International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

IoT & Security

Mr.P.Srinivasa
Lecturer in
Computer Science,
Bhavan's Vivekananda College,
Sainikpuri, Secunderabad.
Telangana, India.

Mr Ch NV Mallikharjuna Rao
Lecturer in Computer
Science,
Bhavan's Vivekananda College,
Sainikpuri, Secunderabad.
Telangana, India.

ABSTRACT:Security is a significant component of IoT operation, IoT security is the attempt of protection, of connected devices and networks in the Internet of things (IoT).The Internet of Things involves the apparent objects and entities known as unique identifiers and the capable of transferring of data over a high speed network. IoT communication is increasing Day to Day life as the increasing no. of Devices with inbuilt Sensors. Protecting and securing IoT devices and the network is a great challenge to administrator IoT network security is a tough task than conventional network security .Here there is are extensive collection of communication protocols, standards, and other devices. One of the solutions to this issue is installing anti--virus and anti--malware software. It is adoptable to have firewalls and other defending systems. Due to increased no. of potential devices, Security is becoming more complex. Security in IoT is also includes authentication. It is a common procedure to identify various users with the location enabled sensors. Authentication includes digital certificates, encryption, and biometric procedures, Generating OTP for every transaction.

Keywords: Iot Security, High Speed Network, Communication Protocols, Sensors, Security Related Problems And Solutions

INTRODUCTION

The Internet of Things (IoT) is, perhaps, the hottest topic in IT. Every organization wants to participate in the IoT, In Iot, as you know, both hardware and software works together. In IOT, Devices connect one another and they interacts using internet
Many devices like

- **MACRO DEVICES**(Computers, laptops, tablets ,high processing and much capability devices)
- **MICRO DEVICES** (mobiles, watches)
- **NANO DEVICES**: single board devices

IoT security is the mechanism of safeguarding all the devices connected. The following devices can be connected in IoT

- Arduino
- Raspberri Pi
- Intel galilieo
- Beagleboard

In IoT , we can depend on the following Communication Protocols

- HTTP
- XBEE
- MQTT
- BLE

- RFID

IoT Top Segments are

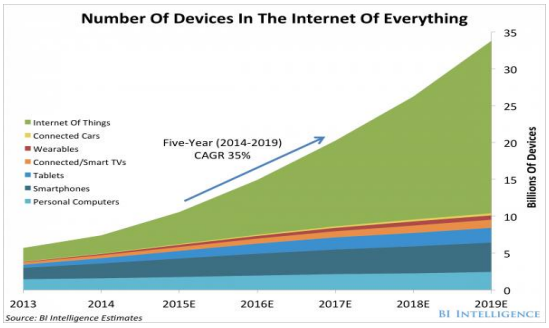
- SMART HOME & Smart Cities
- WEARABLES
- SPORTS
- AUTOMOTIVE,
- LOGISTIC AND HEALTHCARE AND MUCH MORE

Security and privacy are top challenges in IoT

As we know, all these devices and protocol will be connected with sensors. These sensors identify devices when it connected to their network. Because of technology works together devices always, Iot become a successful one. Since many devices connected to internet, identifying them is very important. Besides this, IoT devices need to sense the activity around other devices and technologies.

Year by year , These Devices are increasing , because of smart work done by them.

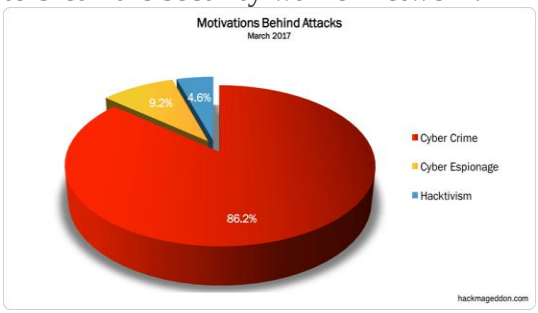
The following image shows the same.



This makes us happy to know that these devices are increasing. This is one side of technology. But other side is to consider privacy and security of data.

Cyber criminals exposed new levels of objectives year by year

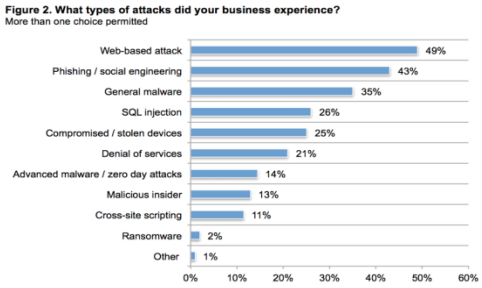
They are following new methods every time to attack on network. Their main intention is to break the security wall of network.



Organizations must pay attention in selecting their suitable technology towards cyber security and privacy. This is not a simple task. This requires analyzing of business, technology, algorithms, data etc.They are concentrating more on security than core business activities.

