International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:12, No:6, 2018

Comparison of Security Challenges and Issues of Mobile Computing and Internet of Things

Aabiah Nayeem, Fariha Shafiq, Mustabshra Aftab, Rabia Saman Pirzada, Samia Ghazala

***Abstract*—**In this modern era of technology, the concept of Internet of Things is very popular in every domain. It is a widely distributed system of things in which the data collected from sensory devices is transmitted, analyzed locally/collectively then broadcasted to network where action can be taken remotely via mobile/web apps. Today's mobile computing is also gaining importance as the services are provided during mobility. Through mobile computing, data are transmitted via computer without physically connected to a fixed point. The challenge is to provide services with high speed and security. Also, the data gathered from the mobiles must be processed in a secured way. Mobile computing is strongly influenced by internet of things. In this paper, we have discussed security issues and challenges of internet of things and mobile computing and we have compared both of them on the basis of similarities and dissimilarities.

***Keywords*—**Embedded computing, internet of things, mobile computing, and wireless technologies.

I. Introduction

MOBILE computing offers services during mobility. Wireless technologies, short range networks, and sensor networks allow internet to be integrated with embedded computing with ease [1]-[4]. Without the involvement of humans, devices are able to sense data, send data, receive data, process data and can take decisions according to data received from multiple homogenous and heterogeneous resources. Mobile Computing enables users to access data from anywhere while moving and internet of things involves in communication among devices, so the combination of internet of things and mobile computing yields the concept of "*communication with mobility*" [5]. But, the biggest challenge is to provide secure communication across the network. Both domains possess their own security challenges. These challenges must be addressed in order to provide a secured communication. In this paper, we introduce the concept of IoT and mobile computing in Section I and Section II covers the Architecture of IOT, Section III describes the security challenges and issues in IoT on the basis of discussed layers, In Section IV, we discuss the basic concept of mobile computing, Section V defines security challenges in mobile computing, Section VI provides brief comparison of security challenges and issues of IoT and mobile computing, and in Section VII, we conclude our study.

Aabiah Nayeem is the student in Jinnah University for Women, Nazimabad, Karachi, CO 74600 Pakistan (phone: +923422274801; e-mail: aabiah.nayeem@yahoo.com).
Fariha Shafiq is the student in Jinnah University for Women, Nazimabad, Karachi, CO 74600 Pakistan (phone: +923130322513; e-mail: farihashafiq17@gmail.com).
Mustabshra Aftab is the student in Jinnah University for Women, Nazimabad, Karachi, CO 74600 Pakistan (phone: +923343422506; e-mail: mustabshra.aftab@yahoo.com).
Rabia Saman Pirzada is the student in Jinnah University for Women, Nazimabad, Karachi, CO 74600 Pakistan (phone: +923350368530; e-mail: pirzadar6@gmail.com).
Samia Ghazala is the assistant professor in Jinnah University for Women, Nazimabad, Karachi, CO 74600 Pakistan (phone: +923333225024; e-mail: samia_ghazala@yahoo.com).

II. Architecture of IoT

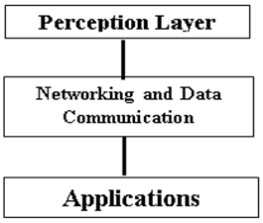

Fig. 1 Architecture of IoT

A. Perception Layer

This layer is responsible to gather data from multiple heterogeneous devices in the IoT environment and to send gathered data on network [6], [7]. This layer is also known as device layer as it consists of sensors and other different objects. Sensors can be RFID, infrared, etc. This layer is responsible to acquire, collect, and send received data from sensors to the network for further secured processing.

B. Network Layer

This layer is also known as transmission layer. This layer is responsible for the communication of information over the internet. For this purpose, an efficient infrastructure of network among devices must be established [6], [7]. The transmission medium may be wired or wireless. This layer transfers the information from perception layer to application layer.

C. Application Layer

This layer is responsible for the integration and presentation of data and to interact with the user [6], [7]. The protocols used in this layer are Constrained Application Protocol (CoAP), Message Queue Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP), RESTFUL services (Representational state transfer), Advanced Message Queuing Protocol (AMQP), Webstocks.

III. Security Issues and Challenges in IoT on the Basis of Discussed Layers

A. Perception Layer Security Challenges and Issues

The perception layer /sensing layer of IoT architecture faces

some security threats that are discussed below:

- *Weakness of Signals:* When signals are transmitted between nodes in a network, their strength is affected by upsetting waves or by interruption of new signal introduced by the intruder.
- *Intercepted by Intruder:* It is easy for the attacker to influence the devices because IoT nodes operate in exterior and open-air environment, attacker is able to attack the hardware devices on IoT network [7].
- *Inherently Dynamic Nature of Network Topology:* The dynamicity of IoT devices leads to dynamic nature of network. The perception layer of IoT consists on sensors and other hardware, having limited storage area, limited computation and low power consumption opens up them to different security issues [7], [8].
- *Constrained Resources:* The devices in this layer have limited resources that are limited computational speed, limited storage capacity. Hence the implementation of security system is harder to implement in this layer [9].

