A SOLUTION FRAMEWORK OF SOFTWARE SECURITY SERVICE FOR INTERNET OF THINGS (IOT)

SUSHIL KUMAR

Research Scholar, Dept. of Computer Application,

Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal-Indore Road, Madhya Pradesh, India

Dr. Jitendra Seethlani

Research Guide, Dept. of Computer Application,

Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal Indore Road, Madhya Pradesh, India

ABSTRACT

Internet of Things (IoT) refers to heterogeneous systems and devices (often referred to as smart objects) that connect to the internet, and is an emerging and active area of research with tremendous technological, social, and economical value for a hyper-connected world. In this paper, we will discuss how billions of these internet connected devices and machines will change the future in which we shall live, communicate and do the business. Programmable management frameworks have paved the way for managing devices in the network. Lately, emerging paradigm of Software Defined Networking (SDN) has revolutionized programmable networks. Designers of networking applications i.e. Internet of things (IoT) have started investigating potentials of SDN paradigm in improving network management. IoT envision interconnecting various embedded devices surrounding our environment with IP to enable internet connectivity. Unlike traditional network architectures, IoT are characterized by constraint in resources and heterogeneous inter connectivity of wireless and wired medium. Therefore, unique challenges for managing IoT are raised which are discussed in this paper. Ubiquity of IoT has raised unique security challenges in IoT which is one of the aspects of management framework for IoT. In this paper, security threats and requirements are summarized in IoT extracted from the state of the art efforts in investigating security challenges of IoT. Also, SDN based security service provisioning framework for IoT is proposed.

KEYWORDS—IoT; Software Defined Security; Security in IoT; Software Defined Networking; Software Defined based IoT (SDIoT)

INTRODUCTION

Recent revolutions in embedded technologies and Internet have made it possible for the things surrounding us to be interconnected with each other [1]. It is expected in the coming era IoT devices will be part of the environment around us which will generate enormous amount of data. Processing is required on the generated data which is then presented in an understandable form to the requester. Mobile operators, software developers, integrators and alternative access technology are involved in the IoT ecosystem [2]. There are many different application domains where IoT plays crucial role like manufacturing, health-care, transport, administration, insurance, public safety, local community, metering, road safety, traffic management, tracking, etc. IoT enables interconnection with people's devices exchanging information and performing actions without humans involved. This is possible by amalgamating heterogeneous communication infrastructure. This has motivated the researcher to design smart gateways which connects IoT devices with traditional internet. Most recently, enabling Everything as a Service model by merging IoT and Cloud Computing is the focus of attention in the research community [3] (see figure 1). In order to tackle management problems in IoT, resource management frameworks have received considerable attention. SDN paradigm offers an attractive solution to manage IoT resources which is been lately under focus. Proposal of a framework for managing traffic and network resources in an IoT environment is given in [4]. Other efforts which have adopted SDN based approach to solve management issues in IoT.

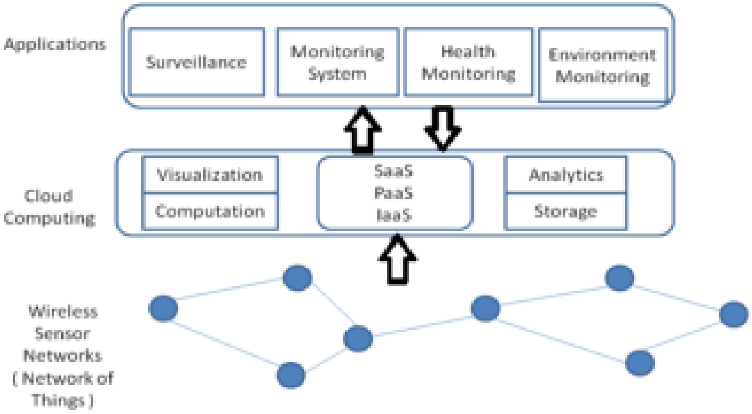

Fig. 1. IoT and Cloud Convergence

Numerous security challenges are illuminated with the increasing complexity of IoT networks. There is a desire for a complete framework which manages data generated from the IoT devices. Up till now there is no SDN based comprehensive security framework for IoT network. For managing security of IoT networks the promise of SDN to manage IoT resources makes it a prime candidate for management framework. Contribution in this paper is twofold which are as follows.

1) Identified and discussed management challenges of IoT. Furthermore in this paper security management of IoT is dealt with and security issues, threats, attacks and requirements in IoT are identified.

2) Proposed SDN based framework for provisioning security services over IoT network.

