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 privacyissues by inserting a separate layer which employs the message authentication and server authentication in distributed environment, in the IoTarchitecture 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 timethan 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 networkis 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

From	Technology	Standard
1999	RFID	RFID tag, ISO 11785, etc.
2005	WSN	ISO/IEC JTCI SC31, sensor interface
2012	Smart things	payment smart card
2017	QoS	ITU-T, IETF

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, JamiaMilliaIslamia, New Delhi, India.

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 is 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.

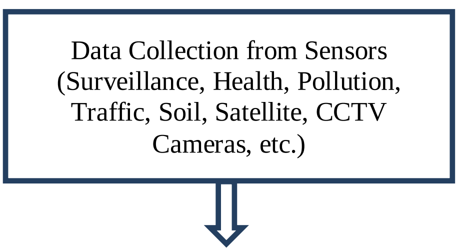
Table2: Architecture levels, security requirements, challenges, and solutions

Layer	Features	Security Requirements	Security Challenges	Solutions
Application Layer	Personalize Information Service Transportation, Environment Monitoring, Medical Applications	Authentication,Key Management, Privacy,	Ddos ,Sniffers/Loggers, Session Hijacking, Injection Social Engineering etc.	Authentication, Selected, IPS, Disclosure, IDS, Verification, Data Encryption, Access Control List, Firewall, Antivirus, Session Inspection
Support Layer	Intelligent and Cloud Computing, Data Storage, Data Analytics	Cloud Computing, Ani-Virus, Multi-Party Computing(Secure)	Data Tampering, Dos, Unauthorized Access	Encryption, Access Control
Network Layer	2G/3G Communication Protocol, TV, Satellite and Mobile networks,	Encryption, Communication Security, Anti-Doss, Identity Authentication	Sybil, Selective Forwarding, Sinkhole, Wormhole etc.	TSL/SSL, IPSec, Firewall, IPS etc.
Perception Layer	RFID, Sensors, Jammers, PDoS and GPS	Sensor Data Protection, Key Agreement, Light Weight Encryption	Spoofing, Jamming, PDOS, Eavesdropping, Node Outage	Cryptography, Steganography, Authentication, Authorizationetc.

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.

.



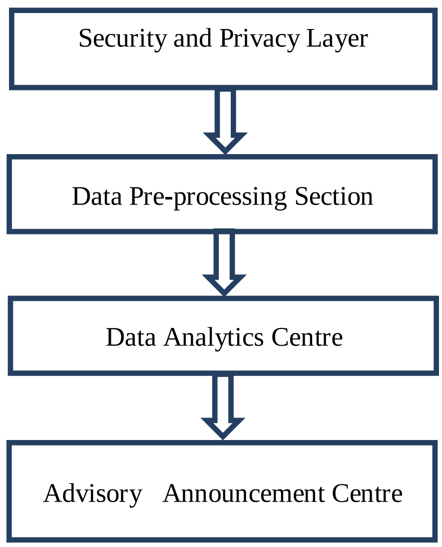


Figure1: Position of Security and Privacy in IoT

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.

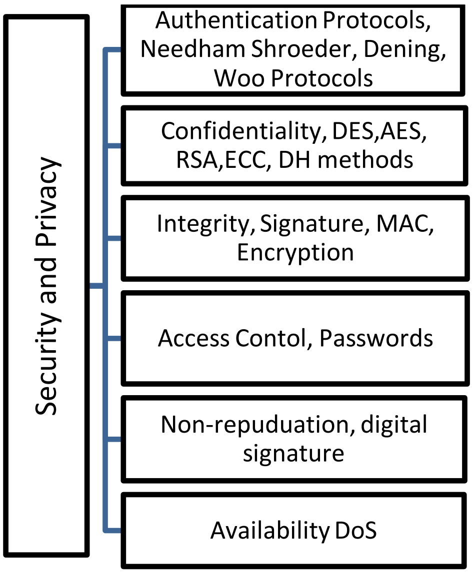


Figure 2: Expansion of Privacy and Security layer of IoT

B. Authentication Protocols

There aretwo 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. For this process there are 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_s, 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_b, [id (A) ||$nonce_a$|| T_b])

TTP→A : E (K_a, [id (B) ||$nonce_a$||K_s||Tb]) ||E (K_b, [id (A) ||K_s||T_b]) ||$nonce_b$

A→B : E (K_b, [id (A||K_s||T_b]) || 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_b, [id(A||$nonce_a$])

B→TTP: id (A) || id (B) || E (PU_{auth}, $nonce_a$)

TP→B : E (PR_{auth}, [id (A) ||PUa]) ||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)] || $nonce_b$)

A→B : E (K_s, $nonce_b$)

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)s. 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_{tgs}||TS_1

AS→C :E(K_c,[$K_{c,tgs}$||id_{tgs}||TS_2|| $lifetime_2$||$Ticket_{tgs}$])

