Security Issues of IOT Architecture In Network Layer

N. Sriram[1]Dr. K. Tamizharasi [2]
[1, 2] Assistant Professor
[1, 2] Sri VidyaMandir Arts and Science College

Abstract- *The Internet of Things, or IoT, is a system of unified computing devices, which is automatic and digital machines, objects, animals or people that are used by unique identifiers (UIDs) and the capacity to transmit the data from a network without needful human-to-human or human-to-computer interface. The IoT which denotes a new advanced future where objects will be connected to the internet and make a smart collaborations with other objects anywhere, anytime. Even though we are developed a lot in technology, there are still problem in security thoughts of its usage that becomes a major worry in the plan of IoT architectures. In this paper we generally survived all the security issues in IoT along with an study of IoT architectures. It defines security needs and challenges that facing in IoT implementations and discusses security threats and related solutions on each layer of IoT architecture to make this technology secure and more ubiquitous.*

Keywords- Internet of Things, IoT, Security necessities, Security Challenges, Security intimidation, Security Solutions, IoT Implementations, IoT architecture

I. INTRODUCTION

Internet of Things (IoT) is the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment.

Although Internet of Things (IoT) is a well-known term and a rising trend in IT arena, there has been no agreed definition by the world group of people of users awaiting now. In fact, there are many different groups in industry and equivalence organizations that formulate similar ideas but in different forms and based on different mechanism or aspects of an IoT system.

Highlighting security issues surrounding IoT is the main goal of this paper. Security is an important concern for IoT technology because of following reasons [4]:

- IoT is accepted as an extended version of some different technologies such as Wireless Sensor Networks, Mobile Broadband and 3G/4G Communications Networks which are already under threat because of various security flaws.
- Every device is connected to Internet in IoT technologies and Internet is an unsecured environment naturally. There are many evil-minded people who are on the lookout for various system cracks and remote code executions.
- Objects in IoT communicate with each other; hence, there is a possibility that privacy and security can be delayed. This study presents a general survey of all the security issues in IoT along with an analysis of IoT architectures.

II. IOT ARCHITECTURE

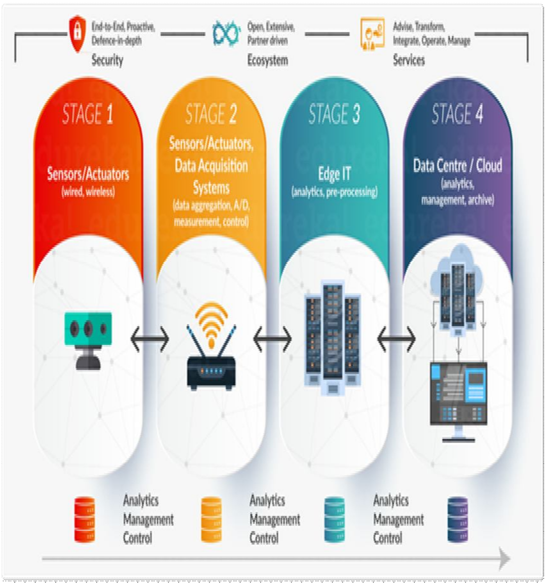

End-to-End, Proactive, Defence-in-depth
Security
Open, Extensive, Partner driven
Ecosystem
Advise, Transform, Integrate, Operate, Manage
Services
STAGE 1
Sensors/Actuators
(wired, wireless)
STAGE 2
Sensors/Actuators, Data Acquisition Systems
(data aggregation, A/D, measurement, control)
STAGE 3
Edge IT
(analytics, pre-processing)
STAGE 4
Data Centre / Cloud
(analytics, management, archive)
Analytics
Management
Control
Analytics
Management
Control
Analytics
Management
Control

Fig – 1 IoT Architecture

IoT architecture is the system, it as a plenty of elements like: sensors, protocols, actuators, cloud services, and layers. It has four stages of IoT architecture.

- Stage 1 IoT architecture consists of your networked things, typically wireless sensors and actuators.
- Stage 2 includes sensor data aggregation systems and analog-to-digital data conversion.
- Stage 3, edge IT systems perform preprocessing of the data before it moves on to the data center or cloud.

