EFFECTIVE ANALYSIS OF RISKS AND VULNERABILITIES IN INTERNET OF THINGS

Shradha Jain
M.Tech. Research Scholar
Computer Science and Engineering
Ambala College of Engineering and Applied Research
Mithapur, Ambala, Haryana, India

Ashok Kajal
Assistant Professor and Research Guide
Computer Science and Engineering
Ambala College of Engineering and Applied Research
Mithapur, Ambala, Haryana, India

ABSTRACT
The Internet of Things (IoT) is the incorporation of gadgets and software in any gadget not typically viewed as mechanized in nature, to empower it to accomplish more noteworthy esteem and administration by providing for it a capacity to system and correspond with different gadgets. Everything is particularly identifiable through its installed processing gadget however has the capacity interoperate inside the current Internet base. Ordinarily, IoT
Internet of Things (IoT) is one of the recent technologies in current era that focus on the interconnection of every object in the real world. We can imagine the real life objects with embedded computing devices and communicating with each other. By this technology, we can track everything from remote location using Internet infrastructure. Using IoT, the interconnection in every system, device, machine, human being, home equipments, office products can be established using existing network resources. As an example or case of IoT, we can track any train by using the messaging service of Indian Railways. As per the instructions, we can send the message to a specific short code. After this message, we get the

Keywords - Internet of Things, Security in Sensor Networks

INTRODUCTION
The Internet of Things (IoT) is one of the recent technologies in current era that focus on the interconnection of every object in the real world. We can imagine the real life objects with embedded computing devices and communicating with each other. By this technology, we can track everything from remote location using Internet infrastructure. Using IoT, the interconnection in every system, device, machine, human being, home equipments, office products can be established using existing network resources. As an example or case of IoT, we can track any train by using the messaging service of Indian Railways. As per the instructions, we can send the message to a specific short code. After this message, we get the

Approved by Council of Scientific and Industrial Research, Ministry of Science and Technology, Govt. of India
exact location and upcoming station of that train. In the same way, many taxi or cab services are trying to utilize and implement IoT. Currently, many taxi operators are connected with GPS and we can track the location of that car on mobile phone, tablet or any network connected device. Smart Cities, Smart Home are implemented using IoT in which everything is connected and searchable.

At the base level, IoT makes use of sensors and embedded chips which are inserted in the system that we want to monitor and track. RFID (Radio Frequency Identification) based devices are classically used for IoT implementation. The Things, in IoT, refers to a wide variety of devices such as heart monitoring implants, biochip transponders deployed with patients for remote monitoring and prescription, animals, electric clams in coastal waters, automobiles with built-in sensors, or field operation devices that assist fire-fighters in search and rescue. Current market examples include smart thermostat systems and washer or dryers that utilize wifi for remote monitoring.

The Internet of Things (IoT) is that the network of physical objects or "things" embedded with physics, software, sensors and property to change it to attain bigger worth and repair by exchanging knowledge with the manufacturer, operator and/or different connected devices. Every issue is unambiguously recognisable through its embedded computer system however is in a position to interoperate inside the prevailing net infrastructure.

Real Life Implementations and Applications of IoT
From building and home automation to wearables, the IoT touches every facet of our lives. Many corporate giants including Texas Instruments, Cisco, Ericsson, Freescale, GE are working in the development as well as deployment of IoT scenarios. The companies are making and developing the applications easier with hardware, software and support to get
anything connected within the IoT. A set of key markets exists for the IoT with potential for exponential growth.

- Medical and healthcare systems
- Building and home automation
- Transportation
- Wearables - Smart watch for Location and tracking
- Building & home automation
- Smart cities
- Smart manufacturing
- Employee safety
- Predictive maintenance
- Health care
- Remote monitoring
- Ambulance telemetry
- Drug tracking
- Hospital asset tracking
- Access control
- Automotive

**Open Source Cloud Platforms for Internet of Things**

Numbers of open source platforms are available to simulate the IoT infrastructure and related protocols.

