Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 9, Issue, 1(G), pp. 23340-23344, January, 2018

ISSN: 0976-3031

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

IOT SECURITY ISSUES - A SURVEY

Vishnu Priya K*., Muthuselvi S and Ebenezer Juliet S

Department of Computer Science VV College of Engineering
Tuticorin Tamil Nadu, India

DOI: http://dx.doi.org/10.24327/ijrsr.2018.0901.1449

ARTICLE INFO

Article History:

Received 16th October, 2017
Received in revised form 25th November, 2017
Accepted 23rd December, 2017
Published online 28th January, 2018

Key Words:

Internet of Things (IoT), security issues, security and Trust.

ABSTRACT

The Internet of Things (IoT) is the combination of devices such as software, sensors and electronics, communicates through wireless technology. The key enabling applications of Internet of things are smart healthcare system, smart grid, intelligent transportation, smart building, retail, military and business. Internet of Things (IoT) has received a considerable research attention in recent years. As the population increases drastically, the data has to be processed digitally and automatically. It is expected that, the importance of Internet of Things may rise rapidly in the upcoming years. Due to the increased usage of IoT devices, the IoT networks are prone to the security issues. The IoT network must ensure Authentication, Access control, Privacy, Policy Enforcement, Trust, Mobile security, Secure Middleware, Confidentiality. This paper provides a comprehensive study on security and policy issues in IoT.

INTRODUCTION

Due to the fact that world urbanization continues to grow with the expected total population doubling by 2050, there is a worldwide trend towards Internet of Things. In IoT, data are collected from various physical sensors, transmitted over wireless networks, and then analyzed in a real-time manner. The sensed and analyzed data will be utilized to control actuators. IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit. "Things," in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/ pathogen monitoring or field operation devices that assist fire-fighters in search and rescue operations. These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices.

Internet of Things is not the result of a single novel technology; instead, several complementary technical developments provide capabilities that taken together help to bridge the gap between the virtual and physical world. These capabilities include: Communication and cooperation, Addressability, Identification, Sensing, Actuation, Embedded information processing, Localization, User interfaces.

The IoT is used in various applications such as Smart Home, Wearables, Industrial Internet, Smart Cities, IoT in agriculture, Smart Retail, Energy Engagement, IoT in Healthcare and IoT in Poultry and Farming.

The rest of the paper is organised as: Section II discusses the security requirements followed by the analysis of security issues in section III. Section IV provides the summary of the analysis and finally section V concludes the brief study.

Security Challenges

As the communications between the devices in Internet of Things are through wireless network, it may experience some of the following challenges (developer.ibm.com).

Secure Constrained Devices

Security approaches that rely heavily on encryption are not a good fit for the devices that run on batteries, because they are not capable of performing complex encryption and decryption quickly enough to be able to transmit data securely in real-time.

Corresponding author:* **Vishnu Priya K
Department of Computer Science VV College of Engineering Tuticorin Tamil Nadu, India

Authorize and Authenticate Devices

The process of authorization and authentication is critical for securing IoT systems which prevents the unauthorized person from accessing the device and data by enforcing the use of strong passwords or certificates.

Manage Device Updates

Not all devices support over-the-air updates, or updates without downtime, so devices might need to be physically accessed or temporarily pulled from production to apply updates. Also, updates might not be available for all devices, particularly older devices or those devices that are no longer supported by their manufacturer.

Secure communication

Communication across the network between devices and cloud services or apps is insecure because many IoT devices don't encrypt messages before sending them over the network.

Ensure Data Privacy and Integrity

It is also important that wherever the data ends up after it has been transmitted across the network, it is stored and processed securely. Implementing data privacy includes redacting or anonymizing sensitive data before it is stored or using data separation to decouple personally identifiable information from IoT data payloads. Data that is no longer required should be disposed of securely, and if data is stored, maintaining compliance with legal and regulatory frameworks is also an important challenge.

Secure web, mobile, and cloud applications

Web, mobile, and cloud apps and services are used to manage, access, and process IoT devices and data, so they must also be secured as part of a multi-layered approach to IoT security.

Ensure high availability

The impact of the lack of availability could mean loss of revenue, damage to equipment, or even loss of life. To ensure high availability, IoT devices must be protected against cyber-attacks as well as physical tampering. IoT systems must include redundancy to eliminate single points of failure, and should also be designed to be resilient and fault tolerant, so that they can adapt and recover quickly when problems do arise.

Detect vulnerabilities and incidents

In large scale IoT systems, the complexity of the system in terms of the number of devices connected, and the variety of devices, apps, services, and communication protocols involved, can make it difficult to identify when an incident has occurred.