SILO OF THINGS TO INTERNET OF THINGS (IOT)

The current mode of operation in IoT space is very fragmented and silo based. Application specific connected devices mostly have proprietary interconnection and work in a closed system. For example, the alarm system in a smart home is operated by alarm and security companies with dedicated servers and applications specifically to address security concerns of the home and alert stakeholders in case of a security breach. Again, the same home is monitored for utility usage often by different companies and applications (e.g. water, electricity, gas) in a very independent and uncorrelated manner.

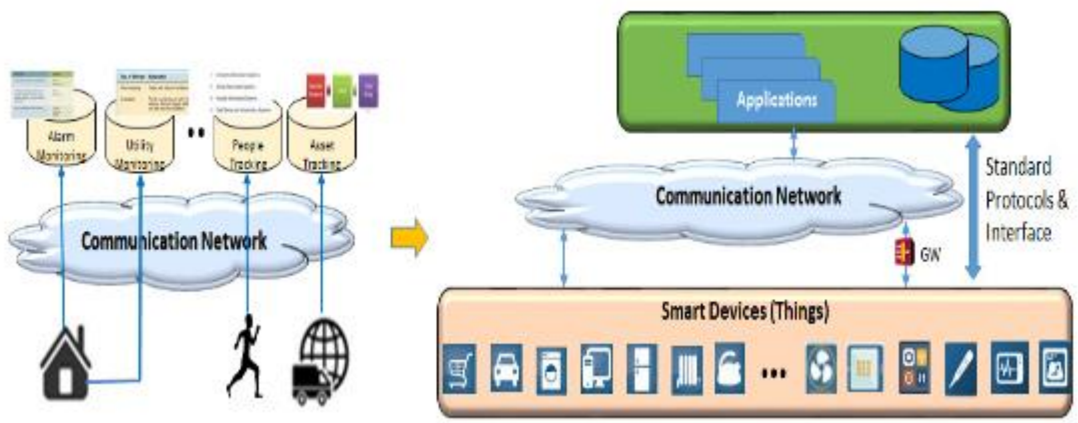

Figure 2: Silo of Things to Internet of Things

IoT has been evolving to meet the challenges of growth of billions of interconnected smart devices in an open system with standard based connectivity for varying capacity and models of smart devices. In an open, non-silo based system, the huge volume of data obtained from smart objects could be used in more intelligent and correlated manner with significant qualitative impact on our daily life, health, communication, and work environment. For example, the food habits of a person in a smart home with data from a smart refrigerator could be correlated with his/her smart health wearable, predicting/inferring appropriate health guidance for the person. Also an open IoT ecosystem shall bring subject matter experts from various domains to effectively contribute and enrich the system. Figure 2 above depicts the transformation of Silo of Things (SoT) to Internet of Things (IoT).

MANAGEMENT CHALLENGES OF IOT

Conventional network management techniques are inapplicable in IoT due to distinctive challenges. An IoT device connected to the internet via gateway is shown in figure 3. CoAP (Constrained Application) protocol running over 6LowPAN is used for communication between gateway and IoT nodes. IoT network devices are not sufficient in resources. Usually in IoT network high fault rates are experienced due to shortfall in energy and connectivity interruptions. To improve the efficiency of the network main concerns are of monitoring and administration of node communication. A typical management solution should provide various management functions integrating configuration, security operation, and administration of devices and services of IoT. Following set of functions should be provided by management solution for IoT.

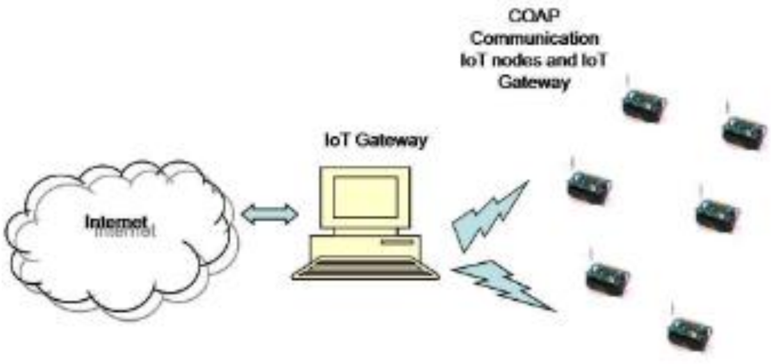

Fig. 3. IoT devices connected with Internet via IoT Gateway

A. Fault Tolerance

Failures are encountered in the IoT network for various reasons. Depletion of batteries is one possibility. Effects on the sensing components results in inaccurate readings disseminated by the devices. Vigorous changes in network topology and a partition in the network is created due to inherent nature of adhoc wireless network links tendency of failures. Due to erroneous nature of communication, delivered packets get corrupted. Packet losses are not experienced due to failures of link but are also caused by congestion. Multihop communication nature of IoT worsens all the fault scenarios discussed. An effort in this direction is summarized in [12].