**OpenIoT** - OpenIoT is an open source middleware for getting information from sensor clouds, without worrying what exact sensors are used. OpenIoT is now included in the teaching program (syllabus) of Santa Clara University, CA, USA. The master program includes theory in Internet of Things and practical experience. OpenIoT among other IoT tools from CISCO, ARM etc are pioneers in this program in the University. Dr Martin
Serrano from the OpenIoT project will be teaching IoT principles and also facilitate lab experiments and projects for the students that will be using the OpenIoT middleware. This is the first wide adoption of OpenIoT in education and outside of Europe. [Source - http://openiot.eu]

OpenIoT is a joint effort of prominent open source contributors towards enabling a new range of open large scale intelligent IoT (Internet-of-things) applications according to a utility cloud computing delivery model. OpenIoT is perceived as a natural extension to cloud computing implementations, which will allow access to additional and increasingly important IoT based resources and capabilities. In particular, OpenIoT provides the means for formulating and managing environments comprising IoT resources, which can deliver on-demand utility IoT services such as sensing as a service.

OpenIoT is pertinent to a wide range of interrelated scientific and technological areas spanning:

(a) Middleware for sensors and sensor networks,
(b) Ontologies, semantic models and annotations for representing internet-connected objects, along with semantic open-linked data techniques
(c) Cloud/Utility computing, including utility based security and privacy schemes.

From a more technical point of view, the OpenIoT middleware infrastructure allows flexible configuration and deployment of algorithms for collection, and filtering information streams stemming from the internet-connected objects, while at the same time generating and processing important business/applications events.

Power firms scan meters through tele-metering systems rather than visiting houses; doctors remotely monitor the conditions of their patients 24/7 by having the patients use devices reception rather than requiring the patients to remain at hospital; vehicle-mounted terminals
mechanically show the closest parking space; sensors in good homes put off utilities, shut windows, monitor security, and report back to owners in real time. These are situations that solely existed in fantasy antecedently. With the approaching mature of the net of Things, however, they're changing into a reality.

Also known as M2M standing for Machine to Machine, Machine to Man, Man to Machine, or Machine to Mobile, the net of Things showing intelligence connects humans, devices, and systems. Thought-about as another IT wave following computers, the net, and mobile communications, it represents the top of our current ICT ambitions.

The ITU states that the goal of ICT is to attach all objects on the premise of networked people to create a present network, that is termed the net of Things. In layman's terms, this network covers all everyday objects like watches, keys, family appliances, cars, and buildings.

**AllJoyn**

Originally created by Qualcomm, this open source operating system for the Internet of Things is now sponsored by one of the most prominent IoT organizations - The AllSeen Alliance, whose members include the Linux Foundation, Microsoft, LG, Qualcomm, Sharp, Panasonic, Cisco, Symantec and many others. It includes a framework and a set of services that will allow manufacturers to create compatible devices. It's cross-platform with APIs available for Android, iOS, OS X, Linux and Windows 7.

**Contiki**

Contiki is the open source OS for the Internet of Things. It connects low-power microcontrollers to the internet and supports standards like IPv6, 6lowpan, RPL and CoAP. Other key features include highly efficient memory allocation, full IP networking, very low power consumption, dynamic module loading and more. Supported hardware platforms
include Redwire Econotags, Zolertia z1 motes, ST Microelectronics development kits and Texas Instruments chips and boards. Paid commercial support is available.

**Raspbian**

While the Raspberry Pi was intended as an educational device, many developers have begun using this credit-card-sized computer for IoT projects. The complete hardware specification is not open source, but much of the software and documentation is. Raspbian is a popular Raspberry Pi operating system that is based on the Debian distribution of Linux.

**RIOT**

RIOT bills itself as "the friendly operating system for the Internet of Things." Forked from the FeuerWhere project, RIOT debuted in 2013. It aims to be both developer- and resource-friendly. It supports multiple architectures, including MSP430, ARM7, Cortex-M0, Cortex-M3, Cortex-M4, and standard x86 PCs.

**Huge market potential**

The Internet of Things is probably going to possess a staggering impact on our daily lives. It will greatly improve productivity and our lives. And unsurprisingly, its nice market potential is attracting investments from governments, medium operators, makers, and business users.