- Stage 4, the data is analyzed, managed, and stored on traditional back-end data center systems. Clearly, the sensor/actuator state is the province of operations technology (OT) professionals

1) **Perception Layer:** The sensor technology, intelligence embedded technology,nano technology and tagging technology are located in this layer. Main purpose of the layer is the identification of unique objects and the collection of information from the physical world with the help of its sensors.

2) **Network Layer:** It contains WSN, optical fiber communication networks, broad television networks, 3G/4G communications networks, fixed telephone networks and closed IP data networks for each carrier. Transfer of collected information from sensors, devices, etc., to an information processing system is under the responsibility of this layer.

3) **Support Layer:** The layer involves information processing systems which takes information in one form and processes (transforms) it into another form. This processed data is stored in a database and will be available when there is a demand. This layer works very closely with applications. Therefore, researchers prefer to place it in application layer.

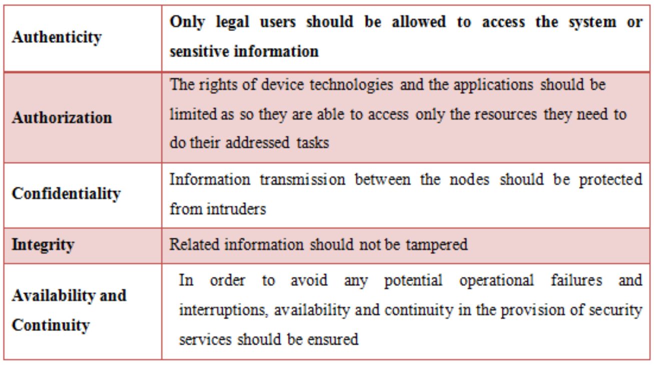
4) **Application Layer:** In this layer, there are practical and useful applications which are developed based on user requirements or industry specifications such as smart traffic, precise agriculture, smart home, mining monitor, etc.

III. SECURITY IN IOT ARCHITECTURE

The Internet of things aspires to connect anyone with anything at any point of time at any place. IoT is generally made up of three-layer architecture. Namely Perception, Network and Application layers.

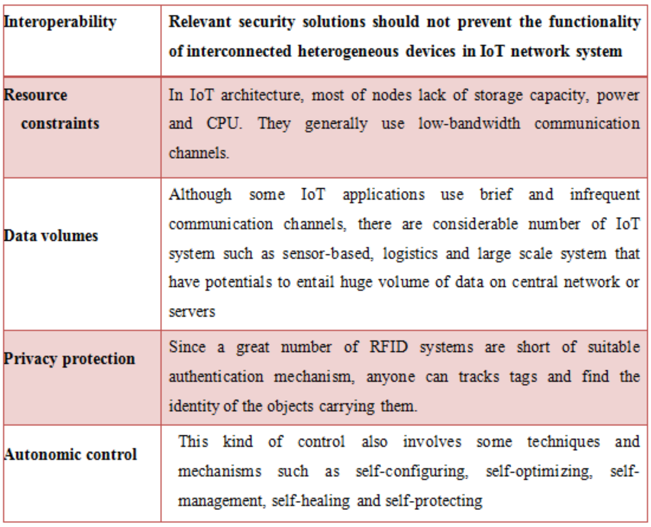
3.1 Existing Security Threats in IoT Systems

Table 1. Security requirements.



Authenticity	**Only legal users should be allowed to access the system or sensitive information**
Authorization	The rights of device technologies and the applications should be limited as so they are able to access only the resources they need to do their addressed tasks
Confidentiality	Information transmission between the nodes should be protected from intruders
Integrity	Related information should not be tampered
Availability and Continuity	In order to avoid any potential operational failures and interruptions, availability and continuity in the provision of security services should be ensured

Table 2. Security challenges.



