Security and Privacy of Internet of Things

Taran Singh Bharati

Abstract: Today in many fields, work is being carried out without human interventions. In place of humans, devices like sensors, cameras, wireless networks, etc. are installed in different locations and they collect the information throughout day and night and transmit the information at regular interval of time to their control rooms where the information is processed and analysed for predicting about special unusual incidents to be taken place in near future. Such collection of sensor devices makes internet of things (IoT) network possible. Since these devices are remain unattended and uncovered therefore there are many issues regarding their nature and their working. The focus of this paper is on the IoT and their security and privacy issues by inserting a separate layer which employs the message authentication and server authentication in distributed environment, in the IoT architecture to enhance the security and privacy of IoT. This paper also elaborates the techniques, architecture and the position of the security and privacy layer as a sandwich layer in the architecture of IoT.

Index Terms: IoT, Trust, Security, Threats, Attacks, Authentication Protocols

I. INTRODUCTION

Today we are capable enough of getting the information about, temperature, storm, about any tough terrain, availability of power supply, smart grid, healthcare, about soil, for resource exploration, etc. well ahead of time than before because of the availability of the internet of things network. Timely getting the information makes public and civic authorities aware about the incidents to be occurred so as to minimize the loss of lives and the other property losses. The internet of things (IoT) is a network formed by connecting the sensor devices, WSN, RFID, and other technologies as nodes together by the internet. These nodes sense data throughout the day and send the data to master control rooms where data is analysed for making sure about the unusual incidents i.e. raining, cyclones, cold wave, heat wave, etc., very quickly and very early so that alert can be announced timely. Timely alert announcement can save the loss of lives and property damages around. Security gives the feeling of protection from intrusions and attacks to keep the data secure and fresh. It is provided in the form of authentication, access control confidentiality, non-repudiation, and integrity. Security mechanisms are functions or procedures to provide the security services i.e. encryption, identity cards, thumb impression, digital signature [16]-[22] etc. Some security requirements are as:

- Network Security: availability, confidentiality, authenticity
- Identity Management: accountability, authentication, revocation, and authorization
- Privacy: data privacy, pseudonimity, anonymity, unlinkability
- Trust: entity trust, data trust, device trust
- Resilience: resilience against failures, robustness against attacks

The IoT devices are nature uncontrolled environment, mobility, physical accessibility, and trust [1]. Therefore IoT devices face the security requirements i.e. network security identity management, trust, privacy, and resilience. The characteristics of IoT devices existas comprehensive perception, reliable transmission, and intelligent processing [2].

There are the technologies which make IoT possible i.e. radio frequency identification (RFID)- to automatically identify the source; Wireless sensor networks (WSNs)- collection of sensors which is a category of adhoc networks; Cloud and fog computing- services, software, hardware, and services can be hired on demand and paid according to their usage, so this framework is called cloud computing; middleware- to hide the complexities of technologies to enable communication simple; application software- for developing application for industry; merging of RFID and WSN- for making IoT more industry oriented. The development of the technologies lists the journey of evolution (Table1).

Table: Evolution of Technologies

<table>
<thead>
<tr>
<th>From</th>
<th>Technology</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>1999</td>
<td>RFID</td>
<td>RFID tag, ISO 11785, etc.</td>
</tr>
<tr>
<td>2005</td>
<td>WSN</td>
<td>ISO/IEC JTC1 SC31, sensor interface</td>
</tr>
<tr>
<td>2012</td>
<td>Smart things</td>
<td>payment smart card</td>
</tr>
<tr>
<td>2017</td>
<td>QoS</td>
<td>ITU-T, IETF</td>
</tr>
</tbody>
</table>

II. RELATED PREVIOUS WORK

A. Security Architectures, Requirements, Security Challenges, And Solutions

Revised Manuscript Received on June 05, 2019
Taran Singh Bharati, Department of Computer Science, Jamia Millia Islamia, New Delhi, India.

Retrieved Number: H69400985819/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering & Sciences Publication
Security and Privacy of Internet of Things

IoT architectures are listed in literature [1]. IoT-A (internet of things architecture)- reference model uses views and perspectives to suggest architecture generation; (BeTaaS) Building the environment for the things as a service):- machine to machine architecture for running on local cloud gateways; (OpenIoT) Open source cloud solution for the internet of things):- this reference model focuses on cloud based middleware infrastructure for on demand access of IoT services; IoT@ work (Internet of things at work):- established for industry applications.

