A third party entity evaluates the user's security and privacy preferences and reports it to the service provider that gives the user an appropriate security level based on its sensed preferences before it connects the device to the Internet of Things.	The security mechanism and levels at which to set privacy still require more development as the Internet of Things is fairly new
CCM/Weiss et al. [13] (Application Layer)	Security metrics model based on risk assessment approach	In their model, the security is quantified in terms of incident and asset loss.	Availability and attainability of the data is a challenge to measure security metrics
SMSC/Pierre de Leusse et al. [14] (Application Layer)	Scalable security model for IoT infrastructure	Scalable security enhancement system of the SMC model for distributed resources	This generic model needs to validated for specific applications and security objectives
ASTM/Abie, H. [15] (Application Layer)	System that Adapts to changing environment dynamically and anticipating unknown threats	Adaptive learning technique by changing the internal parameters and the dynamic change to the architecture of security systems	This abstract model needs to be validated against dynamic scenarios of application domain and the unknown threats and failures.

VI. Recommendations for Future Work

To address some of the limitations indicated in Table 2, we recommend that the security framework, as shown in Figure 2 can be expanded to address those limitations. In this framework, Threat Index (TI) calculates the vulnerability of an IoT environment to threats and attacks. This threat index is calculated based on the parameters collected from IoT environment based on security control, legal control and policy control perspectives. By calculating the threat index, performance trend of IoT environment from the security perspective, can be identified and communicated to the user. Threat Index can be calculated over a specified period of time and that can be compared with the benchmark index thresholds obtained with the help of historical training Historical training is performed by the collection of data, with and without attacks, with and without legal control, with and without policy control over a long period of time. The comparison of the index threshold with the threat index helps the IoT provider to gain knowledge of the current security, policy and legal state [35 -37]. This will help the IoT provider to increase or decrease the controls from technical, legal and policy perspectives.

