ISSN:2231-0711
T. Venkat Narayana Rao et al | IJCSET(www.ijcset.net) | December 2016 | Vol 6, Issue 12, 414-418

Internet of Things: Security Challenges and Issues

T. Venkat Narayana Rao[1], Sangam Shayideep[2], Jayesh Jahagirdar[3]

[1]*Professor,*
CSE, SNIST, Hyderabad, T.S, INDIA.

[2]*Student,*
CSE, SNIST, Hyderabad, T.S, INDIA

[3]*Student,*
Pune Vidyarthi Griha, PVG COET, Pune. INDIA

Abstract : The Internet of Things, a developing worldwide Internet-based technical architecture which facilitates trading of merchandise and enterprises in worldwide supply chain networks affects the privacy and security of the included partners. In order to tackle this some measures should be taken which ensures client privacy, access control, data authentication and architecture's resilience to attacks.

No doubt that security is the most needed of prerequisites for the across the board implementation of numerous IoT visions. The scope for IoT security is incredibly wide, in no less than four dimensions. As far as security extension is concerned it rarely incorporates addressed tasks like digital forgetting, privacy, communication, computation and sensing. It additionally requests novel and better strategies for software, hardware and data protection that may access to IoT devices physically. The common components of IoT devices are Sensors and actuators and create many problems related to security including the integrity of actuating events and physical signals. In the final stage of processing of amassed data, numerous semantic attacks can be expected. In this paper various challenges and issues of IoT implementations are discussed.

1. INTRODUCTION

IoT is an interestingly new network architecture that is quickly picking up attention in cutting edge remote wireless communications. The fundamental concept of IoT is giving us numerous articles or objects, for example, cell phones, actuators, sensors and radio frequency identification (RFID) tags, which can interface and coordinate with one another to provide services, processing and communication. A network like this is a perfect platform for large-data multimedia applications as there is a huge demand for newly developing applications like voice over IP (VoIP), IPTV and video on demand (VoD). These days, for different multimedia applications in IoT, security is of basic significance [1]. Both users and applications can be a source of security threats to the IoT as the IoT is built to comprehensively execute unverified user-implemented applications from different users [2][3]. For instance, vindictive clients can access IoT to dispatch vicious service attacks and hack applications and sensors. Also, a genuine client may utilize network to a very large extent or may alter multimedia data that is shared among multiple users this may create hinderance in the availability of services to other genuine clients. As IoT has not utilized any particular security component to manage the dangers specified above, it is imperative to convey a security technique to ensure that the multimedia applications streaming over the IoT are safe.

IoT security incorporates many layers of abstraction and dimensions. The abstraction levels include all the levels like physical layers of sensors, calculation and communication, and gadgets to the semantic layer in which all gathered data is translated and processed. It can be anticipated that most of the security threats will happen at the software area since it is as of now most prominent and can at the same time cover a substantial number of processes and gadgets. From the perspective of research, most unprecedented assaults are on physical signals and specifically semantic assaults amid processing of the data and decision making steps. The most minimal security at any level and at any dimension decides the overall security. Most of the IoT gadgets will work without batteries in a passive mode. They will utilize energy with the help of a wireless medium. A considerable amount of these systems will take into account very less hardware and hence it will require very compact security solution with a very small footprint and energy requirement. So IoT security is important as numerous IoT gadgets frequently work in hostile environments without any protection.

2. SECURITY ARCHITECTURE OF IOT

The data and network security should be equipped with properties like integrity, confidentiality and identification. Not quite the same as web, the IoT will be connected to the pivotal areas of national economy, e.g. Intelligent transportation, medical service and health care as shown in figure 1. Hence the demand for security in the IoT will be high and also these security measures should be available throughout an extensive large area. In terms of secure architecture the IoT can be isolated into four key levels [4].