Manage Vulnerabilities

The complexity of IoT systems also makes it challenging to identify which devices were affected, what data or services were accessed or compromised and which users were impacted, and then taking actions to resolve the situation.

10. Predict and preempt security issues. A longer-term IoT security challenge is to apply security intelligence not only for detecting and mitigating issues as they occur, but also to predict and proactively protect against potential security threats.

Analysis of Security Issues

A brief study of security issues in various work has been discussed in this section. Policy-based Secure and Trustworthy Sensing for Internet of Things in Smart Cities (Wenjia Li er al, 2017) developed by Wenjia Li, Houbing Song and Feng Zeng to address the security issues in IoT. The trustworthiness of both data and the IoT devices are evaluated based on both the reporting history and the context in which the data are collected using policy rules. Finally Dempster Shafer's Theory is used to fuse the report from various sensor nodes to detect the untrustworthy sensor node.

W. Li and H. Song presented an Attack Resistant Trust Management scheme (ART) for VANETs that is able to detect and cope with malicious attacks and also evaluate the trustworthiness of both data and mobile nodes in VANETs (Wenjia Li *et al*, 2016). Specially, data trust is evaluated based on the data sensed and collected from multiple vehicles; node trust is assessed in two dimensions, i.e., functional trust and recommendation trust, which indicate how likely a node can fulfil its functionality and how trustworthy the recommendations from a node for other nodes will be, respectively. ART evaluate the trustworthiness of data and node as two separate metrics, namely data trust and node trust, respectively. In particular, data trust is used to assess whether or not and to what extent the reported traffic data are trustworthy. On the other hand, node trust indicates how trustworthy the nodes in VANETs are.

Z. A. Khan and P. Herrmann revealed a Intrusion Detection Systems (IDS) which helps to retrieve various forms of network attacks for distributed systems, e.g., the denial of service attacks and also IDS try to find abnormalities in the overall behaviour which may be an indication for attacks (Z. A. Khan *et al*, 2017). They use a trust management mechanism that allows devices and manage reputation information about their neighbours. Neighbour Based Trust Dissemination (NBTD), Clustered Neighbour Based Trust Dissemination (CNTD), Tree Based Trust Dissemination (TTD) algorithm are used to find the abnormalities in the network. NBTD calculates trust values periodically based on the trust inputs received from the nodes in the DODAG. In CNTD, the cluster-head is responsible to gather and compute the reputation of each node in its cluster. TTD supervises its parents but not children in order to save network overhead.

D. McCoy, D. Sicker, and D. Grunwald discovered a new Misbehaving Node Detection (MIND) Mechanism is based on a reputation enabled intrusion detection system, in which a centralized trust authority monitors traffic and collects second hand information on potentially misbehaving nodes (D. McCoy *et al*,2007). MIND mechanism integrates policy, detection, and remediation components for identifying and handling misconfigured, misbehaving, or malicious devices. XML based policy engine is used to detect policy violations. These mechanisms are built to be flexible and extensible in order to deal with the issues arising out of software programmable devices. An XML based policy engine is used to detect policy violations including DoS and active attacks against the network Detection policies are transformed into wireless snort rules to enable detection of policy violations. The centralized authority integrates a mixture of alarms generated by the wireless snort system and reports from authenticated devices to create a global reputation vector and their local trust vector to decide what level of trust to assign to a device.

W. Li and A. Joshi exposed an Outlier detection technique which helps to either eliminate or amplify outliers and to observe and record the abnormal behaviours of the neighbours in MANETs (W. Li *et al*, 2009). Outlier detection algorithm identifies the top *k* outliers in terms of some abnormal behaviours observed by neighbours, such as packet drops or modifications. The outlier detection algorithm has the following four steps, viz. local view formation, local view exchange, view combination, and global view formation. Prior to the local view formation, each node observes and record the behaviours of their neighbours, and also keeps track of the total number of incoming packets each of their neighbours has. Based on their observations, the initial local view of outliers is generated. Once all the nodes form their initial local views, they broadcast their initial local views to all of their immediate neighbours, i.e., all the nodes that are within their direct radio transmission ranges. When a node receives a local view from one of its neighbours, it then checks whether the incoming view differs from its own local view. If so, it combines the two views, and rebroadcasts the combined view to its immediate neighbours. If not, it simply retains its local view and keeps silent. The Dempster-Shafer Theory is used to fuse the local views.