B. Energy Management

IoT network are deployed in distant region. Due to scarcity of energy resource in IoT and its deployment in distant region depletion of available energy happens frequently. Substitute of energy is impossible. Balanced energy management among supply and load is required to avoid energy scarcity. Data traffic from devices can be controlled to balance energy in the network which is possible by techniques such as duty cycling, scheduling sleep and wake-up modes of devices studied in [13]. Management solution for IoT should address the energy issue by having essential function of energy management for smooth operation of IoT network.

C. Load balancing

Load balancing can be used for extending lifetime of IoT which results in lessening energy utilization. Load balancing is possible by techniques such as clustering. In clustering technique IoT network is organized into cluster which is coordinated by a cluster head. With such configuration there are numerous benefits, such as reduction in routing table size, conservation of network bandwidth, lengthening network lifetime, reduction in redundant data packets and decreasing energy consumption. This makes load balancing an essential component of management solution for IoT. Efforts in this direction can be found in [14].

D. Security Management

Security, privacy and trust are essential requirements in IoT. Due to resource constraint nature of IoT devices the the provisioning of security has become more challenging. A novel technique for provisioning of security is required as conventional security schemes are inapplicable. This poses unique challenges for management framework designer of IoT. Research on security management can be found in [15].

IOT- ARCHITECTURE MODEL

This section describes in detail the generic architectural framework for managing IoT. First we describe various components and their functionality and then realization of same in a cloud based architecture ensuring high scalability and availability. Figure 4 depicts an overall view of IoT ecosystems in general. Smart devices typically connect to Application domain via a communication network. The communication network could be wireless and/or fixed network generally supported by communication service providers (CSP). Typically, constrained IoT devices shall be connected with communication network via gateway, whereas high performance IoT devices could directly connect to communication network itself.