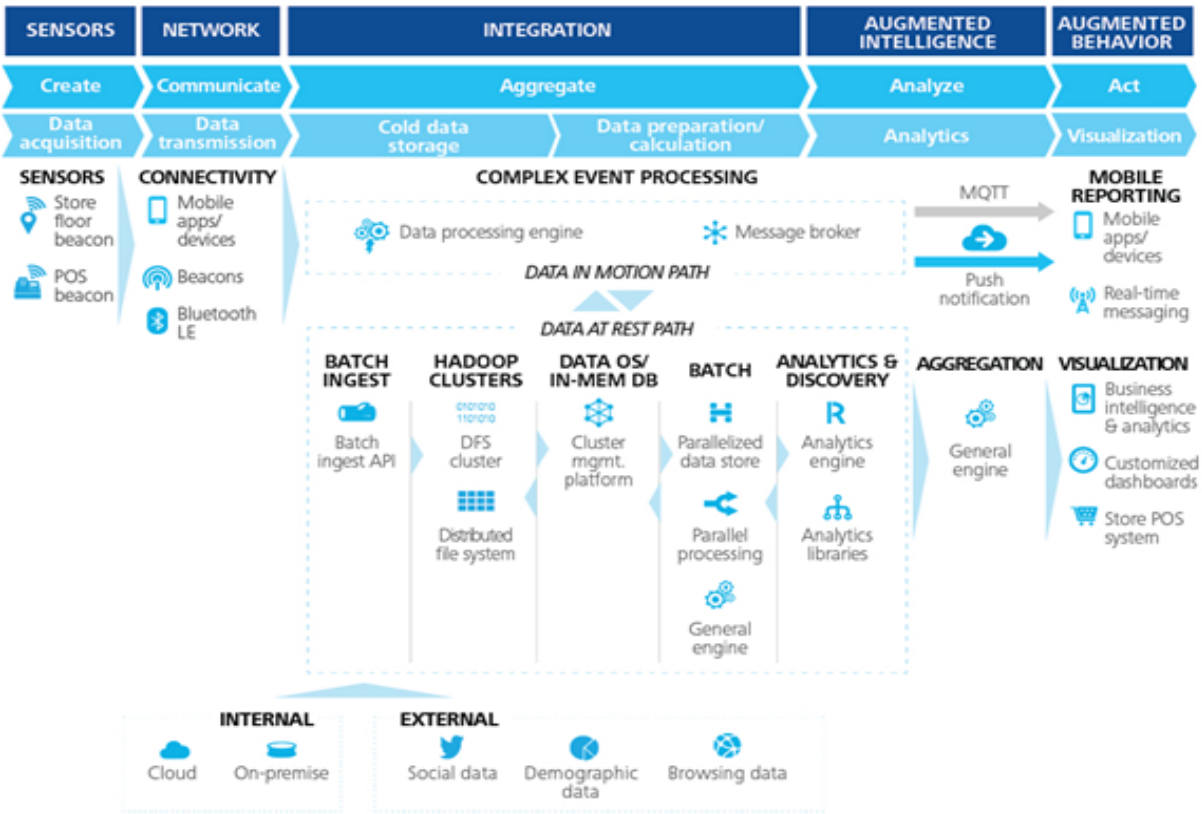

Fig. 1 demonstrates that the level architecture of the IoT.

Security architecture :

Perceptual layer is the most fundamental level (otherwise called recognition layer), It gathers a wide range of data through hardware and recognizes the surroundings, the data incorporates environmental condition, object properties etc. Hardware includes GPS, all kinds of sensors, RFID reader and other equipment. In this layer the important segment is sensors. It is used detect the physical world and express it in a digital format.

Network layer is the next layer. The function of this layer is to transmit of data from perceptual layer, initial processing of data, polymerization and classification. Transmission of data in this layer is depended on a few basic networks, which are the 2012 International Conference on Computer Science and Electronics Engineering internet, network infrastructure, wireless network, satellite nets, mobile communication network and communication protocols are also necessary for inter-device data transfer [5].

Support layer comes after network layer. The function of this layer is to set up a solid support platform for the application layer, upon which all sort of computing powers will be composed through cloud computing and network grid. It consolidates application layer upward and network layer downward.