Interoperability	**Relevant security solutions should not prevent the functionality of interconnected heterogeneous devices in IoT network system**
Resource constraints	In IoT architecture, most of nodes lack of storage capacity, power and CPU. They generally use low-bandwidth communication channels.
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
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.
Autonomic control	This kind of control also involves some techniques and mechanisms such as self-configuring, self-optimizing, self-management, self-healing and self-protecting

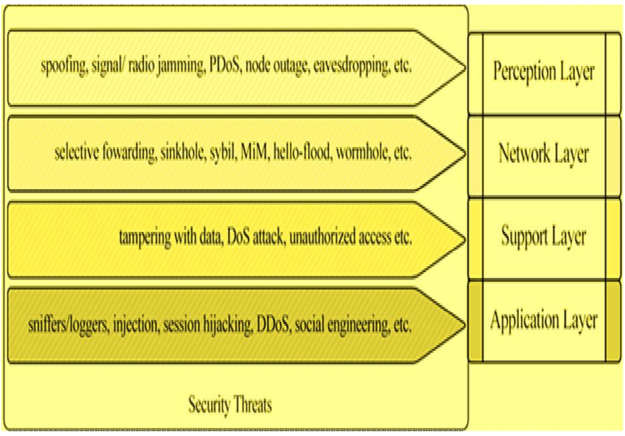

spoofing, signal/ radio jamming, PDoS, node outage, eavesdropping, etc.
Perception Layer
selective fowarding, sinkhole, sybil, MiM, hello-flood, wormhole, etc.
Network Layer
tampering with data, DoS attack, unauthorized access etc.
Support Layer
sniffers/loggers, injection, session hijacking, DDoS, social engineering, etc.
Application Layer
Security Threats

Fig – 2 Security attacks of IoT Layers.

3.2Threats of Network Layer

Network layer which is known as the next-generation network are exposed to many kinds of threats.

Selective Forwarding:

In such attacks, malicious nodes do not forward some messages and selectively drop them, ensuring that they cannot propagate later on. The attacker who is responsible for suppression or modification of packets originating from a select few nodes can sometimes forward the remaining traffic not to reveal her wrongdoing.

Sybil Attack:

It is simplified as a malicious device unlawfully taking on multiple identities. Sybil attack, an attacker can “be in more than one place at once” as a single malicious node.

Sinkhole Attack (Black hole):

The sink hole is defined in by intense resource contention among neighboring nodes of the malicious node for the limited bandwidth and channel access. It results in congestion and can accelerate the energy consumption of the nodes involved.

Wormhole:

This form of DoS attack induces relocation of bits of data from its original position in the network. This relocation of data packet is carried out through tunneling of bits of data over a link of low latency.

Man - in - the - Middle Attack:

This attack is described as a form of eavesdrop- ping in which the unauthorized party can monitor or control all the private communications between the two parties hideously. The unauthorized party can even fake the identity of the victim and communicate normally to gain more in- formation.

Flooding:

Routing algorithms in sensor-based systems need acknowledgements from time to time. In this type of DoS attack, a malicious node sends false information to destined neighboring nodes by the help of these salutations

IV. SOLUTIONS OF SECURITY ATTACK IN LAYERS

4.1 Security of Network Layer

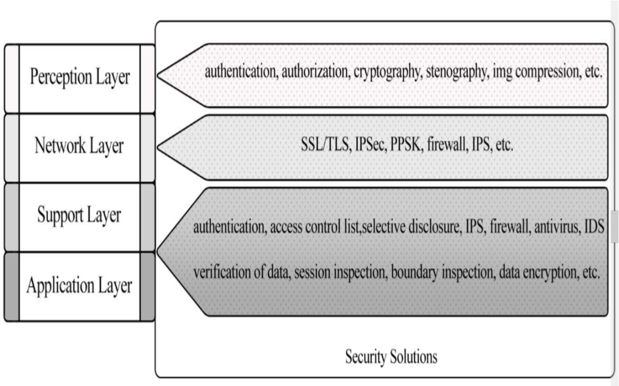
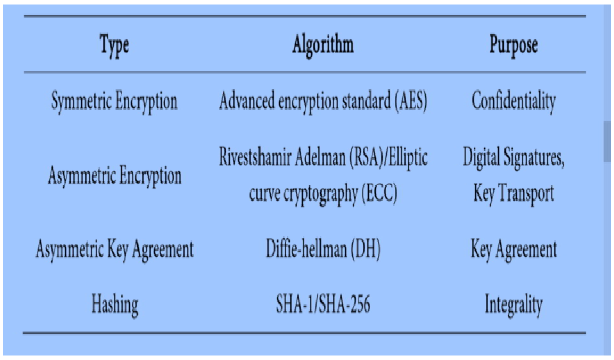

