International Journal of Engineering & Technology, 7 (2.7) (2018) 274-276

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A survey on secured internet of things architecture

Ms. U. Harita [1] *, K. V. Daya Sagar [1]

[1] Research Scholar, Dept. of Comp. Sci &Engg Koneru Lakshmaiah Educational Foundation
**Corresponding author E-mail: uharita@gmail.com*

Abstract

The Internet of Things (IoT) introduces an inventive and perceptive of a future Internet where users, computing systems, and everyday items owning sensing and actuating abilities cooperate with unique comfort and financial advantages. Many heterogeneous devices get connected and contribute to the IoT and are known as things. Internet of Things (IoT) enables these things to correspond, compute and make decisions on the network. In such a heterogeneous environment, every user of IoT will have a unique purpose to be served in the form of communication and computation. There is a threat that a malicious user can demolish the security and privacy of the network. Hence any application in the environment of IoT is prone to various attacks and threats. At this point, security becomes a high priority in IoT. To ensure security, care must be taken to guarantee confidentiality, authenticity, data integrity and non-repudiation. In this paper address various conventional techniques for providing security of IoT devices and present analysis of existing solutions for IoT. Firstly, as security will be a fundamental allowing thing of most IoT applications, mechanisms must also be designed to defend communications enabled by such technologies. Later, we identify some suitable security algorithms.

Keywords: *Internet of Things (IoT); Lightweight Algorithms; RFID; Data Encryption; Privacy.*

1. Introduction

The internet of things (IoT) is an interconnection of physical devices and referred to as "Smart devices surrounded with electronics, software, sensors, actuators, and a speaking network functionality that facilitate those objects to gather and exchange information amongst them. The eventual goal is to create "A better World for human beings", by making the objects around us intelligent in a way that they understand our preferences and act accordingly without any human interventions. IoT holds a predominant position in applications such as smart medical services, smart homes, smart cities, smart environment and smart enterprise.

The technological advancements led to an exponential increase in the number of interconnected sensing and computing devices (smart devices a consequence, the number of potential threats and possible effects against security or privacy of things or an individual has grown rigorously. For providing many reliable services, designers stumble upon several challenges, in security-related research areas. The global data company predicts that extra than 2 hundred million devices might be related the world over with the aid of the year 2020, with a very good quantity of these being appliances, there could be a huge possibility for hackers to use these devices for his or her advantage through "Denial of Service" assaults, malicious email different harmful Trojans or worms. A recent HP study document says that on commercialized IoT deployments determined that 80% of IoT devices violate the privacy of personal facts such as call, date of start etc., extra than eighty% didn't require passwords of sufficient length and complexity and 60% had security vulnerabilities in their person interfaces.

Security may be considered because the safety of records from unauthorized interference and assure the confidentiality, integrity, and authenticity of facts.Confidentiality is defensive the records from disclosure to unauthorized people, events or structures. Integrity is described because of the preventions of falsification or statistics amendment by way of intruders. Authenticity refers to the verification of the identity of a device or device. Any protection mechanism needs to be designed to offer confidentiality, Integrity, authentication, and non-repudiation. IEEE and IETF are especially operating in the direction of the layout of communication and protection issues for communique between IoT and the net.

2. Security in IoT devices

HTTP over Secure Socket Layer (SSL) after which its successor Transport Layer Security (TLS). The combination became popular as HTTPS, a protocol for secure communication designed to prevent eavesdropping, tampering, or message forgery using cryptography [1]. HTTP and HTTPS run over the transport layer protocol Transmission Control Protocol (TCP) which is connection-oriented and quite reliable.TCP ensures error protection and flow control for data transmission. These data checking features require additional systems resources to ensure the communication is reliable.