**Building and home automation**

IoT devices is wont to monitor and management the mechanical, electrical and electronic systems utilized in numerous kinds of buildings (e.g., public and personal, industrial, establishments, or residential). Home automation systems, like alternative building automation systems, area unit usually wont to management lighting, heating, ventilation, air-
con, appliances, communication systems, recreation and residential security devices to enhance convenience, comfort, energy potency, and security.

**Devicehub.net**
Devicehub.net is the open source backbone for the Internet of Things. It's a cloud-based service that stores IoT-related data, provides visualizations of that data and allows users to control IoT devices from a Web page. Developers have used the service to create apps that track health information, monitor the location of children, automate household appliances, track vehicle data, monitor the weather and more.

**IoT Toolkit**
The group behind this project is working on a variety of tools for integrating multiple IoT-related sensor networks and protocols. The primary project is a Smart Object API, but the group is also working on an HTTP-to-CoAP Semantic mapping, an application framework with embedded software agents and more. They also sponsor a meetup group in Silicon Valley for people who are interested in IoT development.

**Mango**
Mango bills itself as "the world's most popular open source Machine-to-Machine (M2M) software." Web-based, it supports multiple platforms. Key features include support for multiple protocols and databases, meta points, user-defined events, import/export and more.

**Nimbits**
Nimbits can store and process a specific type of data—data that has been time- or geo-stamped. A public platform as a service is available, or you can download the software and deploy it on Google App Engine, any J2EE server on Amazon EC2 or on a Raspberry Pi. It supports multiple programming languages, including Arduino, JavaScript, HTML or the Nimbits.io Java library.
OpenRemote
OpenRemote offers four different integration tools for home-based hobbyists, integrators, distributors, and manufacturers. It supports dozens of different existing protocols, allowing users to create nearly any kind of smart device they can imagine and control it using any device that supports Java. The platform is open source, but the company also sells a wide variety of support, ebooks and other tools to aid in the design and product development process.

SiteWhere
This project provides a complete platform for managing IoT devices, gathering data and integrating that data with external systems. SiteWhere releases can be downloaded or used on Amazon’s cloud. It also integrates with multiple big data tools, including MongoDB and ApacheHBase.

ThingSpeak
ThingSpeak can process HTTP requests and store and process data. Key features of the open data platform include an open API, real-time data collection, geolocation data, data processing and visualizations, device status messages and plugins. It can integrate multiple hardware and software platforms including Arduino, Raspberry Pi, ioBridge/RealTime.io, Electric Imp, mobile and Web applications, social networks and MATLAB data analytics. In addition to the open source version, a hosted service is also available.

Arduino
Arduino is both a hardware specification for interactive electronics and a set of software that includes an IDE and the Arduino programming language. Arduino is a specialized tool for making computers than can sense and control more of the physical world than your desktop computer.
Eclipse IoT Project
Eclipse is sponsoring several different projects surrounding IoT. They include application frameworks and services; open source implementations of IoT protocols, including MQTT CoAP, OMA-DM and OMA LWM2M; and tools for working with Lua, which Eclipse is promoting as an ideal IoT programming language. Eclipse-related projects include Mihini, Koneki and Paho. The website also includes sandbox environments for experimenting with the tools and a live demo.

Kinoma
Owned by Marvell, the Kinoma software platform encompasses three different open source projects. Kimona Create is a DIY construction kit for prototyping electronic devices. Kimona Studio is the development environment that works with Create and the Kinoma Platform Runtime. Kimona Connect is a free iOS and Android app that links smartphones and tables with IoT devices.

M2MLabs Mainspring
Designed for building remote monitoring, fleet management and smart grid applications, Mainspring is an open source framework for developing M2M applications. It capabilities include flexible modeling of devices, device configuration, communication between devices and applications, validation and normalization of data, long-term data storage, and data retrieval functions. It's based on Java and the Apache Cassandra NoSQL database.