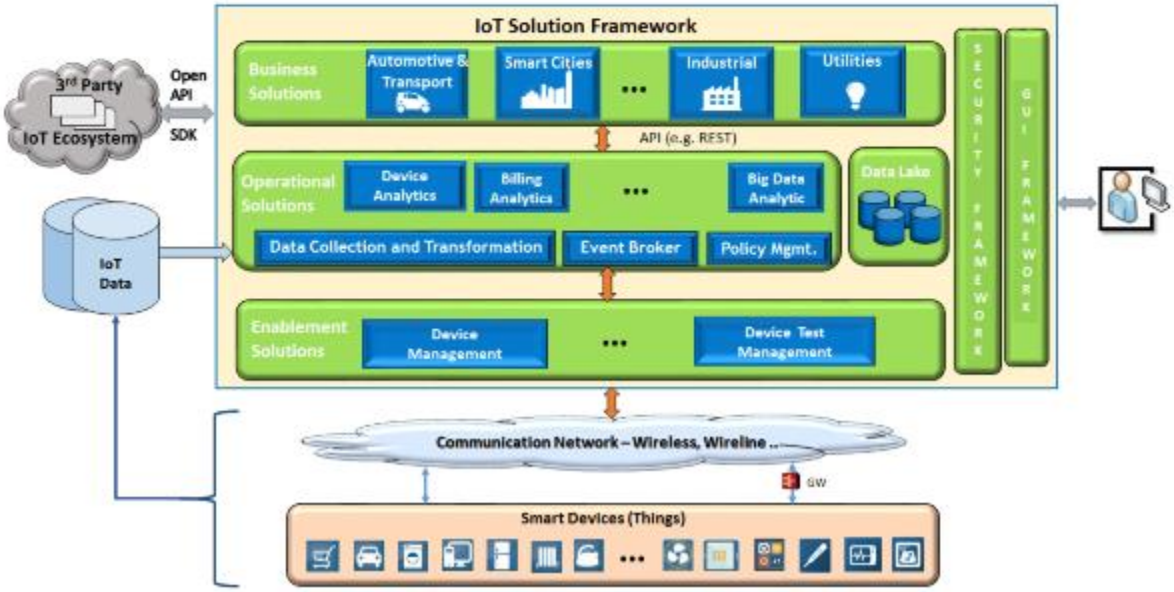

Figure 4: Architectural Framework for Managing IoT

In Figure 4, IoT data refers to IoT device communication related data and IoT device usage specific data. This data could be available from different sources. For example, device communication related data could be available from different operation support systems of communication service provider, whereas device usage specific data could be available from application servers supported by application service providers (e.g., alarm/security service providers for smart home/enterprise). Thus IoT data could be very large, varied data type (text, video, message, etc.) and shall be available over different storage mechanisms (different type of database, files, objects storage, etc.). The reference architecture for IoT solution framework is component based model, where various components and sub-components can be added in plug-and-play mode. Also, components could operate logically in centralized way in a distributed manner on a cloud based platform.

SECURITY THREATS AND ATTACKS IN IOT

This section lists the security threats and attacks, which are applicable to IoT ecosystem. Efforts in summarizing challenges of security in IoT. Detail taxonomy of security challenges can be found in [41].On the other hand, comprehensive identification of security challenges and requirements in IoT architecture. Challenges from all the above efforts are summarized which are required to be addressed by a comprehensive security management solution for IoT. These threats and challenges are given below.

A. Eavesdropping

Because IoT involves wireless communication interface it is obviously vulnerable to eavesdropping. IoT services are expected to contain sensitive data, therefore it is important to protect the data of IoT connected objects against an eavesdropper for possible data leakages. Consider a Smart home environment where IoT objects control and monitor different activities. It is of major importance that the personal information of the smart home owner is kept private and the attacker/eavesdropper is not able to tap the communication between IoT devices.

B. Data Corruption

Instead of eavesdropping or listening to the data, an attacker can also try to modify the data which is transmitted over the air between the IoT devices. A simple motivation here would be to disturb the communication such that the receiving device is not able to understand and process the data sent by the other device. This attack is a simple form of DoS attack where the devices are not been able to perform the required operation over the data. Other than that this attack does not allow the attacker to manipulate the actual data.

C. Data Modification

IoT nodes are expected to exchange critical data with other services and sometime also with intermediate entities i.e. authorities, service providers and control centers. This put stringent requirement that the sensed, stored and transmitted data must not be tampered either maliciously or accidentally. In data modification the attacker is capable of manipulating/modifying the data in such a way that the receiving device is unable to detect modification and treats the input to be valid. This is very different and sophisticated from just data corruption attack. It is crucial to design reliable and dependable IoT applications secure against active modification.

D. Identity Spoofing Attack

IoT device's identity can be compromised through which malicious traffic is sent to victim nodes in the network. This is a devastating attack which can disrupt the normal operation of IoT network. This can also be used to launch DoS and DDoS attacks in the network. There is a strong desire for robust and resilient techniques for validating IoT devices in the network to prevent spoofing.

E. Injection Attack

IoT devices run lightweight code to assist IoT applications in sensing, data collection or performing some activity in a particular region in a field. There is a possibility a malicious code can be injected by the attacker on IoT devices which then perform malicious actions with the intention of disrupting normal operation of IoT network or application. Malicious code can also sabotage IoT device in the network.

F. Denial of Service and Insider Detection in IoT

Emerging technology of IoT experiences severe attacks in IoT. Insider attack is one of the devastating attacks that has received attention from researchers. It is desired to address the issue by incorporating a mechanism in security management framework for IoT.

G. Attacks on Availability

Availability is extremely important for IoT services which enable access from anywhere at any time in order to provide information continuously. Existing security protocols fails to effectively prevent attacks on availability of IoT services. Let's consider an example of Smart Home application, where the sensor nodes are incapable of handling huge number of requests due to resource limitations. Attacker can leverage this limitation to launch DoS attack by sending huge volume of false service requests. Since the wireless transmissions are also battery hungry operation, unnecessary handling of service request will also drain the battery of IoT devices. Security management framework for IoT should be able to mitigate DoS attacks in IoT.

H. Impersonation Attacks

In an IoT ecosystem, both the service provider and service consumer need to make sure that the service is accessed by the authenticated users and it is also offered by an authentic source. It is very crucial to have strong authentication mechanisms deployed to prevent any form of impersonation.