The application layer is the highest level. It gives the customized services as indicated by the requirements of the clients. IoT is made available to clients through the interface of this layer utilizing of TV, PC or mobile gadgets etc.

Security Features

a) Perceptual Layer: As perceptual nodes are basic and require less power they are short of computer power and storage capacity. In this manner it cannot have frequency hopping communication and public key encryption algorithm for security protection. Furthermore, it is extremely hard to set up security protection system. In the interim assaults from the external network like deny of service also bring new security problems. On the other hand sensor information still need the protection for confidentiality, authenticity and integrity.

b) Network Layer: Even though the core network has generally total security protection capacity, yet Man-in-theMiddle Attack and fake assault still exist, in the interim garbage mail and PC viruses cannot be overlooked, a substantial number of information sending cause blockage and congestion. Hence security component in this level is critical to the IoT.

c) Support Layer: It does the mass data processing and intelligent decision of network behavior in this layer, intelligent processing is constrained for vindictive data, so it is difficult to enhance the capacity to perceive the noxious data.

d) Application Layer: In this level security requirements for various application environment are distinctive, and information sharing creates problem of access control, information protection and disclosure of information[5].

3. SECURITY REQUIREMENTS

a) Perceptual Layer: In the very initial step the authentication of node is important, as it counteract illicit node access; furthermore data encryption is extremely necessary to ensure the privacy of data that is exchanged between two or more nodes. Key agreement is an imperative process before the data encryption. The utilization of assets increases with the strength of the security, to take care of this issue, lightweight encryption innovation is necessary, which incorporates Lightweight cryptographic protocol and lightweight cryptographic algorithm. It is also important to check that the data that is provided by the sensor is complete and correct so research is also done in this direction.

b) Network Layer: The communication security measures that are now in use, cannot be implemented in the network layer of IoT security. Identity authentication is a sort of measure to keep the illicit nodes, which is the basis of the security system. Privacy and integrity are of equivalent significance, along these lines we likewise need to set up integrality mechanism and data confidentiality. Besides distributed denial of service attack (DDoS) is a typical assault strategy in the system and is especially extreme in the IoT, hence prevention of DDOS assault on the vulnerable node is another challenge that is to be dealt with in this layer.

c) Support Layer: It demands high application security design, for example, secure multiparty computation and cloud computing, most of the encryption protocol and encryption algorithm, stronger system security technology and anti-virus.

d) Application Layer: there are two ways to take care of the security issue of this layer. First is the validation and key agreement over the different networks and the second is client's security assurance. Moreover, management and education are vital to data security, particularly password management [6].

Hence we can come to a conclusion that the security in the IoT is imperative and loaded with difficulties. At the same time it is also important to consider problems related to laws and regulations, we will further scrutinize this issue in detail.

3.1 Physical Security

Physical security is denoted in external context and inherent infrastructure, in which human-like security immune safeguard is achieved.

1) External Context: Complex context and simple context are indicated in [6], in which the previous decides the essential location, identity, and entity status with the help of only one parameter; the latter alludes to real world conditions, traceability information, and geographical structures. Both the above context are refined to bolster developing, debugging and integrating applications of Ubiquitous IoT, and give connections between the interfaces and confinement for Unit IoTs. In U2IoT model, the borders of each entity's external context merge even vanish, and the obscure contexts spanning from an individual, an object, or an environment to social relationships, should support the hierarchical IoT subsystem. (Didn't understand). Especially, interruption identification algorithm is noteworthy to secure context information for checking sensors behavior, find control node breaches, and other potential vulnerabilities.

2) Inherent Infrastructure: Artificial immune security system as computational intelligence is applied to analyze inherent infrastructure, which belongs sensorial system inspired by principles and processes of the natural immune system. General algorithms (e.g. immune network, negative selection, and clonal selection) exploit the immune system's features of detection, learning and memory to constitute innate resistance and adaptive invulnerability. Physical security issues, for example, error recovery, context-driven feedback, adaptive disposition, and intrusion detection can be addressed in the following manner.

