International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

Secure Voice Based Authentication for Future IOT Applications

[1] Mr.K.Ravi kishore [2] Dr.M.Humera Khanam, [3] Ms.D.Sucharitha, [4] Ms.G.Divya
[1][2]Dept. of CSE, S.V.University, Tirupati,

Abstract - **Internet of Things (IOT) is a network of all devices that can be accessed through the internet. Using existing network infrastructure, the devices can be remotely accessed and controlled, thus allowing a direct integration of computing systems with the physical world. It also reduces human involvement along with improving accuracy, efficiency and resulting in economic benefit. The IOT devices facilitate the day to day life of people. However, due to its heterogeneous and dynamic nature the IOT has an enormous threat to security and privacy in IOT environment the Authentication is one of the most challenging security requirement, where a user can directly access information from the devices, provided the mutual authentication between user and devices happens. A system that recognizes and authenticates the voice of a user by extracting the distinct features of their voice samples is usually termed as Voice recognition system. Converting the human voice into digital data can be carried out by Voice identification. The digitized audio samples then undergo feature excerption process to extract Mel Frequency Cepstral Coefficients (MFCC) features. These coefficients are subjected to feature matching through Dynamic Time Warping (DTW) to match with the patterns existing in the database for limited language words. In this paper we provide the IOT applications to the voice based authentication by providing a natural language processing interface. For better performance we can combine the digital and mathematical knowledge using MFCC and DTW to extract and match the features to improve the accuracy.**

Keywords:— **MFCC (Mel Frequency cepstral coefficients), DTW (Dynamic Time Warping)**

I. INTRODUCTION

Voice based authentication is also known as speech recognition authentication. IOT provides us a way to exchange data between devices using internet. These devices are equipped with processing and communication technologies and locatable through IP addresses. The main focus here is to combine the computer systems and physical world for economic saving and to improve consistency and completeness while reduce in human involvement. The connectivity provided should be machine to machine communication covering various protocols and applications interconnecting systems, services. While spreading access to information, IOT has an threat to security and privacy due to its non-homogeneity and dynamic nature .cyber attacks would be change from wearable devices. Although we have effective signature schemes for IOT devices, we required another level of security. Employing effective voice based authentication to protect privacy, is required.

A. Models for the system

In this paper we used two models they are

1. IOT Authentication model:

IoT authentication model shown in the following Fig.1 we consider four scenarios smart pill boxes, heart beat sensor weight scales and blood pressure. These devices facilitate people to day to day life. In the given scenario all smart devices are connected through internet gateway. Different type of people can access the data of relative devices through gateways. Here authentication is between user and device is provided through gateways.

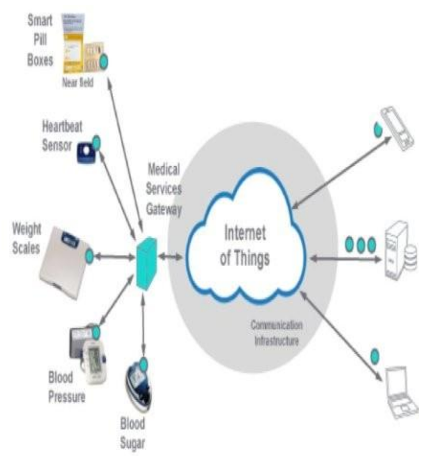

Fig.1

2. *Model for threat*

The process by which potential threats can be identified is known as Threat modeling. These threats can be enumerated, prioritized from hypothetical attacker's point of view. The purpose of symmetric analysis of the probable attackers profile is provided by threat modeling. Where the highest value assets can be answered by threat modeling.

B. Methodologies

- IOT Authentication model is presented and its requirements are discussed.
- A secure voice based authentication is proposed to address the security challenges.
- By using BAN (Burrows-Abadi-Needham) logic and an informal security analysis have been used to prove the system is secure.
- By AVISPA (Automated validation of internet security protocols and applications) tool for the verification of security schemes simulation is done.
- We provide a multi lingual interface for natural understanding of languages..