HTTP and HTTPS had been not keen for IoT devices with resource issue and hence there was a need for greater efficient protocol mainly for limited resource gadgets. The Constraint Application Protocol (CoAP) is a specialized application layer protocol layout for aid-constrained devices along with IoT [4]. Like HTTP, CoAP operates using REST techniques and became design so that the two protocols should without difficulty interface with each different [4].Unlike HTTP which typically runs over TCP, CoAP by default runs over UDP, a less complex protocol which 14 required less header information than TCP making it more suitable for constrained devices. UDP by default does not check data transmission for errors and so it is considered an unreliable protocol as a result [4]. Due to the constrained nature of IoT, devices have limited resources and so are limited to which protocols and mechanisms they can support. While these devices may have limited functionality, they may still collect and transmit personal sensitive information

across the internet to web or cloud services. This presents challenges as data being exchanged over the internet is potentially exposed to attack and must be secured [3]. To standardize constrained device communication organizations such as the IETF have developed efficient web standards for constrained devices such as CoAP [4]. Security standards have also been created with the goal of securing IoT data exchange across networks by adapting existing TLS security protocols for constrained devices. The resulting DTLS protocol provides a method for securing data communication in some IoT devices. DTLS protects data confidentiality, integrity, and authenticity of CoAP communications in a comparable way that TLS protects HTTP communication on the web i.e. HTTPS [3] [4]. While suitable for some IoT devices, DTLS is still a heavyweight protocol and so devices must have sufficient resource to run it while still being able to perform the devices intended function e.g. temperature sensor collecting data.

3. Secured IoT architecture

IoT must make sure the security in all its layers. In addition, IoT protection must additionally do not forget the security of entire device crossing the notion layer, community layer, middleware layer, and application layer.

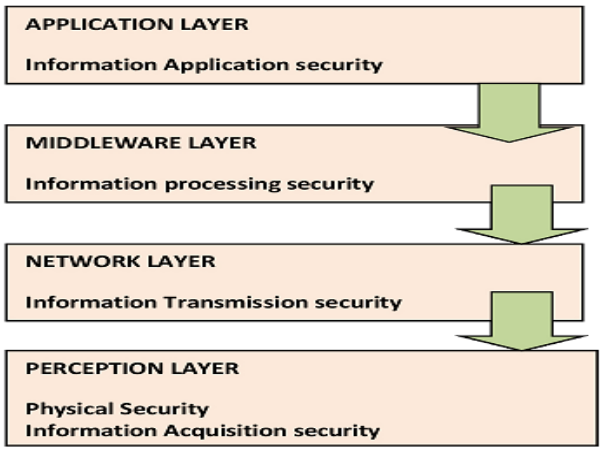

Fig. 1: Secured IoT Architecture.

3.1. Perception layer

i). Physical Security Policy

Being at the bottom, this layer is expected to gather information throughout the IoT network. There arise a lot of issues in terms of security during information collection and physical protection of hardware. Hardware may be like sensors, sensor terminals, and RFID codes. etc.

a) Sensor Network Security Policy

Sensor network technology has barriers inclusive of the physical capture of sensor nodes and gateway nodes, integrity and congestion attacks, DoS assaults, eavesdropping and node replication attacks. To grant a safety framework for the sensor community, regulations together with encryption algorithms, key distribution regulations, intrusion detection mechanisms need to be concerned [1]. Tinysec, LEAP protocol is among the existing security frameworks.

b) RFID security policy

The security issues associated with RFID include leakage of area records of RFID tags and clients, sniffing assaults, man-in-middle attacks, cloning, replay and tampering assaults. In predominant instances, RFID safety has implemented the usage of code mechanisms or a few bodily methods or every so often each. Some of the physical safety techniques are Data encryption, blogger tag, jamming, kill order coverage. Few of the RFID safety protocols are LCAP, Hash Lock, Hash Chain, re-encrypt protocol [1].

c) Sensor Terminals security policy

From the view of the Internet of things, with respect to terminals of sensors, the following issues are to be given priority, SIM information replication, destruction of confidential information, Unauthorized access and imitation of air interface information.

d) Security Policy in Acquisition of Information

Apart from the security problems of the physical security, it is the duty of notion layer to handle problems related to records acquisition protection. Security troubles consisting of Wiretapping, tampering, dishonest, and replay attacks are some of the possible attacks.

