VOLUME - 12, ISSUE - 02, FEBRUARY - 2023 • PRINT ISSN No. 2277 - 8160 • DOI : 10.36106/gjra

Original Research Paper

Information Technology

INTERNET OF THINGS (IOT) A NEW PERSPECTIVE

Gagandeep Kaur

KEYWORDS :

INTRODUCTION

Now days, the implementation of Internet of Things (IoT) is very prominent and widely used for the automation using Sensor Devices and Advanced Wireless Technologies. All the wireless sensor devices based on Internet Protocol are mapped with their identification modules and these modules are accessed by the servers and satellites for monitoring. Because of the increasing number of devices for smart city and home automation, there are many portals which index the sensor devices and IP based sensors on their databases. These are known as IoT Search Engines. Any person can search the presence of IP based sensors and can misuse it. Shodan, Thingful, Censys, IoTCrawler are few of these prominent IoT search engines. As per the reports, there are thousands of devices including web cams, servers and routers which are found open and vulnerable on these IoT search engines. From the research reports and analytics from many agencies it is found that even the secured government offices are having IoT devices including web cams which are not secured and highly vulnerable. These IoT search engines are frequently updated based on the deployment of new IoT devices. There is need to integrate the higher degree of security and privacy in the IoT based devices and sensors so that any type of sniffing from these IoT can be pushed back.For prediction of the behavior of mobile network, there are number of tools and libraries which can be used to generate virtual nodes, towers, base stations, controllers and servers. Following is the list of prominent tools and frameworks used for the network simulations. These tools and libraries can be used to test the behavior of a new network without having actual smartphones, devices, computers, towers and related actual infrastructure.

- 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

Frameworks, Tools and Libraries for Network Simulation

Software Suite	Taxonomy	Official Web Based Link
DSA	Library	http://www.iot-dsa.org/
Contiki-Cooja	Framework / Toolkit	https://www.contiki-os.org
GLOMOSIM	Framework / Toolkit	http://pcl.cs.ucla.edu/projects/glomosim
GNS-3	Library	http://www.gns-3.net
CISCO Packet Tracer	Library	https://www.netacad.com/courses/packet-tracer
CNET	Library	http://www.csse.uwa.edu.au/cnet/
CORE	Framework / Toolkit	https://www.nrl.navy.mil/itd/ncs/products/core
Cloonix	Framework / Toolkit	http://clownix.net/
IMUNES	Library	https://github.com/imunes/
IoTivity	Library	https://www.iotivity.org/
JIST / SWANS	Framework / Toolkit	http://jist.ece.cornell.edu/
JSIM	Framework / Toolkit	https://www.physiome.org/jsim/
MIMIC	Library	http://www.gambitcomm.com
MOBIREAL	Framework / Toolkit	http://www.mobireal.net
MiniNet	Framework / Toolkit	http://mininet.org/
NCTUNS	Library	http://nsl10.csie.nctu.edu.tw
Node-RED	Framework / Toolkit	http://nodered.org/
Ns-3	Framework / Toolkit	https://www.nsnam.org/
Ns-3 mmWave	Library	https://apps.nsnam.org/app/mmwave/
OMNET++	Framework / Toolkit	http://www.omnetpp.org
OPNET	Library	http://www.opnet.com/
OpenIoT	Framework / Toolkit	http://www.openiot.eu/
NETSIM	Library	http://www.tetcos.com/software.html
NS2	Library	http://www.isi.edu/nsnam/ns
NetKit	Library	http://wiki.netkit.org/
PARSEC	Framework / Toolkit	http://pcl.cs.ucla.edu/projects/parsec/
PHYSIM	Framework / Toolkit	http://tetcos.com/physim.html
PSIM	Library	https://powersimtech.com/products/psim/
PeerSim	Library	http://peersim.sourceforge.net/
QUALNET	Library	http://www.scalable-networks.com/
SNMP	Framework / Toolkit	http://snmpsim.sourceforge.net/download.html
Shadow	Library	https://shadow.github.io/
TRAFFIC	Framework / Toolkit	http://members.iinet.net.au/~clark/
VNX / VNUML	Library	http://www.dit.upm.es/~vnx/
WEBNMS	Library	http://www.webnms.com

Zetta	Framework / Toolkit	http://www.zettajs.org/

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 iew, 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.