II. MATHEMATICAL PRELIMINARIES

In this section, we briefly discuss the properties of an elliptic curve over a finite field.
A. Suppose a ∈ Zp and b ∈ Zp be two constants, where Zp = {0, 1, . . . , p−1} and p > 3 is a prime. A non-singular elliptic curve y 2 = x 3 + ax + b over the finite
field GF (p) is the set Ep (a, b) of the solutions (x, y) ∈ Zp ×
Zp to the congruence
B. y 2 ≡ x 3 + ax + b (mod p),
C. where a, b ∈ Zp such that 4a 3 + 27b 2 6= 0 (mod p), with a point at infinity or zero point O.
Let P = (xP, yP) ∈ Ep (a, b) and Q = (xQ, yQ) ∈ Ep (a, b) be two points. Then xQ = xP and yQ = −yP when P +Q = O. Q
= −P ∈ Ep (a, b) is called the inverse of P ∈ Ep(a, b). Also, P
+ O = O + P = P, for all P ∈ Ep (a, b). Hasse's theorem states
that the number of points on curves Ep (a, b), denoted as #E,
satisfies the following inequality [6]:
p + 1 − 2 √ p ≤ #E ≤ p + 1 + 2√ p.
In other words, there are about p points on an elliptic curve
Ep (a, b). In addition, Ep (a, b) forms a commutative or an
abelian group under addition modulo p operation with O as
the additive identity and −P ∈ Ep (a, b) as the additive inverse
of the point P ∈ Ep (a, b).
A. Elliptic Curve Point Addition
Suppose G is the base point on Ep (a, b) with order n, that is,
nG = G+G+ . . . +G (n times) = O. Let P, Q ∈ Ep (a, b) be two
points on the elliptic curve. Then, R = (xR, yR) = P +Q is calculated as follows [6]:
xR = (λ 2 − xP − xQ) (mod p),
yR = (λ(xP − xR) − yP) (mod p),
Where
λ = (yQ−yP xQ−xP (mod p), if P 6= Q 3xP 2+a 2yP (mod
p), if P = Q.
B. Elliptic Curve Point Scalar Multiplication
The elliptic curve multiplication is done as repeated additions. For example, 5P = P + P + P + P + P where P ∈ Ep
(a, b).

III CHALLENGES FOR SECURITY AND IOT APPLICATIONS REQUIREMENTS

As accessibility and global connectivity or requirements of IoT application, it increases avenues of threats and attacks. The non-homogeneous nature of IoT further raises constraint in the development of mechanisms for security. Possible constraints it also be taken while developing techniques
Security: System components can prone to sudden failures and security is required to reduce corrupting capabilities Identification and Authorization: Privacy and Security access can be ensured through this. Global access in IoT could have permanent and temporary identities.

Reliability: It guarantees information availability while managing data storage. Providing duplication among communication channels through several paths is one way to ensure availability.

Responsibility: Also known as access control it provides legitimate accessing to services by defining privacy conditions.

Privacy: Privacy is very important concept in IoT there are following areas where privacy as to be provided, in the cases of data sharing and management, data collection and data security.

IFERP connecting engineers... developing research

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

IV PROPOSED SYSTEM

Here we present a new speech based authentication establishment scheme for IoT applications provided in Fig: 1 As shown in the above Fig users communicate with each other with various devices through gateways to provide secure communication. The proposed system applied to all kind of IoT applications.

This system consists of following phases namely

1. Setting up the system
2. Device sensing registration
3. Registration for user through speech
4. Login through speech
5. Authentication
6. Password and Biometric update
7. Revocation of Smart card
8. Sensing device addition dynamically

D. Setting up the system:

System setup is done by gateways as follows

First Phase: GW N chooses a non-singular elliptic curve Ep over a prime finite field Zp, p being a large prime. GW N then selects a base point P of order n over Ep such that n.P = O, where O is called the point at infinity or zero point. GW N also chooses its private key dGW N and computes the corresponding public key QGW N = dGW N .P.

Second Phase: GW N then chooses a collision-resistant one way cryptographic hash function h (•). Third Phase: For biometric authentication, GW N uses the following two fuzzy extractor functions: − Gen: It is a probabilistic generation function that takes as input the user personal biometrics Bioi , and returns σi ∈ {0, 1} l that is the biometric key of length l bits and τi that is a public reproduction parameter. − Rep: It is a deterministic function to be used during authentication. The input is the user biometrics, say Bio0 and τi, provided the hamming distance between Bio0 and the original previously entered biometrics Bioi is less than t, where t is an error tolerance threshold value. The output is the original biometric key σi, that is, σi = Rep (Bio0 i, τi). • Step S4. Finally, the system parameters {Ep (a, b), p, P, h (•), QGW N, Gen (•), Rep (•), t} are made public, whereas dGW N is kept secret by GW N.