Node-RED
Built on Node.js, Node-RED describes itself as "a visual tool for wiring the Internet of Things." It allows developers to connect devices, services and APIs together using a browser-based flow editor. It can run on Raspberry Pi, and more than 60,000 modules are available to extend its capabilities.
RESEARCH AREAS IN THE DOMAIN OF INTERNET OF THINGS

As the domain of IoT is much diversified, there is lots of scope of research for the scholars and practitioners.

In IoT, the following research areas can be worked out by the research scholars -

• Security and Privacy Issues in smart objects
• Resource Oriented Architecture
• Cloud of Things
• Cross Platform Compatibility and Efficiency Issues
• Quality of Service
• Fog Computing and its association with IoT
• Social Structure of IoT
• Compatibility and Adaptability of IoT with IPV6 and upcoming technologies

SECURITY ISSUES

A different criticism is that the Internet of Things is being developed rapidly without appropriate consideration of the profound security challenges involved and the regulatory changes that might be necessary. According to the BI (Business Insider) Intelligence Survey conducted in the last quarter of 2014, 39% of the respondents said that security is the biggest concern in adopting Internet of Things technology. In particular, as the Internet of Things spreads widely, cyber attacks are likely to become an increasingly physical (rather than simply virtual) threat. In a January 2014 article in Forbes, cybersecurity columnist Joseph Steinberg listed many Internet-connected appliances that can already "spy on people in their own homes" including televisions, kitchen appliances, cameras, and thermostats. Computer-controlled devices in automobiles such as brakes, engine, locks, hood and truck releases, horn, heat, and dashboard have been shown to be vulnerable to attackers who have access to the onboard network. (These devices are currently not connected to external computer networks, and so are not vulnerable to Internet attacks.)
The U.S. National Intelligence Council in an unclassified report maintains that it would be hard to deny "access to networks of sensors and remotely-controlled objects by enemies of the United States, criminals, and mischief makers… An open market for aggregated sensor data could serve the interests of commerce and security no less than it helps criminals and spies identify vulnerable targets. Thus, massively parallel sensor fusion may undermine social cohesion, if it proves to be fundamentally incompatible with Fourth-Amendment guarantees against unreasonable search." In general, the intelligence community views Internet of Things as a rich source of data.

ASSORTED ATTACKS AND VULNERABILITIES

Malicious node is one which causes attacks on various layers on IOT like application layer, data link layer, physical and network layer.

There were two types of attacks on IOT, they are

- Active attacks
- Passive attacks

**Active attacks** - In this attack, some harmful information is injected into the network, which causes malfunctioning of the other nodes or network operation. For performing this harmful information it consumes some sort of energy from other nodes, those nodes are called as malicious node.

**Passive attacks** - In this passive attack, the malicious nodes disobey to perform its task for some sort reasons like saving energy for its own use of moving randomly, by diminishing the performance of the network.
Wormhole attack

Wormhole attack is also known as tunnelling attack, in this tunnelling attack the colluding attackers build tunnel between the two nodes for forwarding packets claiming that providing shortest path between the nodes and taking the full control of the nodes, which is invisible at the higher layers.

Black hole attack

Black hole attack is the serious problem for the MANETs, in this problem a routing protocol has been used by malicious node reports itself stating that it will provides shortest path.

In flooding based protocol, a fake route is created by the malicious node rather than the actual node, which results in loss of packets as well as denial of service (DoS).

Resource consumption attack

In the resource consumption attack, a malicious node can try to consume more battery life demanding too much of route discovery, or by passing unwanted packets to the source node.

Location disclosure attack

In the location disclosure based attack, the malicious node collects the information of routes map and then focus on further attacks. This is one of the unsolved security attacks against MANETs.

Multi layer attacks in IoT

There are different types of multilayer attacks in IOT, they are as follows

- Denial of Service (DoS)
- Jamming
- SYN flooding

Approved by Council of Scientific and Industrial Research, Ministry of Science and Technology, Govt. of India
• Man In Middle attacks
• Impersonation attacks

**Denial of service (DoS) attacks**

In this type of attacks, the attacker injects enormous amount of junk packets into the network which leads to the loss of network resources and causes congestion among the wireless networks.