Guoxing Zhan, Weisong Shi, Julia Deng presented TARF, a robust trust aware routing framework for dynamic WSNs which secures the WSNs against adversaries misdirecting the multihop routing (Guoxing Zhan *et al*, 2012). Without tight time synchronization or known geographic information, TARF provides trustworthy and energy-efficient route. Most importantly, TARF proves effective against those harmful attacks developed out of identity deception. It identifies such intruders by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory throughput. Trust Manager is responsible for tracking trust level values of neighbours based on network loop discovery and broadcast messages from the base station about data delivery. Once N is able to decide its next-hop neighbour according to its neighbourhood table, it sends out its energy report message: it broadcasts to all its neighbours its energy cost to deliver a packet from the node to the base station. For each neighbour b of N, T_{Nb} denotes the trust level of b in N's neighbourhood table. At the beginning, each neighbour is given a neutral trust level 0.5. After any of those events occurs, the relevant neighbours' trust levels are updated.

Daojing He, Sammy Chan and Mohsen Guizani developed a novel protocol, named APAC is used to hide the users data access privacy from anyone else including the network owner and, at the same time, identifies the misbehaving users (Daojing He *et al*,2015). First, APAC can enforce strict access control so that the sensed data is only accessible by the authorized users. Second, APAC offers sophisticated user privacy protection. Third, misbehaving users or owners can be audited and pinpointed. Last but not least, it does not rely on the existence of a trusted third party, and thus is more feasible in practice.The trust and key management model adopted for APAC does not assume the existence of a trusted third party. Before accessing the network, each user has to enroll in at least one user group whose manager thus knows the identity of the user. For the whole network, the law authority generates partial group public key and partial group private key, and then allocates the former one to each group manager and keeps the latter one secretly. With partial group public key from the law authority, the group manager generates the full group public key and the other partial group private key, and keeps the latter one secretly. To access the network, each user generates partial member secret key and then requests the other partial member secret key and group public key from his/her group manager. Each group manager distributes the corresponding group public key to the sink and sensor nodes before network deployment. Additionally, according to the agreement among network owners, the access privilege of each group is pre-loaded on each node. Without the help of the group manager, the law authority cannot compromise the privacy of any user. Also, without the full member secret key, both the law authority and network owners cannot impersonate any legitimate user. Finally, in case of service disputes or frauds, the law authority can collect the partial group private key and the identities of users from the corresponding network owner to pinpoint the responsible user.

Yu Zhang, Loukas Lazos, William Jr. Kozma presented an Audit-based Misbehaviour Detection (AMD) which addresses the problem of identifying and isolating misbehaving nodes that refuse to forward packets in multi-hop ad hoc networks (Yu Zhang *et al*, 2016). AMD effectively and efficiently isolates both continuous and selective packet droppers. The AMD system integrates reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavioural audits. These modules closely interact to coordinate the functions of misbehaviour detection, discovery of trustworthy routes, and evaluation of the reputation of peers. The reputation module is responsible for managing reputation information based on the recommendations of the audit module. Reputation values are exploited by the route discovery module for establishing routes that exclude nodes with low reputations. Finally, the audit module efficiently identifies misbehaving nodes via an audit process. This process is accelerated based on input received from the reputation module.

Tian Wang, Yang Li, Yonghong Chen, et.al revealed a Fog-Based Evaluation Approach to identify malicious attacks that can cause sensor communications to become unreliable and to improve the compatibility, verifiability and accuracy of trust evaluation (Tian Wang *et al*, 2015). Establishing the relationship between sensor's behaviour and its trust value is similar to a multiple linear regression problem. Therefore, Least squares algorithm is used to find the fitting function between the communication feature and the trust value. The fog nodes compute the trust value based on the feature set and return the result to sensors. A universal trust model based on the sensor's communication history feature sets are first established. Then, when sensors upload communication features to fog nodes during each upload interval, the fog nodes compute the trust value of the communications and divide the sensors into three classes: credible nodes, suspect nodes and unbelievable nodes.

Summary

Methodology	Security Issue	Algorithm Used	Application	Advantages	Disadvantages
Policy Based Trustworthy Scheme	Bad Mouth Attack On and Off Attack	Dempster Shafer's Theory	Smart City	Detect malicious nodes Detects trustworthiness of data	Accuracy decreases as the number of attackers increases. Low recall rate
An Attack Resistent Trust Management Scheme	Malicious Attacks Zig Zag Attack	ART	Smart Vehicular System	Better resistant to various attack patterns. Improve traffic safety, mobility, and environmental protection with enhanced trustworthiness.	Approach gets significantly degraded when the percentage of the attackers who follow Zig Zag pattern increases.
Intrusion Detection Systems	DoS Attacks	NBTD, CNTD, TTD	IoT Nerwork	Reduces the computing efforts for the small devices. Detects previously unknown attacks.	Very high overhead in terms of network load. Accuracy is high only for small devices.
MIND Technique	Policy Violation Attack	XML based Policy Algorithm	Smart Heealthcare System	The trust computations are lightweight. Flexible and Extensible	Takes longer time to remove malicious node.
Outlier Detection Algorithm	Packet Drop, Data Integrity	Weighted Voting Method, Dempster Shafer's Theory	Smart Transportation	Highly resilient to attackers	Performance gets significantly degraded when there is a higher percentage of malicious nodes.
TARF	Misdirecting the Multi-hop Routing	Network loop Discovery	Routing Framework in WSN	Energy Efficient Highly Scalable	Attacks such as the DoS cannot be addressed.
APAC	Privacy issues	Trust and Key Management Model	Data Transfer in IoT	User privacy is enhanced. User accountability is achieved.	Trust between entities is limited. Computational complexity is high.
AMD	Authentication and integrity issues.	Reputation and Audit Management	Multihop Routing in WSN	Prevent user impersonation, message modification attacks, integrity and authenticity	AMD incurs overhead
Fog Based Evaluation Approach	Malicious Node Attacks, Compatibility issues	Least Square Algorithm.	Area Monitoring	Improve compatibility and verifiability of trust evaluation Accurate trust evaluation	Incorrect feature selection leads to inaccurate trust evaluation.