Ubiquitous, mobile, constraint, unattended, myriad, interdependence, diversity, intimacy are features of IoT which affect the privacy and security of IoT. There are some threat, challenges, and opportunities to these features [3], [5] i.e. interdependence- static defence, privilege, access control, permission based on context; diversity- protocol of insecurity, fragmented, simulation platform; constraint- insecure system, lightweight protocol, merging, and physical systems; Myriad- botnet, DDoS, intrusion detection and prevention, IDS; unattended- remote attack, verification, attestation lightweight trusted execution; Intimacy- privacy leak, protection, encryption, anonymous protocol; mobile-malware, identification, configuration; ubiquitous- insecure configuration, consciousness.

There are four levels in IoT architecture [4], [6], [7] with features i.e. transportation, environment monitoring, cloud computing, data analytics communication, sensors, and jammers. The attacks, vulnerabilities, threats, and their solutions [9]-[15] are summarized in Table2.

Table2: Architecture levels, security requirements, challenges, and solutions

<table>
<thead>
<tr>
<th>Layer</th>
<th>Features</th>
<th>Security Requirements</th>
<th>Security Challenges</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Layer</td>
<td>Personalize Information</td>
<td>Authentication, Key</td>
<td>Ddos ,Sniffers/Loggers, Session Hijacking, Injection</td>
<td>Authentication, Selected, IPS,</td>
</tr>
<tr>
<td></td>
<td>Service Transportation, Environment Monitoring,</td>
<td>Management, Privacy,</td>
<td>Social Engineering etc.</td>
<td>Disclosure, IDS, Verification, Data</td>
</tr>
<tr>
<td></td>
<td>Medical Applications</td>
<td></td>
<td></td>
<td>Encryption, Access Control List,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Firewall, Antivirus, Session Inspection</td>
</tr>
<tr>
<td>Support Layer</td>
<td>Intelligent and Cloud Computing, Data Storage,</td>
<td>Cloud Computing, Anti-</td>
<td>Data Tampering, Dos, Unauthorized Access</td>
<td>Encryption, Access Control</td>
</tr>
<tr>
<td></td>
<td>Data Analytics</td>
<td>Virus, Multi-Party</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Computing(Secure)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Layer</td>
<td>2G/3G Communication Protocol, TV, Satellite and</td>
<td>Encryption, Communication</td>
<td>Sybil, Selective Forwarding, Sinkhole, Wormhole etc.</td>
<td>TSL/SSL, IPSec, Firewall, IPS etc.</td>
</tr>
<tr>
<td></td>
<td>Mobile networks,</td>
<td>Security, Anti-Doss, Identity Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agreement, Light Weight</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encryption</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

III. PROPOSED WORK

Data is collected at monitoring site from various sensors i.e. surveillance, CCTV cameras installed at different locations in city, pollution, traffic, health, soil, satellite, radiation monitoring sites, terrain etc. Tests are then conducted to make sure the authenticity, integrity, freshness, and validity of the collected data. Since data is collected from different heterogeneous locations or sensors and therefore data may is unstructured. There are some security and privacy issues [15] in IoT; object identification, authentication and authorization, lightweight cryptosystem, vulnerabilities, malware etc. as shown in table1. So the data needs to be pre-processed i.e. noise removing, cleansing, transformation etc. Now data has been transformed into the suitable form hence it is sent to data analytics centre for further processing. At data analytics centre data is analysed to predict some unusual incidents. If some unusual features are predicted, advisory alert note is issued through the advisory announcement section, as shown in below figure 1.

Figure1: Position of Security and Privacy in IoT

Security and privacy layer of architecture is separated and it is shown separately in figure2. For authentication Needham-Shroeder, Deng, and Loo protocols proposed.
For confidentiality we use symmetric and public key encryption algorithms, AES and DES are symmetric cryptosystems while RSA ECC and DH are public crypto systems. Digital signature and message authentication code (MAC) are used for message authentication. Passwords at various levels are needed for access control in distributed computing. Kerberos protocol is used for access control. After receiving or after sending the message party would not able to deny its operation done.

Authentication Protocols, Needham Shroeder, Dening, Woo Protocols
Confidentiality, DES, AES, RSA, ECC, DH methods
Integrity, Signature, MAC, Encryption
Access Control, Passwords
Non-repudiation, digital signature
Availability DoS

Figure 2: Expansion of Privacy and Security layer of IoT

B. Authentication Protocols

There are two types of authentications [23] one is direct authentication in which both parties make sure that they communicate to intended parties. Another method is arbiter method in which, parties make sure the identities of each other through trusted third party (TTP) which is also called authentication server (AS). Trusted third party shares a common secret key with every party. This process has some requirements that; clocks must be perfectly synchronized and there must not be a supress-replay attack. There are the authentication protocols in both symmetric and public key encryption methods like Needham-Shroeder, Dening, Woo and Lam.