B. Sensing Device Registration Phase:

All the sensing devices in IoT are registered offline by the GW N as follows.

• Step SD1. For each device SDj, the GW N chooses a unique identity IDj and a unique private key dj, and calculates the corresponding public key Qj = dj .P. It further computes RIDj = h (IDj k dj).

• Step SD2. The GW N pre-loads {IDj, dj, RIDj} in the memory of SDj. Furthermore, the GW N stores {IDj, RIDj, Qj} in its database, and then makes Qj as public.

C.User Registration Phrase through speech:A user Ui registers with the GW N by executing the following steps:

• Step R1. Ui chooses a unique IDi, a unique private key di and calculates the corresponding public key Qi = di .P. Ui sends registration request message with RIDi = h (IDi k di) to GW N via a secure channel

• Step R2. GW N computes RI = h (RIDi k dGW N), stores it on smart card SCi and sends it to Ui via a secure channel.

D. Login Phase through speech

Ui executes the following steps to login to the GW N:

• Step L1. After inserting SCi, Ui enters his/her identity ID0 i and password PW0 i, and also imprints biometrics Bio0 i at the sensor of a specific terminal.

• Step L2. SCi then computes σ 0 i = Rep(Bio0 i , τi), d 0 i =d ∗ i ⊕ h(ID0 i ⊕ σ 0 i) and RPW0 i = h(PW0 i k ID0 i k d 0i k σ 0 i), and checks if RPW0 i = RPWi holds.

E.Authentication and Key Agreement Phase

In this phase, the GW N validates Ui and helps in establishing a session key between an accessed sensing device SDj and a legal user Ui with the help of the following steps: • Step A1. After receiving the login message from Ui at the time T 0 i , the GW N first checks the validity of timestamp by the condition T 0 i− Ti ≤ ∆T. If it is valid, the GW N then calculates NGW N = dGW N .Ai = ((NGW N)x,(NGW N)y), RID∗ i = DID0 i ⊕ (NGW N)y, ID∗ j = DID0 j ⊕(NGW N)y, Ri = h(RID∗ i k dGW N), V ∗ i = h(ID∗ j k Ti kNGW N k Ri).

F.Password and Biometric Update Phase

Ui executes this phase internally without involving the GW N to reduce overhead as follows

: • Step PB1. Ui enters his/her identity IDi, current password PWold i and imprints current biometrics Bioold i at the sensor of a specific terminal. SCi then computes σ old i =

Rep(Bioold i , τi), d 0 i = d ∗ i ⊕ h(IDi k σ old i), R 0 i = R ∗

i ⊕ h(IDi ||PWold i ||σ old i), RPWold i = h(PWold i k d 0 i k

IDi k σ old i). SCi checks if RPWold i = RPWi and the

request is terminated if the verification is not successful.

G.Smart Card Revocation Phase

If the smart card SCi of a legitimate user Ui is lost, the following steps can be executed for requesting a new one: • Step RV1. Ui creates a registration request message with the same IDi and new private key d new i as RID new i = h (d new i k IDi) and sends it to the GW N via a secure channel. H. Dynamic Sensing Device Addition Phase

Dynamic sensing device addition is necessary as some devices may be physically compromised by an attacker and we need to deploy some new devices in the network. Suppose a new sensing device SDnew j is to be deployed in the network. The GW N then performs the following steps offline: • Step DSD1. The GW N chooses a unique identity IDnew j and a unique private key d new j , and calculates the corresponding public key New j = d new j .P. It further computes RID new j = h(IDnew j k d new j).

REFERENCES

[1] P. Rohatgi, “A Compact and Fast Hybrid Signature Scheme for Multicast Packet Authentication,” in 6th ACM Conference on Computer and Communications Security, New York, NY, USA, 1999, pp. 93–100.

[2] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, “A Dynamic password-based user authentication scheme for Hierarchical wireless sensor networks,” Journal of Network and Computer Applications, vol. 35, no. 5, pp. 1646–1656, 2012.

[3] M. Turkanovi, B. Brume, and M. Holbl, “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, vol. 20, pp. 96 – 112, 2014.

[4] Secure Hash Standard, FIPS PUB 180-1, and National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995.