Perception Layer
Network Layer
Support Layer
Application Layer
authentication, authorization, cryptography, stenography, img compression, etc.
SSL/TLS, IPSec, PPSK, firewall, IPS, etc.
authentication, access control list,selective disclosure, IPS, firewall, antivirus, IDS
verification of data, session inspection, boundary inspection, data encryption, etc.
Security Solutions

Fig – 3: Security Solutions of IoT Layer

Table 3: Cryptography Algorithms



Type	Algorithm	Purpose
Symmetric Encryption	Advanced encryption standard (AES)	Confidentiality
Asymmetric Encryption	Rivestshamir Adelman (RSA)/Elliptic curve cryptography (ECC)	Digital Signatures, Key Transport
Asymmetric Key Agreement	Diffie-hellman (DH)	Key Agreement
Hashing	SHA-1/SHA-256	Integrality

The security of network layer can be examined in two main sub-layers; wireless and wired. One of the initial actions in wireless security sub-layer is the development of protocols for authentication and key management.

SSL, or Secure Sockets Layer, is the predecessor to TLS, or Transport Layer Security. SSL has three versions, which are all considered insecure due to flaws in their design. TLS was created to address the weaknesses in the SSL protocol. The terms SSL, TLS and SSL/TLS are commonly used interchangeably in literature.

Setting up an SSL/TLS session consists of three main steps

- The first step is to agree upon a cipher suite – a combination of key exchange algorithm, cipher and message authentication code.
- The second step is to exchange keys as per the agreed key exchange algorithm.
- The third step is to use the negotiated cipher and exchanged keys to establish an encrypted connection.

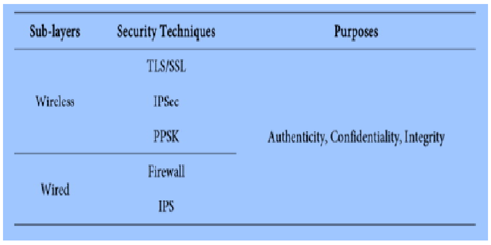
For example; SSL/TLS is developed to encrypt the link in the transport layer, and IP security protocol (IPSec) is developed to keep the network layer secure. They can provide authenticity, confidentiality and integrity in the each layer. Also, using PPSK (Private Pre-Shared Key) for each sensor or device connected to the net- work provides another security measure for IoT system.

Due to the segmentation of multiple types of data, IoT infrastructures will require proper site-to-site encryption. IPsec provides benefits for both remote access and site-to-site connections.Using IPsec in its traditional implementation, where both the IKE control and IPsec data planes are merged, provides no significant benefit over SSL.

The most common type of authentication is PSK (Pre-Shared Key). This type of authentication is what most people use at home. The problem with PSK, while great at home, is it’s challenging to manage in the enterprise. If an employee leaves, you have to change the PSK, and then everyone will have to update the passkey on all of their devices. If you have any IoT devices, you’ll have to change every single one. With an Aerohive Wi-Fi network, there is a better way. It’s called Private Pre-Shared Key (PPSK). PPSK is the perfect technology for when you need the simplicity of PSK with the unique access of 802.1X.

The wired security sub-layer is concerned with devices, which communicate with other devices on the IoT system using wired channels. Common security techniques are applied in wired type networks are firewalls and Intrusion Prevention System (IPS).

Table-4 Security of Network Layer



Sub-layers	Security Techniques	Purposes
Wireless	TLS/SSL IPSec PPSK	Authenticity, Confidentiality, Integrity
Wired	Firewall IPS	

V. CONCLUSION

IoT is an upcoming new technology that has attracted a significant number of re-searchers around the world. There have been major contributions making this technology adapted into our daily life. However, we have a lot of important security issues in IoT and for that we need more research work by the people.

