Security Techniques in Internet of Things (IoT)

Article *in* SSRN Electronic Journal · January 2018

Dr Kamna Solanki

Maharshi Dayanand University

Sandeep Dalal

Maharshi Dayanand University

**Security Techniques in Internet of Things (IoT)**

1. **Introduction :**



**Fig. 1- Internet of Things**

It is simply a global network of the things that are uniquely accessible and interlinked on the basis of standard transmission protocols. That change the human life and now we live in a world or era that is fully surrounded by Smart things or what is called the Internet of Things. Smart City, Smart Home, or in the transportation part is autonomus car drive is the real sample of Internet Of Thing (IOT).

"Internet of Things" refers to such a scenario where network connectivity and computing skills are expanding for, sensors, objects, and conventional goods that are not often considered a computer, let this device generate, exchange and spend data with the least human involvement.

This is just a global network of unique things accessible and interrelated based on **standard transmissions protocol.**

1. **Main body:**

**Security Threats in IoT**

There are numerous security threats that emerge on IoT due to

the distinct purposes. Some of the common security threats in

IoT are as follows

1. Vulnerable Web Interface

The network communication modeled in IoT objectauthorizes the user to interact with the object, but concurrently engage an attacker to acquire an unapproved access to the object. The susceptibilities which may result to:

* Acount Recorded
* Cross Site Scriptng ( XSS)
* SQL Injection

1. Inadequate Authentication/Permission A user can acquire advanced levels of access than permitted due to the faulty objects being dwelled to authorize the IoT user interface or imperfect authorization tools, which leads to the initiation of these threats

* Absence of code word Complication
* Badly Protected Ids

1. Vulnerable Network Services

A trespasser acquires informal authorization to the object or associated information by employing the liabilities for the services of network for accessing the object, which leads to this threat.

1. Deficiency of Transport Encryption

This threat primarily associates with the data in an unencrypted composition that is being transacted among the IoT objects.

* Inadequately used SSL/TLS
* Services being unencrypted via Internet

1. Privacy Involvement

The acquisition for particular data with the requirement of an appropriate protection to the data leads to the emergence of Privacy concerns

1. Susceptible Cloud Interface

This threat primarily correlates with the matters that are linked to interface of cloud employed for interacting with IoT objects

1. Vulnerable Mobile Interface

This threat is quite similar to the preceding threat, i.e. the attacker procures an access to the object or crucial data for IoT device which employs the interface of vulnerable mobile for user alliance because of the ineffective authentication or unencrypted data flows.

1. Poor Security Configurability

When users of the IoT objects holds poor or not any experience to revise its security restraints then Poor security configurability exists. The configuration of poor security is possible as the object network interface left negative options for producing rough user authorization, like, inflicting utilization of tough passwords.

* Nonexistence of the options of Password Security

1. Vulnerable Software/Firmware

The lack of expertise for an object to be reorganized exhibits a security weakness on its own. IoT objects must hold the expertise to be rearranged while the weaknesses are revealed with the updates of software/firmware that could be unpredictable while the efficient record itself plus the arrangement of network being executed. Software may be problematic if the holding of hardcoded obscure data, for instance, IDs [20] takes place. The unsuccessful attempt of software/firmware for being updated indicates that the object endures vulnerabilities to the security dilemma that the update is designed to inscribe.

***The use of biometrics as a safeguard for IoT***

Biometric-based approaches has recently emerged as the

utmost capable method for distinguishing people, as a

replacement for verification of an individual and allowing them

the access to dynamic or virtual domains on the basis of the

alphanumeric passwords, PINs, smart cards, tokens, keys etc.



Biometric technology is primarily employed for the automatic recognition of the human beings on the basis of their physiological attributes or behavioral characteristics.

The use of passwords, keys, tokens are things that might be a security hole to be “hacked, modified, or forgotten”

The application of biometric techniques is safer and more perfect than old school techniques, because :

1. Uniqueness: The biometric characteristics physical or logical are constantly unique for every single human being.
2. Cannot be shared: As biometric asset is an innate property of an individual, it is tremendously hard to replica or share
3. Cannot be forged: Biometric features of a distinct human being are nearly impossible to forget or deceit,.
4. Cannot be lost: As the biometric features are innate and unique assets of an individual and in contrast to passwords, PIN, tokens, etc., they are not mandatory to be recalled. A biometric asset of an individual can only be misplaced in the event of serious accident.
5. More efficient: Biometric verification is an effective method to verify the human identity because the biometrics of an individual human beings cannot be imitated

***Face Recognition System***

The human face is the easiest feature that can be employed in the security system based on biometrics in order to recognize a person. The system involving face recognition is designed to offer a precise and constant mode for identifying the face of an individual human being, Face recognition is among the few biometric techniques that hold the qualities of both extraordinary accuracy and low intrusiveness.

***Steps of Face Recognition system***

 Image Pre-processing

In this step, initially the face images are pre-processed and enhanced in order for enhancing image quality by removing the noises and redundancies from the input image.

 Face Detection

This procedure is the process of face extraction by means of input image.

 Feature Extraction

Facial feature extraction is the process of translating the input data into some set of features. The feature points like eyes, nose, mouth is extracted and afterwards employed as input data to application. As soon as, the face is spotted from the input image, the feature extraction from the face will take place. In feature extraction, a mathematical illustration termed as

biometric template or biometric reference is created, which is

kept in the database and this will form the basis of any recognition task.

 Classification

The final output after the classification is then matched with the template or the image stored in the database with the help of a matching algorithm

**Conclusion**

In this paper, the main focus is placed on security of the Internet of Things for avoiding the intrusion attacks having a trespasser gain access by hacking the accounts due to insecure authorization and significant or confidential information gets

compromised. **Due to the inefficiency of the traditional approaches like security through PIN, Passwords, Tokens, etc.** that are easily faked, forgotten or lost, biometric based security is considered in this paper, as it is the strongest and most fool proof physical security technique used for identity verification.

An individual's body characteristics are pre-stored in a biometric security system or scanner, which may be accessed by authorized personnel. Biometric characteristics includes fingerprint, voice, Iris, hand geometry, palmprint, signature, face, gait, etc.

Note :

**Our review is not include to implementation biometrik as a security of IoT**