**Jamming**

Jamming is known as the DoS attack that affect communication between two nodes, the main goal of jamming is to block the valid user’s like sender and receiver from transmitting and receiving packets, jamming is divided into two types

• Physical jamming attacks
• Virtual jamming attacks

**Physical jamming**

Physical jamming is caused by continuous transmission of packets to the receiver or by causing packet collision at the receiver. Physical jamming is also known as radio jamming. radio jamming is simple attack causing more disrupt to the authorized users. Jammers causing this attack block the authorized users from accessing the wireless channel by controlling the wireless medium.

The nodes trying to communicate strangely waiting for the carrier sense timing of the channel to become idle. This put the nodes into list of larger exponential back off period.

**Virtual Jamming**

Virtual jamming is most often possible at the MAC (Medium Access Control) layer, causing affects on Rate to send (RTS) frames, or Clear to send (CTS) frames, or data frames. One of
the advantage of this attack is it consumes less power than comparing to physical or radio jamming.

In virtual jamming the malicious node try send RTS command continuously on the transmission with more number of times. In this process the malicious node blocks the transmission limited amount of power. This attack more dangerous than that of physical attack, by sending false frames it will disturb other node from accessing for certain period of time. To prevent and secure the network from jammer or from hidden attacker who causes the network jamming RTS and CTS method is implemented, this mechanism minimizes the attacker node from handshaking process.

**SYN flooding attack**

Synchronization (SYN) flooding attack, In this attack a malicious node sends enormous amount of synchronization packets to the affected node and by faking the address of synchronization packets. An SYN-ACK message was sent out from affected node after it receives SYN packets from the attacker, without getting any response from malicious node, the half open request remains in the affected node. The victim node stores this connection in fixed size table while it waits for the acknowledgement, with all these pending connection, the affected node not be able to accept any other valid attempts to open a connection. Normally the half open connection automatically expires at certain period of time, but the malicious node continuously sends the packets before the previous connection expires.

**Impersonation attack**

In this impersonation attack, the attacker node guesses the presence of one node in the network, and then spoof that messages to the another node. It is initial step to conduct further attacks to disturb the operation. In accordance the access level of the attacker node, it can even reconfigure that network to easily join into the network to remove the security measures to perform further attacks, like injecting harmful packets into the network or by modifying routing information.
The existing techniques to prevent this impersonate attack is the extension of Ad-hoc On Demand Distance Vector (AODV) routing and it is named as Secure Ad-hoc On Demand Distance Vector (SAODV) routing. SAODV uses Hash chains and Digital signatures to prevent form this attack.

Sybil Attacks

The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. It is named after the subject of the book Sybil, a case study of a woman diagnosed with dissociative identity disorder. The name was suggested in or before 2002 by Brian Zill at Microsoft Research. The term "pseudospoofing" had previously been coined by L. Detweiler on the Cypherpunks mailing list and used in the literature on peer-to-peer systems for the same class of attacks prior to 2002, but this term did not gain as much influence as "Sybil attack".

LITERATURE REVIEW

[1] This work underlines the emerging standard 6LoWPAN allows a vast number of smart objects to be deployed using the huge address space of IPv6 for data and information harvesting through the Internet. In the paper ‘6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach’, Le et al. analyze potential security threats in 6LoWPAN and review the current countermeasures, in particular, the intrusion detection system (IDS) based solutions for countering insider/internal threats.

[2] This paper addresses the Internet of Things. Main enabling factor of this promising paradigm is the integration of several technologies and communications solutions. Identification and tracking technologies, wired and wireless sensor and actuator networks, enhanced communication protocols (shared with the Next Generation Internet), and distributed intelligence for smart objects are just the most relevant. As one can easily
imagine, any serious contribution to the advance of the Internet of Things must necessarily be the result of synergetic activities conducted in different fields of knowledge, such as telecommunications, informatics, electronics and social science.