C→TGS_{rem} : id_{tgsrem}||$Ticket_{tgs}$|| $Authenticator_c$

TGS→ C : E ($K_{c,tgs}$,[$K_{c,tgsrem}$||id_{tgsrem}||TS_4|| $Ticket_{tgsrem}$])

C→TGS_{rem} : id_{vrem}||$Ticke_{tgsrem}$|| $Authenticator_c$

TGS_{rem}→C : E($K_{c,tgsrem}$,[$K_{c,vrem}$||id_{vrem}||TS_6|| $Ticket_{vrem}$])

C→v_{rem} : $Ticket_{vrem}$||$Authnticator_c$

IV. RESULTSANALYSISAND 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.

Published By:
Blue Eyes Intelligence Engineering & Sciences Publication

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 $2^8 \times 5$ = 1280minutes.

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

1. Vasilomanolakis E, Daubert J, Luthra M, Gazis V, Wiesmaier A, Kikiras P. On the security and privacy of internet of things architectures and systems. InSecure Internet of Things (SIoT), 2015 International Workshop on 2015 Sep 21 (pp. 49-57). IEEE.
2. Chen S, Xu H, Liu D, Hu B, Wang H. A vision of IoT: Applications, challenges, and opportunities with china perspective. IEEE Internet of Things journal. 2014 Aug; 1(4):349-59.
3. Zhang ZK, Cho MC, Wang CW, Hsu CW, Chen CK, Shieh S. IoT security: ongoing challenges and research opportunities. In Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on 2014 Nov 17 (pp. 230-234). IEEE.
4. Suo H, Wan J, Zou C, Liu J. Security in the internet of things: a review. In Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on 2012 Mar 23 (Vol. 3, pp. 648-651). IEEE.
5. Zhou W, Jia Y, Peng A, Zhang Y, Liu P. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. IEEE Internet of Things Journal. 2018 Jun 15.
6. Razzaq MA, Gill SH, Qureshi MA, Ullah S. Security Issues in the Internet of Things (IoT): A Comprehensive Study. International Journal of Advanced Computer Science and Applications (IJACSA). 2017 Jun 1; 8(6):383-8.
7. Leloglu E. A review of security concerns in Internet of Things. Journal of Computer and Communications. 2017 Jan 1;5(1):121-36.
8. Elkhodr M, Shahrestani S, Cheung H. The internet of things: new interoperability, management and security challenges. arXiv preprint arXiv:1604.04824. 2016 Apr 17.
9. Sfar AR, Natalizio E, Challal Y, Chtourou Z. A roadmap for security challenges in the Internet of Things. Digital Communications and Networks. 2018 Apr 1; 4 (2):118-37.
10. Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. Internet of things: Vision, applications and research challenges. Ad hoc networks. 2012 Sep 1;10(7):1497-516.
11. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials. 2015 Jun 15;17(4):2347-76.
12. Perera C, Ranjan R, Wang L, Khan S, Zomaya A. Privacy of big data in the internet of things era. IEEE IT Special Issue Internet of Anything. 2015 Feb; 6
13. Razzaq MA, Gill SH, Qureshi MA, Ullah S. Security Issues in the Internet of Things (IoT): A Comprehensive Study. International Journal of Advanced Computer Science and Applications (IJACSA). 2017 Jun 1; 8(6):383-8.
14. Lee I, Lee K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons. 2015 Jul 1; 58(4):431-40.
15. Sadeghi AR, Wachsmann C, Waidner M. Security and privacy challenges in industrial internet of things. In2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC) 2015 Jun 8 (pp. 1-6). IEEE.
16. Bharati, T. S. (2015). Enhanced Intrusion Detection System for Mobile Adhoc Networks using Mobile Agents with no Manager. *International Journal of Computer Applications*, *111*(10).
17. Bharati, T. S., & Kumar, R. (2015, March). Secure intrusion detection system for mobile adhoc networks. In *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on* (pp. 1257-1261). IEEE.
18. Bharati, T. S., & Kumar, R. (2015). Intrusion Detection System for MANET using Machine Learning and State Transition Analysis. *International Journal of Computer Engineering & Technology (IJCET)*, *6*(12), 1-8.
19. Bharati, T. S., & Kumar, R. (2016). Enhanced Key Distribution for Mobile Adhoc Networks. *International Journal of Engineering Science*, 6(4), 4184-4187.
20. Bharati T. S. (2017). Agents to Secure MANETS. *International Journal of Advanced Engineering and Research Development,* 4(11), 1267-1273.
21. Bharati T.S. (2018). MANETs and Its' Security. *International Journal of Computer Networks and Wireless Communication,* 8(4), 166-171.
22. Bharati T.S. (2019). Trust Based Security of MANETs.*International Journal of Innovative Technology and Exploring Engineering*, 8(8), 1-4.
23. Stallings W. Cryptography and network security, 4/E. Pearson Education India; 2006.

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.