Needham-Schroeder’s Protocol: It is mutual, symmetric authentication protocol and free from suppressed-reply attack and its steps of message exchanges are specified below where A, B, id, nonce, K_a, PU, PR, T, AUTH represent sender, destination, identification, random number nonce, session key, public key portion, private key portion, time-stamp, authority:

A→B : id (A) || nonce_a
B→TTP : id (B) || nonce_b||E (K_s, [id (A) || nonce_a] T_b)
TTP→A : E (K_s, [id (B) || nonce_b] [K_s][T_b]) || E (K_s, [id (A) ||K_s][T_a]) || nonce_b
A→B : E (K_s, [id (A) ||K_s][T_a]) || E (K_s||nonce_b)

Woo and Lam Protocol: It is the improved version of itself which requires clock synchronization and stated as under:

A→TTP : id (A) || id (B)
TTP→A : E (PR_auth, [id (B) ||PU_b])
A→B : E (PU_a, [id (A) || nonce_a])
B→TTP : id (A) || id (B) || E (PU_auth, nonce_a)
TP→B : E (PR_auth, [id (A) ||PU_a]) || E (PU_b, E(PR_auth, [nonce_a] ||K_s) || id (A) || id (B))
B→A : E (PU_a, E (PR_auth, [nonce_a] ||K_s) || id (A) || id (B)) || nonce_a
A→B : E (K_s, nonce_a)

C. Server Authentication

This protocol is used to authenticate the servers in distributed environment. This uses the symmetric key encryption and client server architecture. Here total network is divided into realms or regions and every region has its own authentication and ticket granting servers and many clients. There is a database which stores userIDs and passwords of in realms. Kerberos server shares keys with all authentication server (AS). Its steps of working:

i) User enters login ID and password to authentication server (AS)
ii) This gives the ticket for the ticket granting server (TGS)
iii) This ticket is used to interact with the AS of remote realm.

The protocol is sketched as (Kerberos v4) where C, AS, TGS_{rem, v_{rem}} represent client, authentication server, remote ticket granting server, and remote server to be accessed.

C→AS : id_c || id_{sp} || TS_1
AS→C : E(K_{c,sp}||id_{sp}||TS_1)
lifetime_c || Ticket_{sp}
C→TGS_{rem} : id_{trem} || Ticket_{sp} || Authenticator_c
TGS→C : E(K_{c,trem}||K_{c,sp}||id_{sp}||TS_1)
Ticket_{sp}
C→TGS_{rem} : id_{trem} || Ticket_{sp} || Authenticator_c
TGS_{rem}→C : E(K_{c,trem}||K_{c,vrem}||id_{vrem}||TS_0)
Ticket_{vrem}
C→v_{rem} : Ticket_{vrem} || Authenticator_c

IV. Results Analysis and Performance Measuring

If any client needs the services of any server of any realm, ticket to access the remote server is needed which in turn, can be obtained through authentication server and ticket granting server by exchanging messages as listed in Kerberos protocol. For N realms it requires N (N-1)/2 messages because every realm is connected with all other realms and every server has different key.
In Kerberos version v4, among N realms interoperability needs N^2 Kerberos-Kerberos relationships.

MSB or LSB are used for message byte ordering and here no credit is forwarded to other hosts. Lifetime is encoded in the groups of 8 bits of 5 minutes. Therefore the maximum time would be 2^5×5 = 1280 minutes.

I. CONCLUSIONS

This paper provides the insights of IoT features and characteristics. It also focuses on the security and privacy requirements, challenges and their solutions, and their analyses of IoT. In the architecture of IoT, a new separate layer is inserted which is fully dedicated to security and privacy of the IoT. This layer is proposed to make use of authentication protocols to enhance the security of IoT. The Needham-Shroeder, Woo and Lam authentication protocols are proposed which are free from suppressed attacks’ like contaminations and Kerberos version v4 for server authentication in distributed environment are proposed. Results are performance is measured, analysed empirically.

REFERENCES


Author Profile

Author is B.Tech, Master of Engineering, and Ph.D. in Computer Science Stream from Kanpur, Gwalior, and New Delhi respectively. He has more than 18 years of experience at the time of writing this paper. He has served at different positions in various universities and Engineering Colleges. His area of interests includes Security, Theoretical Computer Science, Data Science, IoT, Big Data, etc.