[3] It goes without saying that we are very content to publish this Clusterbook and to leave it today to your hands. The Cluster of European Research projects on the Internet of Things – CERP-IoT – comprises around 30 major research initiatives, platforms and networks working in the field of identification technologies such as Radio Frequency Identification and in what could become tomorrow an Internet-connected and inter-connected world of objects.

[4] The combination of the Internet and emerging technologies such as nearfield communications, real-time localization, and embedded sensors lets us transform everyday objects into smart objects that can understand and react to their environment. Such objects are building blocks for the Internet of Things and enable novel computing applications. As a step toward design and architectural principles for smart objects, the authors introduce a hierarchy of architectures with increasing levels of real-world awareness and interactivity. In particular, they describe activity-, policy-, and process-aware smart objects and demonstrate how the respective architectural abstractions support increasingly complex application.

[5] At the University of Washington, the RFID ecosystem creates a microcosm for the Internet of Things. The authors developed a suite of Web-based, user-level tools and applications designed to empower users by facilitating their understanding, management, and control of personal RFID data and privacy settings. They deployed these applications in the RFID ecosystem and conducted a four-week user study to measure trends in adoption and utilization of the tools and applications as well as users’ qualitative reactions.

[6] This paper presents a Cloud centric vision for worldwide implementation of Internet of Things. The key enabling technologies and application domains that are likely to drive IoT
research in the near future are discussed. A Cloud implementation using Aneka, which is based on interaction of private and public Clouds is presented. This work conclude our IoT vision by expanding on the need for convergence of WSN, the Internet and distributed computing directed at technological research community.

[7] The contents of the respective legislation encompass the right to information, provisions prohibiting or restricting the use of mechanisms of the Internet of Things, rules on IT-security-legislation, provisions supporting the use of mechanisms of the Internet of Things and the establishment of a task force doing research on the legal challenges of the IoT.

[8] In this article, we present a survey of technologies, applications and research challenges for Internet-of-Things.

[9] This paper address problems associated with the diversifying of the Internet towards an Internet of things, and with increased ways to be reachable, whether the user wants it or not, in the digital world. The paper presents two approaches to cope with the problem: The Identinet and a concept designated by the digital shadow. The paper presents an architecture based on these concepts.

**CONCLUSION**

All Trust Architectures and Intercept detection technology are not effective. These neither provided security to packet formation nor giving any security during transmission. All Trust Architecture developed till now doesn’t provide absolute security and significant features. The IoT sometimes paralyzed and giving a great scope to the intruders/interceptors and other cyber criminals either to damage or alter or misuse the packets during transmission. Most of the fund transfer systems, EDI systems, business applications are using emerging technologies and exposed to vulnerability increases tremendously. Moreover, the cryptographic algorithms used during packet formation and transmission are sometimes
responsible for vulnerabilities. In the close to future the net and wireless technologies can connect completely different sources of data like sensors, mobile phones Associate in Nursing cars in an ever tighter manner. The quantity of devices that hook up with the net is – apparently exponentially – increasing. These billions of elements turn out consume and method info in numerous environments like supplying applications, factories and airports likewise as within the work and everyday lives of individuals. The society want new, scalable, compatible and secure solutions for each the management of the ever a lot of broad, complexly-networked web of Things, and additionally for the support of varied business models. A Secured Trust Architecture for avoidance of SQL Injections and improvements in IoT shall be developed and assessed by developing the effective simulator. A Web Based Simulator can be developed to monitor and manage the web based attacks effectively in the proposed Trust Architecture for Internet of Things.

REFERENCES


There are a huge number of vulnerabilities within poorly secured Internet of Things (IoT) devices which have been exploited in the numerous recent cyber attacks. The usage of IoT devices has been flourishing thanks to the development of wireless technologies, cheaper electronics, advancement in microelectronics and high-speed Internet. Cyber criminals have exploited vulnerabilities in the increasingly connected world to enroll/hijack these devices and operate them under their control. The deadly Mirai botnet attack and the Sony IP device attacks demonstrated the drastic consequences and the huge economic cost that such attacks can have. Both these attacks involved enrolling IoT devices into a botnet and using them to unleash large-scale DDoS (Distributed Denial of Service) attacks.