A short survey of Security and Privacy Issues of Internet of Things

[1]Parshapu.Padma, [2]P.Srilakshmi, [3]M.Anusha

[1,2]Associate Professor, [3]Assistant Professor
Department of Information Technology,
Guru Nanak Institutions Technical Campus, Hyderabad, India

Abstract: **The Internet of Things ("IoT") refers to the ability of everyday objects to connect to the Internet and to send and receive data. It includes, for example, Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and wrist watches that share with your friends how far you have biked or run during the day. Which offers capabilities to identify and connect worldwide physical objects into a unified system? As a part of IoTs, serious concerns are raised over access of personal information pertaining to device and individual privacy. Security and privacy are the key issues for IoT applications, this survey summarizes the security threats and privacy concerns of IoT.**

Index Terms **- Internet of Things (IoT), Threats, Security, Privacy**

I. INTRODUCTION

With the rapid development of Internet technology and communications technology, our lives are gradually led into an imaginary space of virtual world. People can chat, work, shopping, keeps pets and plants in the virtual world provided by the network. However, human beings live in a real world; human activities cannot be fully implemented through the services in the imaginary space. It is the limitation of imaginary space that restricts the development of Internet to provide better services. To remove these constraints, a new technology is required to integrate imaginary space and real-world on a same platform which is called as Internet of Things (IoTs). Based on a large number of low-cost sensors and wireless communication, the sensor network technology puts forward new demands to the Internet technology. It will bring huge changes to the future society, change our way of life and business models. Apart from benefits of IoTs, there are several security and privacy concerns at different layers viz; Front end, Back end and Network. In this paper, the survey is in security and privacy concerns related to Internet of Things (IoTs) by defining some open challenges. Nowadays, the concept of IoT is many-folded, it embraces many different technologies, services, and standards and it is widely perceived as the angular stone of the ICT market in the next ten years, at least.

From a logical viewpoint, an IoT system can be depicted as a collection of smart devices that interact on a collaborative basis to fulfill a common goal. At the technological floor, IoT deployments may adopt different processing and communication architectures, technologies, and design methodologies, based on their target. For instance, the same IoT system could leverage the capabilities of a wireless sensor network (WSN) that collects the environmental information in a given area and a set of smart phones on top of which monitoring applications run. In the middle, a standardized or proprietary middle-ware could be employed to ease the access to virtualized resources and services. The middleware, in turn, might be implemented using cloud technologies, centralized over- lays, or peer to peer systems.

II IOT OVERVIEW AND BACKGROUND

As shown in Fig. 1, the IoTs allow people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service. They are "Material objects connected to material objects in the Internet".

For example, through RFID, laser scanners, global writing system, infrared sensors and other information sensing devices are connected to any object for communication services and data exchange. At last, to reach the smart devices to be tracked, located, and monitored and to handle the network functions, to make the IT infrastructure and physical infrastructure consolidation IoT is the most needed one.

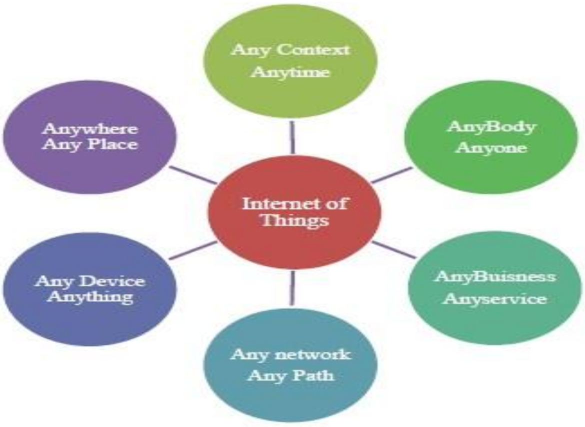


Fig. 1 Definition of Internet of Things .

Evolution:

Before the investigation of the IoTs in depth, it is worthwhile to look at the evolution of the Internet. As shown in Fig. 2, in the late 1960s, communication between two computers was made possible through a computer network. In the early 1980s, the TCP/IP stack was introduced. Then, commercial use of the Internet started in the late 1980s. Later, the World Wide Web (WWW) became available in 1991 which made the Internet more popular and stimulate the rapid growth. Then, mobile devices connected to the Internet and formed the mobile-Internet. With the emergence of social networking, users started to become connected together over the Internet. The next step in the IoTs is where objects around us will be able to connect to each other (e.g. machine to machine) and communicate via the Internet. what we want, and what we need and act accordingly without explicit instructions