B. Network Layer Security Challenges and Issues

Different types of security issues and attacks influence the network layer of IoT architecture and these are:

- *Network congestion:* Network congestion refers to the burden of large amount of data coming from multiple heterogeneous devices on network. This makes difficult to provide security on this level [9].
- *Eavesdropping:* Eavesdropping allows the attacker to retrieve information. This attack is very hard to detect as the attacker only hacks the information without altering it. This attack is very dangerous when confidential information is communicating among nodes [9], [10].
- *Counterfeiting Attacks:* Counterfeiting attack refers to man in the middle attack. An intruder just not only hacks the information but also alters it [9], [11].
- *DDos Attacks:* DDos attack occurs when malicious node makes services unavailable to the users because of tremendous amount of traffic load on network [9], [12].

C. Application Layer Security Challenges and Issues

Security threats also have a great impact on application layer of IoT architecture and these threats are described below:

- *Data Privacy and Leakage:* Data privacy and leakage is main challenge in this layer because this layer is responsible for data sharing. So in order to share data with third parties in a way so as not to leak the private information of users is the biggest issue and challenge [9], [13].
- *Control of Access:* Control of access refers to that to which extent the person is allowed to access the information, service, application, etc. [9].
- *Data Integration:* As the data are gathered from different heterogeneous devices therefore it is difficult to integrate it in order to make sure that data are secured.
- *Availability of Service:* The availability of the services is strongly influenced by the traffic load on network.
- *Authenticity:* Different users using the network are also a threat to the network because it is difficult to recognize which user is authentic or which user is an intruder.

IV. Mobile Computing

Mobile computing is basically a human-computer interaction in which the computer during normal usage is expected to be transported. Mobile computing has signaled a modern new era in the computing and information system field as well as in the IT technology development [14]. It allows the transmission of data through a computer, without making a connection to a fixed physical link. Rather than using wires, a wireless communication takes place through the radio signals which is easy to intercept or eavesdrop on the communication channels, so security is very important factor for all these threads. Many different issues within security that needs to be taken care of individually are confidentiality, integrity, availability, legitimacy, and accountability. The true revolutions in telecommunication world have been seen in the last few years. Taking the three generations of wireless cellular systems beside, ubiquitous computing has been possibly done due to rapidly advancing in wireless communication technology and availability of many portable, light-weight computing devices like cellular phones and electronic organizers. Some more different kinds of security issues in mobile computing are discussed below in detail.

V. Security Challenges in Mobile Computing

The security is a major issue in mobile computing. These are some areas that are focused in mobile computing such as mobile devices, mobile communication, and mobile network and they have their own security challenges which are:

A. Security Issues in Mobile Devices

Mobile devices should be given serious consideration because the issue of security in them acts as an obstacle in the development of mobile services [15]. Every security issue needs to be addressed at the service development process. The main mobile security threats of mobile services include:

- The complexity of technical solutions
- Illegal copying of programs and content.
- Threats provided by the Internet.

B. Security Issues in Mobile Network

Mobile or wandering devices have the need for providing network access through mobile networks. A big issue and challenge is that the data that are shared with the other nodes should be private. The nodes or devices may be harmful if the nodes that share the data are not reliable; on the other hand, rest of the network could be destroyed if it does not sense the data properly. In any case, the need for wireless access to a network is evident, new problems will arise in the wireless medium. However, wireless does not involve mobility [16]. In the wireless networks, both ends of communication are fixed like in wireless local loops. However, the wireless data networks study has some kind of different scope comparatively from networking system. When the wide variety of mechanisms is currently used to provide IPv6

connectivity, the situation in that case becomes more complicated [17].

C. Security Issues in Mobile Communication

The wired counterparts are more secure and reliable than the wireless devices such as mobile phones, PDAs and pagers because of their bandwidth, memory and processing capabilities. The main reason behind this is the interruption of the data that are sent into the air [17]. Establishment of wireless communication channel that should be secure is the big requirement of PCs. In designing the security schemes for mobile communication, some important issues that need serious concentration are:

- Autonomy of communicating entities
- Mobility of the users
- Restriction of hardware.