3.2 Innate immunity: In real-time environment it gives essential hindrances against foreign intrusions. With the help of intelligent pattern recognition algorithm, when the sensors recognize strange or malicious assaults, at that time innate immunity is activated. Unit IoT networks transmit co-stimulation signals to distributed control nodes and when these signals are transmitted the management centers performs rejection reactions. In order to ensure detection optimization during defense operations the activation thresholds are defined as well as for imperfect detection fuzzy diagnosis can also be applied. The innate immune defense is generic, implying that U2IoT model reacts to the different assaults in a generic pattern. A system like this cannot bear enduring invulnerability against some specific attacks. The innate immune system is dominant to counteract the ever changing contexts and dangers that are encountered continuously [7].

3.3 Adaptive immunity: This immunity protects the system when an attack is associated with a unique signature. At the time of attack prototype presentation selective response needs to recognize non-self-element. In the event that U2IoT has been contaminated by the intrusion which had attack in the past then a particular memory module would be activated in order to nullify harmful effects by producing enhanced reaction to return the system into secure state. Fuzzy diagnosis is executed for variations of the similar former attack. It is possible to implement subsidiary vaccination, an optimal stimulation by updating M&DCs' profile databases.

As per both adaptive and innate immunities, three primary components ought to be accomplished in U2IoT model [8].

Multithreaded and Hybrid Configuration: For the hugely parallel system engineering which involves a distinct arrangement of parts, the U2IoT model may apply multithreaded security calculations. The components are sorted out in hybrid mode, in which both distributed and centralized designs are incorporated. The allocation of the sensing and query processing is performed by the central M&DC towards Unit IoT, the designation of the detecting and question preparing is performed by the focal M&DC.

Towards Ubiquitous IoT, the industry IoTs and local IoTs are comparatively independent, which ordinarily constructional IoT (grammar error). In U2IoT model, such hybrid and multithreaded configuration are throughout all the networks, sensor and control nodes, and management and data centers in U2IoT model [9].

Multilayered and Autonomous Organization : Not even a single security system is there that offers end to end resistance. Subsequently, multi-layered protection ought to independently work for complete safeguards. U2IoT model, amid the layered organization, autonomously settles on its choices by distinguishing potential assaults and providing possible solutions which is based on artificial immune algorithms.

Heterogeneity: U2IoT model ought to be open by an extensive number of heterogeneous communication technologies with various hardware and software capabilities, interfaces, channels, and networks. This heterogeneity of components adds makes the security situations intricate. Which makes that a specific assault simultaneously act numerous elements in various IoTs, however the assault can't follow up on all the involved IoTs. The insusceptible assurance guarantees that the whole heterogeneous parts can't be debased because of similar attacks [10].

4. MANAGEMENT SECURITY

In the upcoming IoT, it is barely conceivable to build up a uniform security protocol as Internet, much the same as various countries as well as areas cannot implement similar security measures. Thus distinctive management mechanisms are important for interconnection requirements as well as for security. Apt management ought to couple with the execution of data and physical security because of the impediments of technological approaches. Security working on human behaviors should be considered to guarantee that virtual digital information is translated into real physical contexts [11].

4.1 Application prerequisite for control nodes and distributed sensor gives generic as well as unique security. IPM is of advantage to practical application security, for example, system certification, software design, risk assessment, project management, and historical query. For a particular situation, customized requirements are associated to describe the authorized or unauthorized usage in a particular organization or individual. Furthermore, application necessity ought to be consistent with privacy prevention which realizes that the delicate information is traded, stored, and shared without compromising any user privacy [12].

4.2 Industry/Local/National regulation mainly serves for iM&DC/lM&DC/nM&DC to provide rules and guidance for U2IoT. It takes legitimate or disciplinary actions to oppose the hostile people or organizations that do not abide by the laws. There into, industry regulation delineates methods to have maximum security objective for a special industrial authority organization like military, energy, and agriculture. For example, in the chemical hazards medicinal administration, the regulation require certain parameters (e.g., relative proximity, vibrations, and temperature), alert the clients for violating thresholds, and ensure system security by warning anomalous configuration and implementation. There into, local regulation ought to correspond with local traditions and practices to receive humanistic points of view for designing, implementing, and maintaining the local IoTs. National regulation governs guidelines to realize inter-nation compatibility, and formal memorandum of agreements should be shared internationally. Moreover, customized roles and responsibilities can be systematized among various countries [13]1[4].