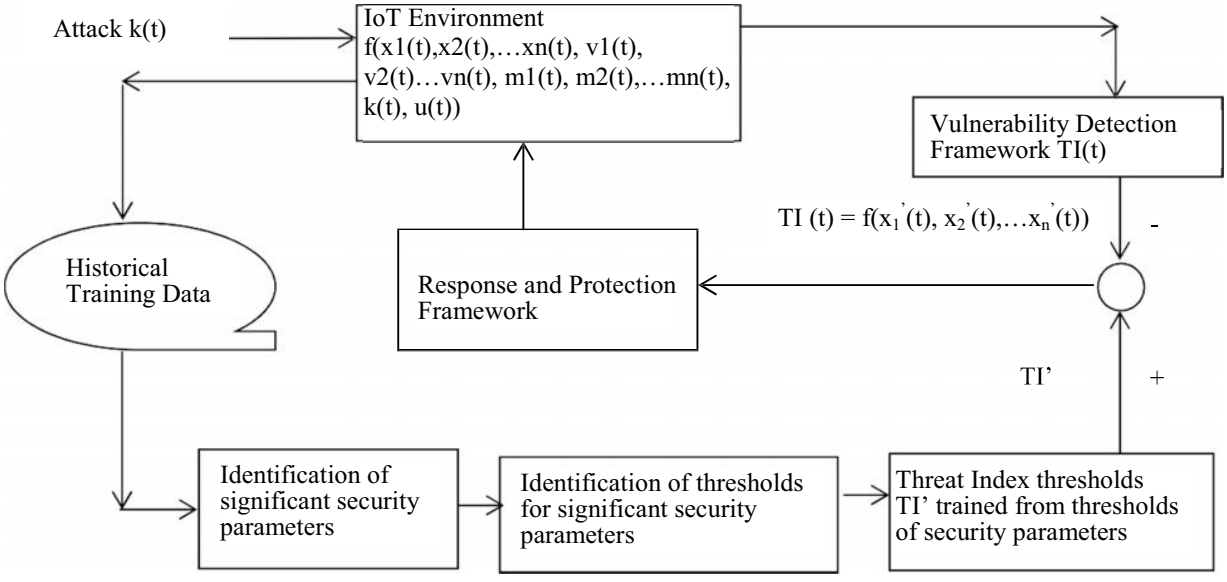

Fig 2. Recommended Security Framework

In the Figure 2, IoT is represented as a function: $f(x_1(t), x_2(t),\ldots x_n(t), v_1(t), v_2(t)\ldots v_n(t), m_1(t), m_2(t),\ldots m_n(t), k(t), u(t))$, where $x_n(t)$ represents the significant attack sensitive network parameters, $v_n(t)$ represents the network parameters which are not significant in representing the node vulnerability, $m_n(t)$ represents the mobility parameters, k(t) represents the attack and u(t) represents the control input. $x_n'(t)$ represents the modified values of the significant attack sensitive network parameter due to the influence of the attack k(t) and the control input u(t). TI for a node is calculated by the detection framework from the attack sensitive network parameters, $x_n'(t)$ using fuzzy logic. The computed Threat Index TI(t) is compared with the threshold values of the Threat Index TI'. The Threat Index thresholds (TI') are obtained with the help of the training dataset where the state of each record is labeled. Data records collected from simulation environment with and without attack are used as training dataset for identifying the Threat Index thresholds. As shown in Figure 2, the training data is derived from the IoT and is used in the identification of significant parameters and the thresholds of these parameters and the threat index. If the computed TI(t) of a node is greater than or equal to vulnerable state threshold reference TI', the node is identified to be under threat. Upon detecting that a node is under threat, the neighboring nodes are subjected to the response and protection algorithm in the response framework. This response algorithm identifies the intruder and sends the control signal u(t) to isolate the intruder from the IoT. The control signal u(t) varies depending upon the type of the intrusion. This control signal reconfigures the IoT and modifies $f(x_1'(t+1), x_2'(t+1),\ldots x_n'(t+1))$ such that TI(t+1) reaches the steady normal state. It should however be noted that $f(x_1'(t+1), x_2'(t+1),\ldots x_n'(t+1))$ also depend on any new attack k(t+1).

Following are some of the capabilities that need to be added and validated in future to the existing methods

1. Devices in the IoT environment need to be implemented with the Identity Management (Authentication and Authorization) suited for the IoT environment with a faster encryption compared to the existing methods [25].
2. Implement cyber sensors that capture data from physical objects to calculate threat index in order to perform actions or real – time event response
3. Identify the privacy requirements, privacy related parameters and the mechanism to evaluate Threat Index for Privacy and protect IoT from privacy related threats
4. Adapt the public key infrastructure to the IoT environment in the framework
5. Ensure the physical level security issues such as physical tampering and power deprivation attacks are addressed
6. Develop threat models for Man in the Middle and Eavesdropping attacks and evaluate threat index for those attacks and respond to them in real time.
7. Develop methods to ensure secure IPSec and transport layer without depending on intermediate nodes in order to assure complete end-to-end security

VII. Conclusion

In this paper, we have articulated that as more and more IoT based devices get connected to the Internet, it results in the extension of the surface area for external attacks. We classified those attacks based on the layers that make up IoT and discussed several such attacks with examples. We have also surveyed the literature on the existing methods to protect the IoT infrastructure and summarized these security methods on how they address the security issues in the IoT. We have summarized the limitations of the existing security methods and proposed future work recommendations to overcome these limitations. In order for the customers to embrace the IoT technologies and the applications, these privacy and security issues and limitations need to be addressed and implemented immediately, so that potential of the IoT technology and their applications can be realized.

References

[1] A. Sardana and S. Horrow, "Identity management framework for cloud based internet of things", Proceedings of the First International Conference on Security of Internet of Things, pp. 200-203, 2012.

[2] Lui, Xiao, Chen. "Authentication and Access Control in the Internet of things" 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW), pp. 588 – 592, 2012

[3] Zhihua Li et al., "Research on PKI-like Protocol for the Internet of Things", Fifth International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), pp. 915 – 918, 2013.

[4] Renu Aggarwal. "RFID Security in the Context of "Internet of Things", Proceedings of the First International Conference on Security of Internet of Things, pp. 51-56, 2012

[5] Tao and Peiran, "Preference-based Privacy Protection Mechanism for the Internet of Things", International Symposium on Information Science and Engineering (ISISE), pp. 531 - 534 2010.

[6] Li You-guo, Jiang Ming-fu. "The Reinforcement of Communication Security of the Internet of Things in the Field of Intelligent Home Through the Use Of Middleware", Fourth International Symposium on Knowledge Acquisition and Modeling (KAM), pp. 254 - 257 2011

[7] Zhao, Walker and Wang. "Security Challenges for the

Intelligent Transportation System", Proceedings of the First International Conference on Security of Internet of Things, pp. 107-115, 2012

[8] Huansheng Ning and Hong Liu, Laurence T. Yang, " Cyberentity Security in the Internet of Things", vol. 46, no. 4, pp. 46-53,. April 2013

[9] Abie, H., and Balasingham. "Risk-Based Adaptive Security for Smart IoT in eHealth".2011 Proceedings of the 7th International Conference on Body Area Networks, pp. 269-275, 2011.

[10] A. Dohr, R. Modre-Osprian, M. Drobics, D. Hayn, G.Schreier, "The Internet of Things for Ambient Assisted Living", Seventh International Conference on Information Technology, pp. 804-809, 2010

[11] Sventek, J., et al.,"Self-Managed Cells and their Federation". 3rd Intl Conference on Mathematical Method, Models and Architectures for Computer Networks Security (MMM- ACNS 2005), pp. 47-52, 2005.