VI. Brief Comparison of Issues and Challenges of IoT on Basis of Similarities and Dissimilarities

TABLE I
COMPARISON OF SECURITY CHALLENGES AND ISSUES OF IOT AND MC

Similarities		Dissimilarities	
Privacy	High extent of security threat in Mobile Computing as well as in Internet of Things	***Weakness of signals***	This is the issue of Iot Architecture not of the Mobile Computing
Reliability	Affects Internet of Things as well as Mobile Computing to high extent	***Control of access***	This problem occurs only in Iot architecture not in Mobile Computing
Eavesdropping	This attack is faced by Internet of things and Mobile Computing to great extent	***Illegal Copying of Program and Content***	Mobile Computing faces this problem to great extent but IoT doesn't possess this problem
Heterogeneity	This problem is faced by Internet of things and Mobile Computing to big extent	***Availability of Service***	This problem occurs only in IoT but not in Mobile Computing
Continuous Sensing	Both Internet of Things and Mobile Computing faces this problem to large extent	***DDos Attacks***	Such attack arises only in IoT but not in Mobile Computing
Data Integration	Internet of Things and Mobile Computing faces this problem to huge extent	***Counterfeiting Attacks***	This attack takes place in IoT but not in Mobile Computing.

VII. Conclusion

In this study, different articles and conferences were reviewed in order to provide a detailed view of security challenges in mobile computing and Internet of Things (IOT). It is found that the security of both is a very serious issue [18]. These areas need proper attention of the researchers to overcome the security issues in the domains of heterogeneity, and to continue sensing, context problem, privacy and reliability. In future, these security issues of both mobile computing and IOT will overcome to some extent [19].

Acknowledgment

In writing this research paper, we had to take the help and guideline of a respected person, who deserve our greatest gratitude. The completion of this research paper gives us much pleasure. We would like to show our gratitude *to Miss Samia Ghazala*, our supervisor for giving us a good guideline for topic, and the research paper throughout numerous consultations. We would also like to expand our deepest gratitude to all those who have directly and indirectly guided us in writing this research paper.

References

[1] Qi, Han, and Abdullah Gani. "Research on mobile cloud computing: Review, trend and perspectives." In Digital Information and Communication Technology and it's Applications (DICTAP), 2012 Second International Conference on, pp. 195-202. IEEE, 2012.
[2] Asokan, N. "Security issues in mobile computing." (1994).
[3] Urbas, Gregor, and Tony Krone. Mobile and wireless technologies: security and risk factors. Australian Institute of Criminology, 2006.
[4] Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions" Future generation computer systems 29, no. 7 (2013): 1645-1660.
[5] Stankovic, John A. "Research directions for the internet of things." IEEE Internet of Things Journal 1, no. 1 (2014): 3-9.
[6] Yan-rong, Shi, and Hou Tao. "Internet of Things key technologies and architectures research in information Processing." In Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013). 2013.
[7] Yousuf, Tasneem, Rwan Mahmoud, Fadi Aloul, and Imran Zualkernan. "Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures." (2015).
[8] Kamilaris, Andreas, and Andreas Pitsillides. "Mobile phone computing and the Internet of Things: A survey." IEEE Internet of Things Journal 3, no. 6 (2016): 885-898.
[9] Adat, Vipindev, and B. B. Gupta. "Security in Internet of Things: issues, challenges, taxonomy, and architecture." Telecommunication Systems (2017): 1-19.
[10] Khattab, Ahmed, Zahra Jeddi, Esmaeil Amini, and Magdy Bayoumi. "RFID Security Threats and Basic Solutions." In RFID Security, pp. 27-41. Springer International Publishing, 2017.
[11] Desmedt, Yvo. "Man-in-the-middle attack." In Encyclopedia of cryptography and security, pp. 759-759. Springer US, 2011.
[12] Mirkovic, Jelena, Sven Dietrich, David Dittrich, and Peter Reiher. "Internet Denial of Service: Attack and Defense Mechanisms (Radia Perlman Computer Networking and Security)." (2004).
[13] Schwartz, Paul M. "Property, privacy, and personal data." Harv. L. Rev. 117 (2003): 2056.
[14] Dinh, Hoang T., Chonho Lee, Dusit Niyato, and Ping Wang. "A survey of mobile cloud computing: architecture, applications, and approaches." Wireless communications and mobile computing 13, no. 18 (2013): 1587-1611.
[15] Yasham Singhal, Saloni Singh, Varsha Mathpal. Security Challenges in Mobile Computing. Vol 3, Issue1, Jan – March 2015.
[16] Wheat, Jeffrey, Randy Hiser, Jackie Tucker, Alicia Neely, and Andy McCullough. Designing a wireless network. Syngress Publishing, 2001.
[17] Ahonen, Pasi, Juhani Eronen, Jarkko Holappa, Jorma Kajava, Tiina Kaksonen, Kati Karjalainen, Kaarina Karppinen et al. "Information security threats and solutions in the mobile world." VTT Research Notes (2005): 1-108.
[18] Vermesan, Ovidiu, Peter Friess, Patrick Guillemin, Sergio Gusmeroli, Harald Sundmaeker, Alessandro Bassi, Ignacio Soler Jubert et al. "Internet of things strategic research roadmap." Internet of Things-Global Technological and Societal Trends 1 (2011): 9-52.
[19] Mendez, Diego M., Ioannis Papapanagiotou, and Baijian Yang. "Internet of Things: Survey on Security and Privacy." arXiv preprint arXiv: 1707.01879 (2017).