Logically, this is not a good idea. This will eat much time of organization. So, organization transferring this activity to a third part company, whose job is to provide security to the data exchanged between Iot devices. If they compromise on security, they have to loose hopes on their business. Because of small loop hole in coding, architecture or technology, they could not achieve their targets

Now, Look at the statistics OF CYBER ATTATCKS



Source:
https://www.google.co.in/search?biw=1366&bih=638&tbm=isch&sa=1&q=cyber+attack+statistics+2017&oq=cyber+attack+statistics+&gs_l=psy-

ab.1.1.0l3j0i30k1.1098.1098.0.2198.1.1.0.0.0.0.130.130.0j1.1.0....0...1.1.64.psy-ab..0.1.129.ufKjqd6y4tA#imgrc=OaNSSMgaQDviyM:

Need for this paper: There is a strong Need of this paper as this paper discuss various issues related to security.Although , there are various IoT security issues discussed before, this paper gives immense Iot Solutions to specific problems

Objectives of this paper: : The objectives of this paper is to present various solutions related to IOT security

To deal with security , we must pay attention towards

1. **IoT security**:
2. **IoT authentication**
3. **IoT encryption**
4. **IoT PKI**:
5. **IoT security analytics**
6. **IoT API security**

Protecting and securing these devices is vey important. Actually this is more challenging task than sensing activities of a device. Although, we have many communication protocols, standards, and device capabilities, security is becoming more challenging day to day. Updating anti virus and anti malware soft ware's are important

Since devices can be macro, micro, and nano, identifying devices and users is another challenging task. This process is known as authentication. It is the ability for the user to authenticate their Iot device. It can include

- Password/Pins
- Two-Factor Authentication
- Digital Certificates
- Biometrics

As connected to network, IOT always communicates with networks without human intervention

Another strongest method is encryption. The devices and technologies must use various encryption algorithms. Whenever IOT connect to a network, a secure connection must be created with the help of encryption. It provides maximum solutions to cyber attacks

IoT PKI is fully fledged encryption and decryption method which provides complete X.509 digital certificate and cryptographic key and life-cycle capabilities, including public/private key generation, distribution, management, and revocation

Another job of IOT technology is accumulating, monitoring and alerting user as when needed . This is very important task with IOT devices . For this, It depends on Artificial Intelligence and big Data analytics and machine learning. IOt technology must provide a mechanism to authorize and authenticate the data movement between devices and network

INTRODUCTION TO ENCRYPTION

One of the way to protect messages and sensitive data , is encryption

Encryption: It is a process of converting user data into a different text so that other than intended user, nobody else can guess /understand what is it. This is what we are expecting from Iot. In IoT, a device always in contact with network, it always changes from one to another network.

In encryption, we have diffirent algoritham from very simple to

complex process. They include ceaser cipher, single key ,public private key,DES ,Diffie Helman ,RSA algorithams.

These algorithms are plays at most important role when we connect public medium

In ceaser cipher algoritham, text is divided into lowest alphabets and symbols and replaced by a new alphabet and symbol. It is pre decided by authenticate users.

TYPES OF ENCRYPTION

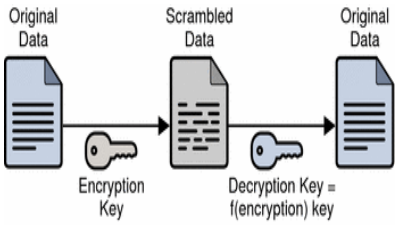
Caesar Cipher with a shift of 3

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Shift: 0

Plain Text: Hello Cipher Text:

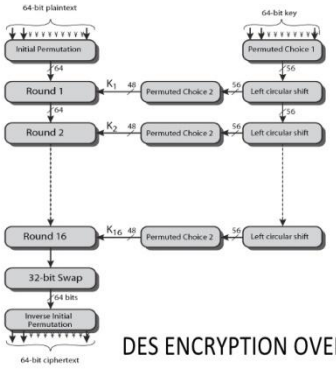
In single encryption, the same key is used for readable and unreadable. Remember, Readable is for converting from decryption to encryption. Unreadable is it's vice versa.



In public private encryption, Intended user sets their own secret keys. One is used to encrypt and other one decrypt. .

In all other encryption, complex mathematical procedures will be used so that, no human being can't decrypt.

DES ENCYPTION:



DES ENCRYPTION OVERVIEW

RSA ALGORITHAM:

Key Generation	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

CONCLUSION

For IoT, Having security over data is very important. Though it is already implemented at various stages, we can upgrade them to have more security.

REFERENCES

1. https://en.wikipedia.org/wiki/Encryption
2. Cryptography and Network Security - Principles and Practice by william stallings
3. https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/gilpress/201 7/03/20/6-hot-internet-of-things-iot-security-technologies/&refURL=https://www.google.co.in/&referrer=https://www.google.co.in/

.