In this paper, security issues of IoT in network layer were reviewed considerably. The important thing is to experiments the security measures in IoT were analyzed and collected under different stages. All kinds of security threats that may be critical in the development and implementation of IoT in different fields have been discussed with respect to the network layers of IoT architecture. Finally, the solutions for these threats is to make some research directions with respect to security concerns have been introduced such as cryptographic mechanisms and firewalls.

REFERENCES

[1] Madakam, S., Ramaswamy, R. and Tripathi, S. (2015) Internet of Things (IoT): A Literature Review. Journal of Computer and Communications , 3, 164-173. https://doi.org/10.4236/jcc.2015.35021

[2] Tyagi, S., Darwish, A. and Khan, M.Y. (2014) Managing Computing Infrastructure for IoT Data. Advances in Internet of Things , 4, 29-35. https://doi.org/10.4236/ait.2014.43005

[3] Gartner Inc. Press Release (2014) http://www.gartner.com/newsroom/id/2905717

[4] Gupta, J., Nayyar, A. and Gupta, P. (2015) Security and Privacy Issues in Internet of Things (IoT). International Journal of Research in Computer Science , 2, 18-22.

[5] Yehia, L., Khedr, A. and Darwish, A. (2015) Hybrid Security Techniques for Inter- net of Things Healthcare Applications. Advances in Internet of Things , 5, 21-25. https://doi.org/10.4236/ait.2015.53004

[6] Arseni, S.C., Halunga, S., Fratu, O., Vulpe, A. and Suciu, G. (2015) Analysis of the Security Solutions Implemented in Current Internet of Things Platforms. IEEE Grid , Cloud & High Performance Computing in Science , Romania, 28-30 October 2015, 1-4. https://doi.org/10.1109/ROLCG.2015.7367416

[7] Chandrakanth, S., Venkatesh, K. and Mahesh, J.U. (2014) Internet of Things. I n- ternational Journal of Innovations & Advancement in Co mputerScience , 3, 8.

[8] Shawish, A. and Salama, M. (2014) Cloud Computing: Paradigms. Inter-Coopera- tive Collective Intelligence: Techniques and Applications, Studies in Computational Intelligence 495, Springer-Verlag, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-35016-0_2

[9] Briseno, M.V., Hirata, F.I., Lopez, J.D.S., Garcia, E.J., Cota, J.N. and Hipolito, J.I.N. (2012) Using RFID/NFC and QR-Code in Mobile Phones to Link the Physical and the Digital World. InTech.https://doi.org/10.5772/37447

[10] Li, B.A. and Yu, J.J. (2011) Research and Application on the Smart Home Based on Component Technologies and Internet of Things. ProcediaEngineering , 15, 2087- 2092. https://doi.org/10.1016/j.proeng.2011.08.390

[11] EnginLeloglu - Journal of Computer and Communications, 2017, 5, 121-136 http://www.scirp.org/journal/jcc R&D Department, Vestel Electronic Inc., Manisa, Turkey

[12] IEC Market Strategy Board (2014) Internet of Things: Wireless Sensor Networks. http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf

[13] Wang, R., Wang, J. and Wang, N. (2015) Analysis of Key Technologies in the Internet of Things. 3 rd International Conference on Material , Mechanical and Manufacturing Engineering , Guangzhou, 27-28 June 2015, 938-941. https://doi.org/10.2991/ic3me-15.2015.180

[14] An, J., Gui, X.L. and He, X. (2012) Study on the Architecture and Key Technologies for Internet of Things. Advances in Biomedical Engineering , 11, 329-335.

[15] Huang, X., Craig, P., Lin, H. and Yan, Z. (2015) SecIoT: A Security Framework for the Internet of Things. Security

and Communication Networks , 9, 3083-3094. https://doi.org/10.1002/sec.1259

[16] Cloud Security Alliance (2015) Security Guidance for Early Adopters of the Internet of Things(IoT).https://downloads.cloudsecurityalliance.org/ whitepapers/Security_Guidance_for_E arly_Adopters_of_the_Internet_of_Things.pdf

[17] Suo, H., Wan, J., Zou, C. and Liu, J. (2012) Security in the Internet of Things: A Re- view. IEEE International Conference on Computer Science and Electronics Eng i- neering , Hangzhou, 23-25 March 2012, 648-651. https://doi.org/10.1