If a sensor is judged as an unbelievable node, the fog node broadcasts that information to the other sensors. Subsequently, the unbelievable node cannot gain access to resources, such as channels, data, and so on.

F. J. Wu and H. B. Lim developed a Smartphone based mobility sensing system, called Urban Mobility Sense, which captures human mobility information automatically to conduct transportation activity surveys (F. J. Wu *et al*,).The Urban Mobility Sense system was designed to address two critical issues: 1) energy conservation and 2) privacy preservation. To optimize the energy utilization of smart phone, it avoids using the GPS sensor when the user is at long-stay places and filter out redundant data before data uploading. To preserve personal privacy, each smart phone maintains the user's long-stay places by two separate profiles: 1) private place profile and 2) public place profile. The former maintains the privacy-preserved places (e.g., home), whereas the latter maintains the public places (e.g., parks).

CONCLUSION

The main theme of this paper was to expose the security issues in Internet of Things. Due to the lack of security mechanisms in IoT, the intruders may compromise the IoT devices to generate fake data which sometimes leads to disastrous situation. In this survey some of the important security issues and their countermeasures are discussed.

Considering the importance of security in IoT applications, it is really mandatory to install security mechanism in IoT devices and communication networks. Moreover, to protect the IoT devices from any intruders or security threat, it is also recommended not to use default passwords for the devices and read the security requirements for the devices before using it for the first time. And, it is important to study different security protocols used in IoT devices and networks.

References

https://developer.ibm.com/dwblog/2017/iot-security-challenges/

Wenjia Li, Houbing Song and Feng Zeng (2017), "Policy-based Secure and Trustworthy Sensing for Internet of Things in Smart Cities," IEEE Internet Of Things Journal.

W. Li and H. Song (2016), "Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks," IEEE Transactions on Intelligent Transportation Systems.

Z. A. Khan and P. Herrmann (2017), "A trust based distributed intrusion detection mechanism for internet of things," IEEE 31st International Conference on Advanced Information Networking and Applications (AINA).

D. McCoy, D. Sicker, and D. Grunwald (2007), "A mechanism for detecting and responding to misbehaving nodes in wireless networks," 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks.

W. Li and A. Joshi (2009), "Outlier detection in ad hoc networks using dempster-shafer theory," in Proceedings of the Tenth International Conference on Mobile Data Management: Systems, Services and Middleware, 2009. MDM '09. IEEE Computer Society.

Guoxing Zhan, Weisong Shi, Julia Deng (2012), "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs" IEEE Transactions On Dependable And Secure Computing.

Daojing He, Sammy Chan and Mohsen Guizani (2015), “Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks”, IEEE Transactions on Wireless Communications.

Yu Zhang, Loukas Lazos, William Jr. Kozma (2016), “AMD: Audit-Based Misbehavior Detection in Wireless Ad Hoc Networks”, IEEE Transactions on Mobile Computing.

Tian Wang, Yang Li, Yonghong Chen, Hui Tian, Yiqiao Cai, Weijia Jia, Baowei Wang (2015), “Fog-Based Evaluation Approach for Trustworthy Communication in Sensor-Cloud System”, *Journal of Latex Class Files*.

F. J. Wu and H. B. Lim (2014), “Urban Mobility Sense: A user-centric participatory sensing system for transportation activity surveys,” IEEE Sensors.

How to cite this article:

Vishnu Priya K., Muthuselvi S and Ebenezer Juliet S.2018, Iot Security Issues - A Survey. *Int J Recent Sci Res.* 9(1), pp. 23340-23344. DOI: http://dx.doi.org/10.24327/ijrsr.2018.0901.1449

****