3.2. Network layer

a) Information Transmission Security policy

This layer takes the responsibility of transmissions across the network, the vital information. Since IoT is implemented on the basic communication framework, it faces the threat of various attacks like man-in-middle attack, DOS attack, gateway attacks and storage attack. At the community layer, it's far essential to keep authenticity, confidentiality, integrity, and availability of data for the duration of its transmission across the network. Policies such as authentication, intrusion detection and negotiation and key management, can be implemented to make the network invulnerable against the above-mentioned attacks.

3.3. Middleware layer

a) Information Processing Security Policy

It is the obligation of middleware layer for processing statistics and to bridge the gap between the network layer and alertness layer within the IoT layered architecture. Some of the problems are associated with privateness, security, and reliability in the middleware layer. Ensuring confidentiality and safe garage makes the middleware layer extra cozy.

3.4. Application layer

a) Information Application Security Policy

Privacy performs a number one role in the software program layer protection. Access privileges need to be minimal, so you can ensure the unauthorized get right of entry to and usage of records. Data distortion technology and facts encryption technology dealers are building blocks of privateness safety technology that can be relied on for ensuring the privacy of database. [1]. For organizing a tight facts safety, backup and recovery mechanism need to be carried out well. Some of the statistics privacy strategies are TLS, SSL, DNS and many others.,

3.6. Challenges

Challenges can be either focusing on the things or related to the network. Challenges with reference to things are limitations of power, dissimilar platforms, and privacy and various security aspects. Challenges pertaining to the network may be scalability bandwidth issues, and security, privacy that is to be given priority. Another confront is to ensure security, aegis, data trustworthiness, and utilizer confidentiality.

Few more challenges pertaining to IoT system are listed below

- As seen earlier, IoT limits human interventions, which in turn may cause numerous logical and physical attacks.
- Identical Attacks DoS/DDoS, reply attack, eavesdropping rising in wireless sensor networks.
- Another challenge faced is because of the concept of restricted assets or devices in phrases of eating power, confined battery life, bandwidth, hybridous structures, and intricate protection methodologies which can delay the effectiveness of the device.

4. Critical issues

Conventional cryptography algorithms do not make a perfect space in IoT scenario since it has its own boundaries established in terms of power, restricted battery life, execution etc.
Hence light-weight cryptography is considered more companionable to work with within the IoT environment. There exist several lightweight cryptographic algorithms categorized as an asymmetric and uneven set of rules, but the reality that this lightweight algorithm will assure the safety in real-time is still a question left unanswered.
Another fact to be kept in mind is that these algorithms have their own strengths and weaknesses.
For instance, the symmetric algorithms fail to provide authentication whereas asymmetric is known for its bulky key size and demands more memory. This causes hindrances in acquiring and processing of real-time information. Added to that it is expected to utilize more IoT resources, which is wastage.

5. Securied IoT protocols

5.1. Lightweight algorithm using symmetric cryptography

Advanced Encryption Standard (AES) AES is popular in three versions of Rijndael code, which can be AES128, AES192 andAES256. Applied at the software layer and providing a solution in CoAP. The (turning messages into secret code) operation has a 4*4 matrix and a 128bit sized blocks. The internal country is organized by sub-byte, shift-rows, mix-column, and add the spherical key.

5.2. Twine

TWINE works on sixty-four-bit block size and uses a key size of 80-bit and 128-bits. The method of algorithm processing is as follows, sixty-four-bit undeniable textual content of sixty-four bit, and 36 32-bit spherical keys are provided as input that during flip generates a sixty-four- bit ciphertext. In every spherical, 8 F-features carry out simple XOR the plaintext with subkey and applying 4x4 S-Box. Complex permutation and aggregate in twine accelerate diffusion. In TWINE, permutation is the handiest half as many as rounds as the circular shift for an unmarried sub-block distinction to diffuse all sub-blocks. Decryption utilizes the same S-Box, key timetable as encryption but the diffusion layer considered is the inverse of encryption [1]. Full cipher TWINE80 and TWINE128 are prone to biclique attacks [1]. 23-spherical TWINE80 and 25-spherical TWINE128 also go through zero-correlation attacks. Hence,36 rounds for both the important thing sizes are exceptionally endorsed to provide such an acceptable protection enhancement.