SOFTWARE DEFINED NETWORK BASED FRAMEWORK FOR IOT

The heterogeneity of IoT multi-networks and its complexity is a challenge to organize and to make effective the use of heterogeneous resources with the objective of managing and securing as numerous jobs as possible. The researchers have considered SDN a hot candidate for solving resource management needs of IoT environment. This is due to inherent nature of SDN paradigm which is managed by a centralized controlling agent i.e. controller. Current practical implementation of SDN technologies are long way dealing with diversified and vigorous demands of IoT multi-network. Although, there are various differing SDN based solution for IoT a generic architecture can be constructed from the existing solutions in the literature as shown in Figure 4. In this architecture, IoT applications and services are implemented at application layer. SDN controller related functionalities is implemented at control layer. While IoT devices and gateway exists at infrastructure layer. The control software interacts with the IoT application services at application layer and IoT devices at infrastructure layer using APIs.

CONCLUSION

Advancement in programmable networks have enabled novel paradigm of SDN which have opened opportunities of easing management of networks. Emerging interconnected embedded devices paradigm of IoT is different than conventional wired networks which are usually constrained in resources. Hence, managing such type of network raises challenges which are of unique nature. In this paper, management challenges of IoT are identified and discussed . One of the aspect of management solution for IoT is security provisioning. In this paper, security management of IoT is dealth with. Security threats, attacks, issues and requirements in IoT are discussed which need attention from the researchers. Lately, potentials of SDN to manage IoT is been investigated. It is no doubt that SDN paradigm offer an excellent opportunity to assure security in IoT as security control will be centralized. Hence, in this paper, management framework based on SDN principles for provisioning security services in IoT is proposed. Proposed security controller consists of privacy, trust, key management, IoT and service access authentication and security attack mitigation agent module. Privacy module ensures privacy is preserved in IoT. Trust module makes sure that the communication in IoT network takes place in a trusted environment. Key management module handles key generation and revocation in IoT network. IoT and service access authentication authenticates nodes and services within IoT network. Security attack mitigation agent detects attacks in the network and takes countermeasure actions to prevent attacks. In the end, how the security attacks and threats in IoT are handled by the proposed SDN based framework is discussed. In the future, each module will be implemented and evaluated in the framework with respect to overall overheads and resource consumption.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1389128610001568

[2] A. Levakov and N. Sokolov, “Internet of Things, Smart Spaces, and Next Generation Networking,” Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 7469, no. January, pp. 424–428, 2012. [Online]. Available: http://www.scopus.com/inward/record.url?eid=2- s2.0-84866127166&partnerID=tZOtx3y1

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (iot): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[4] Hai Huang, Jiping Zhu, and Lei Zhang, “An SDN based management framework for IoT devices,” 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies (ISSC 2014/CIICT 2014), pp. 175–179, 2014. [Online]. Available: http://digitallibrary.theiet.org/content/conferences/10.1049/cp.2014.0680

[5] O. Flauzac, C. Gonzalez, A. Hachani, and F. Nolot, “SDN Based Architecture for IoT and Improvement of the Security,” 2015 IEEE 29th International Conference on Advanced

Information Networking and Applications Workshops, pp. 688–693, 2015. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7096257

[6] N. Omnes, M. Bouillon, G. Fromentoux, and O. L. Grand, "A Programmable and Virtualized Network & IT Infrastructure for the Internet of Things," pp. 64–69, 2015.

[7] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian, "A software defined networking architecture for the internet-ofthings," IEEE/IFIP NOMS 2014 - IEEE/IFIP Network Operations and Management Symposium: Management in a Software Defined World, pp. 1–9, 2014.

[8] P. Hu, "A System Architecture for the Software-Defined Industrial Internet of Things," Icuwb'15, p. To appear, 2015.

[9] Y. Jararweh, M. Al-Ayyoub, A. Darabseh, E. Benkhelifa, M. Vouk, and A. Rindos, "SDIoT: a software defined based internet of things framework," Journal of Ambient Intelligence and Humanized Computing, vol. 6, no. 4, pp. 453–461, 2015. [Online]. Available: http://link.springer.com/10.1007/s12652-015-0290-y

[10] V. R. Tadinada, "Software Defined Networking: Redefining the Future of Internet in IoT and Cloud Era," 2014 International Conference on Future Internet of Things and Cloud, pp. 296–301, 2014. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6984209

[11] N. Feamster, J. Rexford, and E. Zegura, "The Road to SDN: An Intellectual History of Programmable Networks," ACM Sigcomm Computer Communication, vol. 44, no. 2, pp. 87–98, 2014.

[12] D. Wajgi and N. V. Thakur, "Load Balancing Algorithms in Wireless Sensor Network : A Survey," IRACST International Journal of Computer Networks and Wireless Communications, vol. 2, pp. 2250–3501, 2012.