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 Feuer Where 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.

Spark
Spark is a distributed, cloud-based IoT operating system. Spark includes a Web-based IDE, a command-line interface, support for multiple languages, and libraries for working with many different IoT devices. It has a very active user community, and a lot of documentation and online help are available.

Freeboard
Freeboard aims to let users create their own dashboards for monitoring IoT deployments. The code is freely available on GitHub or you can try the service for free if you make your dashboard public. Low-priced plans are also available for those who want to keep their data private. Sample dashboards oon the site show how they can be used to track air quality, residential appliances, distillery performance or environmental conditions in a humidor.

Exciting Printer
Exciting offers an open source kit for experimenting with IoT printing. It makes it possible to build your own small printer and use that printer to print out information obtained from various IoT devices. For example, it could print out a list of daily reminders, the weather report, etc. And in a interesting twist, if you want to contact the project owners, you can draw a picture that will be printed on the IoT printer in their office.

Device Hive
This project offers a machine-to-machine (M2M) communication framework for connecting devices to the Internet of Things. It includes easy-to-use Web-based management software for creating networks, applying security rules and monitoring devices. The website offers sample projects built with DeviceHub, and it also has a "playground" section that allows users to use DeviceHub online to see how it works.

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 meet up 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.

Open Remote

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.

Site Where

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.

Thing Speak

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 Kimona 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.

Problem Formulation

As there are assorted pessimistic aspects in the security and integrity with IoT based advanced networks, there is need to devise and implement the approach for higher degree of accuracy and security in the IoT based scenarios.

With the increasing devices and smart objects, there is need to work on the security and integrity aspects which are mandatory for any distributed as well as shared environment. This research work is having key focus on the elevation of security and overall performance with minimum latency in the wireless network associated with IoT. Here latency signifies the time taken for round trip of the data packet.

This time can be reduced with the parallel algorithmic approaches and soft computing. The smart devices and objects in the IoT environment are increasing exponentially for assorted applications and with this increase the security and integrity with the inherent performance is also a significant issue. Now days, IoT is in use for military and corporate applications, that's the key point by which it is paramount important to devise and enforce the higher degree of security and integrity in the IoT based wireless communication.

RESEARCH OBJECTIVES

The objectives associated with the research work are:

1. To evaluate the Security Issues and Assaults in Internet of Things (IoT)
2. To analyze the cavernous literature with the Hash Functions and Dynamic Key Generation on Security and Performance of IoT
3. To devise a novel and effective multilayered approach for security in IoT
4. To perform the implementation of advanced secured approach for security in IoT

CONCLUSION AND FUTURE SCOPE

Internet of Things is having huge prominence in the research and development. For research and development, the performance of wireless applications can be evaluated on multiple cross platform frameworks. The same application can be developed using Lua, Cordova, Corona and similar frameworks. After development and deployment for specific devices and platforms, the performance of these development environments can be evaluated so that the best development framework can be identified for the development of advanced apps.

Following are some of the approaches on which the novel and effectual algorithms can be devised and implemented using Cooja

- Lifetime Analytics for Robustness of IoT Environment
- Prediction and Avoidance of Energy Consumption Attacks
- Development of Energy Aware IoT Scenarios
- Interoperability and Cross-Protocol Compatibility
- Power Aware Scheduling and Routing
- Reproducible and Multi-Interface Implementationsand many others

REFERENCES

[1] A. Zanella A, N. Bui, A. Castellani, L. Vangelista and L, Zorzi. "Internet of things for smart cities" IEEE Internet of Things Journal. pp. 22-32., 2014

[2] R. van Kranenburg, E. Anzelmo, A. Bassi, D. Caprio, S. Dodson, and M. Ratto, "The Internet of Things" in Proc. 1st Berlin Symp. Internet Soc., Berlin,

Germany, pp. 25–27. 2011

[3] Y. Li, M. Hou, H. Liu, and Y. Liu, "Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of Internet of Things," Inf. Technol. Manage., vol. 13, no. 4, pp. 205–216, 2012.