4.3 Worldwide policy considers the international IoT consociation during connectivity and consistency of nM&DC and global IoT. Additionally, universal measures ought to be addressed by governments to enhance security assurance and guarantee interoperability. It shows that a general worldwide administration system with enforcement policies will give permanent solution towards security protection [15].

CONCLUSION

In this paper, a security design IPM is put-forth for U2IoT display which includes issues and challenges. The principle reason is to build a coordinated security architecture while considering cyber-physical-social world. The proposed IPM includes three key security points of view (i.e. information, physical, and management), in which three-dimensional data security model introduces compatibility and social layer and intelligence for security consideration. Physical security is portrayed by applying artificial immunity; and a progression of social strategies are recommended to attain feasible management security.

REFERENCES

[1] R. H. Weber, “Internet of things – new security and privacy challenges,” Computer Law & Security Review, vol. 26, pp. 23-30, 2010.

[2] J. F. Wan, H. H. Yan, H. Suo, and F. Li, “Advances in cyber-physical systems research,” KSII Transactions on Internet and Information Systems, 2011, 5(11): 1891-1908.

[3] M. Chen, J. F. Wan, and F. Li, “Machine-to-machine communications: architectures, standards, and applications,” KSII Transactions on Interneand Information Systems, to appear, January 2012.

[4] G. Yang, J. Xu, W. Chen, Z. H. Qi, and H. Y. Wang, “Security characteristic and technology in the internet of things,” Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30, no. 4, Aug 2010.

[5] Z. H. Hu, “The research of several key question of internet of things,” in Proc. of 2011 Int. Conf. on Intelligence Science and Information Engineering, pp. 362-365.

[6] G. Gan, Z. Y. Lu, and J. Jiang, “Internet of Things Security Analysis,” inProc. of 2011 Int. Conf. on Internet Technology and Applications (iTAP),Aug. 2011.

[7] M. Langheinrich, “Privacy by design-principles of privacy-aware ubiquitous systems,” In Proc. of Ubicomp, pp. 273-291, Oct. 2001.

[8] C. P. Mayer, “Security and privay challenges in the internet of things,” Electronic Communications of the EASST, vol. 17, 2009.

[9] T. Polk, and S. Turner. “Security challenges for the internet of things,” http://www.iab.org/wp-content/IAB-uploads/2011/03/Turner.pdf

[10] C. Ding, L. J. Yang, and M. Wu, “Security architecture and key technologies for IoT/CPS”, ZTE Technology Journal, vol. 17, no. 1, Feb. 2011.

[11] J. F. Wan, H. Suo, H. H. Yan, and J. Q. Liu, “A general test platform for cyber-physical systems: unmanned vehicle with wireless sensor

network navigation," in Proc. of 2011 Int. Conf. on Advances in Engineering, Nanjing, China, December, 2011.

[12] J. H. Shi, J. F. Wan, H. H. Yan, and H. Suo, "A survey of cyber-physical systems," in Proc. of the Int. Conf. on Wireless Communications and Signal Processing, Nanjing, China, November, 2011.

[13]. Blass, E. O., Elkhiyaoui, K., & Molva, R. (2011). Tracker:security and privacy for RFID based supply chains. In Proceeding of the 18th network and distributed system security symposium.

[14]. Elkhiyaoui, K., Blass, E. O., & Molva, R. (2012). CHECKER:On-site checking in RFID-based supply chains. In Proceedings of the fifth ACM conference on security and privacy in wireless and mobile networks.

[15]. Chen, M., Kwon, T., Mao, S., & Leung, V. (2009). Spatial–temporal relation-based energy-efficient reliable routing protocol in wireless sensor networks. International Journal of Sensor Networks, 5(3), 129–141.