[12] Jafari, S., Mtenzi, F., Fitzpatrick, R., and O'Shea, B., Security metrics for e-healthcare information systems: a domain specific metrics approach", Int. Journal of Digital Society, Vol. 1, No.4, pp. 238-245, 2010.

[13] Weiß, S., Weissmann, O., and Dressler, F., "A comprehensive and comparative metric for information security", In Proceedings of IFIP International Conference on Telecommunication Systems, Modeling and Analysis (ICTSM'05), pp. 1-10, 2005.

[14] Pierre de Leusse., Panos Periorellis., Theo Dimitrakos., and Srijith K., Nair., "Self-Managed Security Cell, a security model for the Internet of Things and Services", First International Conference on Advances in Future Internet, pp. 47 – 52, 2009.

[15] Abie H., and Balasingham I., "Adaptive security and trust management for autonomic message- oriented middleware", IEEE 6th Int. Conference on Mobile Ad hoc and Sensor Systems (MASS'09), pp. 810-817, 2009.

[16] Reijo, M, Savola., Habtamu, Abie., Markus Sihvonen., "Towards Metrics-Driven Adaptive Security Management in E-Health IoT Applications". Proceedings of the 7th International Conference on Body Area Networks, pp. 276-281, 2012.

[17] Hi Suo, Jiafu, Caifeng Zoua, Jianqi Liua Wan. "Security in the Internet of Things – A Review", International Conference on Computer Science and Electronics Engineering (ICCSEE), pp. 648 –651, 2012.

[18] Xu Xiaohui. "Study on Security Problems and Key Technologies of The Internet of Things Fifth International Conference on Computational and Information Sciences (ICCIS),pp.407–410,2013.

[19] Arun Kanuparthi, Ramesh Karri, Sateesh Addepalli. Hardware and Embedded Security in the Context of Internet of Things. Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles , pp. 61-64, 2013

[20] Atzoria, L., Ierab, A., and Morabito, G. 2010. "The Internet of Things: A survey", Computer Networks, vol. 54, no. 15, pp. 2787-2805.

[21] Kozlo et al., "Security and Privacy Threats in IoT Architectures", Proceedings of the 7th International Conference on Body Area Networks pp. 256-262, 2012

[22] Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I.. Internet of things: Vision, applications and research challenges", Ad Hoc Networks, 10(7), 1497-1516, 2012.

[23] S. P. Alampalayam and A. Kumar, "Security Model for routing attacks in Mobile Ad hoc Networks", IEEE 58th Vehicular Technology Conference, 2003. VTC Fall 2003, pp. 2122 – 2126, 2003

[24] S. P. Alampalayam and A. Kumar, "An adaptive and predictive security model for mobile ad hoc Networks", Springer Wireless Personal Communications 29 (3-4), pp. 263-281, 2004

[25] M. Turkanovic, B. Brumen, M. Hölbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion, Ad Hoc Networks 20:96-112, 2014

[26] Deering, S.; Hinden, R. RFC 2460-Internet Protocol, Version 6 (IPv6) Specifi cation, 1998. Available online: http://tools.ietf.org/rfc/rfc2460.txt, accessed Nov 2014

[27] Dierks, T.; Allen, C. RFC 5246-The TLS Protocol, 2008. Available online: http://tools.ietf.org/rfc/rfc5246.txt, accessed Nov 2014

[28] Rescorla, E.; Modadugu, N. RFC 6347-Datagram Transport Layer Security Version 1.2, 2012.Available online: http://tools.ietf.org/rfc/rfc6347.txt, accessed Nov 2014

[29] Kent, S.; Atkinson, R. RFC 2401—Security Architecture for the Internet Protocol, 1998. Available online: http://tools.ietf.org/rfc/rfc2401.txt, accessed Nov 2014

[30] Simone Cirani, Gianluigi Ferrari, and Luca Veltri, "Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview", Algorithms 2013, 6, 197-226

[31] K.Sonar and H. Upadhyay, "A Survey: DDOS Attack on Internet of Things", Intl. Journal of Engineering Research and Development, vol. 10, no. 11, pp. 58-63

[32] Do-Yeon Kim, "Cyber security issues imposed on nuclear power plants", Annals of Nuclear Energy, Volume 65, 2014, pp. 141 –143, 2014

[33] HP Whitepaper retrieved in Aug 2015 http://go.saas.hp.com/fod/internet-of-things

[34] D. E. Denning, "Stuxnet: What Has Changed", Future Internet, vol.4 pp. 672-687, 2012

[35] SAP Kumar, A Kumar, S Srinivasan Statistical based intrusion detection framework using six sigma techniques, IJCSNS 7 (10), 333, 2007

[36] Intrusion Recovery Framework for Tactical Mobile Ad hoc Networks, SP Alampalayam, S Srinivasan The International Journal of Computer Science and Network Security 9 (9), 1-1, 2009

[37] Control Framework for Secure Cloud Computing H Srivastava, SA Kumar Journal of Information Security 6 (01), 12, 2014