[4] L. Tan and N. Wang, "Future internet: The internet of things," in Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE), Chengdu, China, Aug. 20–22, pp. V5-376–V5-380., 2010

[5] X. Jia, O. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in internet of things (IoT)," in Proc. 2nd IEEE Int. Conf. Consum. Electron., Commun. Netw. (CECNet), Yichang, China, pp. 1282–1285., Apr. 21–23, 2012,

[6] M. A. Feki, F. Kawsar, M. Boussard and L. Trappeniers, L. "The internet of things: the next technological revolution. Computer, 46(2), pp. 24-25, 2013

[7] E. W. T. Ngai, K. K. Moon, F. J. Riggins, and C. Y. Yi, "RFID research: An academic literature review (1995–2005) and future research directions," Int. J. Prod. Econ., vol. 112, no. 2, pp. 510–520, 2008.

[8] D. Uckelmann, M. Harrison, and F. Michahelles, "An architectural approach towards the future internet of things," in Architecting the Internet of Things. New York, NY, USA: Springer, pp 1–24, 2011

[9] L. Wang, L. Xu, Z. Bi, and Y. Xu, "Data filtering for RFID and WSN integration," IEEE Trans. Ind. Informat., vol. 10, no. 1, pp. 408–418, 2014.

[10] ITU NGN-GSI Rapporteur Group, "Requirements for Support of USN Applications and Services in NGN Environment", Geneva, Switzerland: International Telecommunication Union (ITU), 2010.

[11] N. R. P. Prasad, and R. Prasad, "Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things," J. Cyber Secur. Mobil., vol. 1, no. 4, pp. 309–348, 2013.

[12] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, "Towards viable certificate-based authentication for the internet of things," Proc. 2nd ACM Work.Hot Top.Wirel.Netw.Secur.Priv. - HotWiSec '13, pp. 37, 2013.

[13] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wireless Networks, vol. 20, no. 8, pp. 2481–2501, 2014.

[14] L. Chen, Z. Yan, W. Zhang, and R. Kantola, "TruSMS: A trustworthy SMS spam control system based on trust management," Future Generation Computer Systems, vol. 49, no. October, pp. 77–93, 2015.

[15] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.

[16] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: A survey of existing protocols and open research issues," IEEE Commun. Surv.Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015.

[17] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," Ad Hoc Networks, vol. 32, no.February, pp. 17–31, 2015.

[18] M. Vucinic, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "OSCAR: Object Security Architecture for the Internet of Things," Science Direct Ad Hoc Networks, pp. 3-16,2014.

[19] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the internet of things," IEEE Security and Privacy, vol. 13, no. 1, pp. 14–21, 2015.

[20] F. Li, Z. Zheng, and C. Jin, "Secure and efficient data transmission in the Internet of Things," Telecommunication Systems, vol. 62, no. 1, pp. 111–122, 2016.

[21] S. R. Moosavi, T. N. Gia, E. Nigussie, A. M. Rahmani, S. Virtanen, H. Tenhunen, and J. Isoaho, "End-to-end security scheme for mobility enabled healthcare Internet of Things," Futur. Gener.Comput.Syst., vol. 64, no.May, pp. 108–124, 2016.

[22] K. A. RafidhaRehiman and S. Veni, "A secure authentication infrastructure for IoT enabled smart mobile devices - an initial prototype," Indian J. Sci. Technol., vol. 9, no. 9, pp. 1-6 2016.

[23] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," Journal of Network and Computer Applications., vol. 66, pp. 198–213, 2016.

[24] E. Bertino, "Data Security and Privacy in the IoT," Proc. 19th Int. Conf. Extending Database Technol., Open Proceedings, pp. 1–3, 2016.

[25] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, "SIT : A Lightweight Encryption Algorithm for Secure Internet of Things," International Journal of Advanced Computer Science and Applications, vol. 8, no. 1, pp. 1–10, 2017.

[26] M. B. Mollah, A. K. Azad, and A. Vasilakos, "Secure data sharing and searching at the edge of cloud-assisted internet of things," IEEE Cloud Computing, vol. 4, no. 1, pp. 34–42, 2017.

[27] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation," Future Generation Computer Systems, pp. 1–10, 2017.