5.3. High security and lightweight

It is a block cipher with block period of 64-bit. It has 128-bit key length. It is taken into consideration to be apt for low-aid hardware implementation, which includes an RFID tag or any sensor. HIGHT is composed of simple operations which might be considered as ultra-light, for this reason, it's far believed to be the perfect encryption algorithm. The hardware implementation necessitates 3048 gates on 0.25 μm technology. HIGHT is prone to saturation attack.
5.4. PRESENT: It includes 31 rounds and is predicated on SP Network. PRESENT is a lightweight algorithm that is broadly standard for protection. Its block period is sixty-four bits and it operates on two keys i.e 80 and 128 bits respectively. It utilizes4-bits of entering and the S-box output and receives carried out at the substitution layer.
Table 1 depicts the comparative study of the symmetric algorithms in terms of certain key factors such as #of rounds, key size used, and block size implemented.

Table1: Symmetric Algorithms for IoT

Algo-rithms	Code Length	Struc-ture	# Rounds	Key sizes	Block Size	Attack
AES	2606	SPN	10	128	128	Man, in the Mid-dle
TEA	1140	Feistel	64	128	64	Related Key
HEIGHT	5672	GFS	32	128	64	Satura-tion At-tack
PRE-SENT	936	SPN	32	80	64	Differen-tial At-tack

5.5. RSA

In general, RSA is not considered among the lightweight cryptographic systems due to the usage of large key size. It Makes use of two large prime numbers and performs modulo operation, but since it is good at maintaining the user's privacy and it assures more security, it has become quite popular.

5.6. Elliptic curve cryptography

ECC dominates over RSA for the following benefits it assures to the small location of hardware implementation, the key size is much smaller in ECC, higher processing velocity, and its constrained reminiscence needs. Hence, its consequences in faster computation in the real-time environment. The nodes in 6LoWPAN utilize the ECC algorithm, which may be carried out to constrained devices.

Table 2: Asymmetric Algorithms for IoT

Algorithm	KeySize	Code Length	Attack
RSA	1024	900	Module Attack
ECC	160	8838	Timing attack

6. Conclusion

Though IoT is fast emerging technology and is widely spreading in our day to day life, IoT faces several demanding situations in phrases of electricity, bandwidth, scalability, heterogeneous environment, security, and privacy among which the last are taken into consideration the essential challenges to resolve with a view to maintaining the trust of IoT users. Pre-defined security answers at each layer are nevertheless prone to many assaults. So, cryptographic algorithms are taken into consideration useful to pledge the security. But traditional heavyweight algorithms are considered incorrect for IoT because of their restricted surroundings. Hence, alternate lightweight cryptography solutions symmetric in addition to asymmetric are being applied for entrusting the IoT customers

References

[1] Santhosh Krishna B V, Gnanasekaran T, A Systematic Study of Security Issues in Internet-of-Things (IoT), International conference on I-SMAC (I-SMAC 2017).
[2] Matharu, Gurpreet Singh, Priyanka Upadhyay, & Lalita Chaudhary. "The Internet of Things: Challenges & security issues", 2014 International Conference on Emerging Technologies (ICET), 2014.
[3] Isha and Ashish Kr. Luhach, "Analysis of Lightweight Cryptographic Solutions for the Internet of Things", July 2016, Indian Journal of Science and Technology, Vol 9(28).
[4] Saurabh Singh, Pradip Kumar Sharma, Seo Yeon Moon, Jong Hyuk Park. "Advanced lightweight encryption algorithms for IoT devices: survey, challenges, and solutions", Journal of Ambient Intelligence and Humanized Computing, 2017.
[5] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qiu. "Security of the Internet of Things: perspectives and challenges", Wireless Networks, 2014.
[6] Christos Karamanolis. "Hybrid Cloud Storage", ACM SIGOPS Operating Systems Review, 2017.