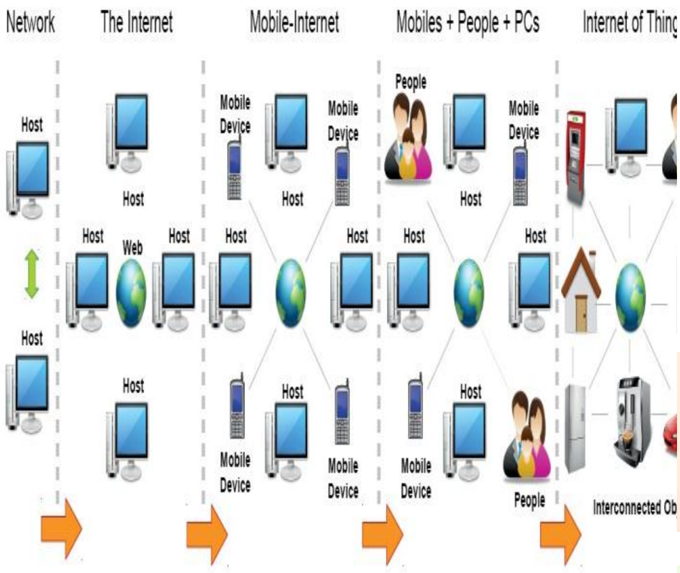


Fig. 2 Evolution of the Internet of Things

Architecture and Protocal Stack of IoTs:

IoTs can be divided into three important layers.

Perception

Network and

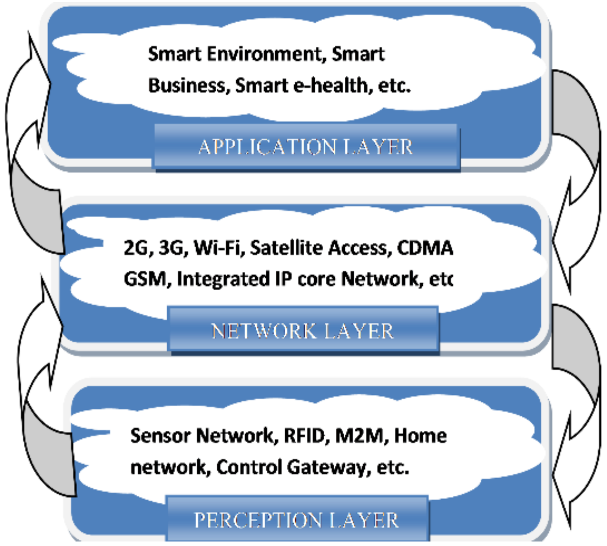
Application.

As shown in Fig.3, perception layer (also called as recognition layer) gathers data/information and identifies the physical world.

Network layer is the middle one (also called as wireless sensor networks), which accountable for the initial processing of data, broadcasting of data, assortment and polymerization.

The topmost application layer offers these overhauls for all industries. Among these layers, the middle one network layer is also a "Central Nervous System" that takes care of global services in the IoTs, since it acts the part of aggregating with upward application layer and makes the link downward of perceptual layer.

Various basic networks including, mobile/ private network, wireless and wired network offers and affirms the underlying connection. IoTs are set up in this new network which is composed Business applications of networks .


Smart Environment, Smart Business, Smart e-health, etc.

APPLICATION LAYER

2G, 3G, Wi-Fi, Satellite Access, CDMA GSM, Integrated IP core Network, etc

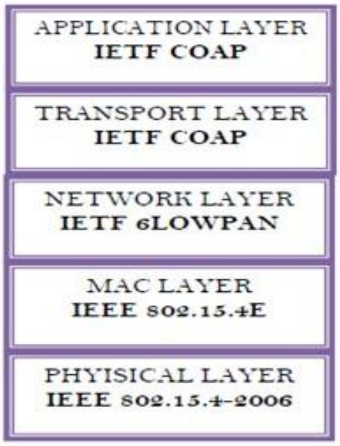
NETWORK LAYER

Sensor Network, RFID, M2M, Home network, Control Gateway, etc.

PERCEPTION LAYER

Fig. 3.a. Architecture of Internet of things .

Regarding the IOT Protocol Stack, as shown in the Fig 3.b, from a PHY perspective, the current IEEE 802.15.4-2006 PHY layer(s) sufficient in terms of energy efficiency. Given that a large amount of IoT applications however will require only a few bits to be send. It may be advisable to commence looking into a standardized PHY layer which allows ultra low rate Transmissions over very narrow frequency bands, with the obvious advantage of enormous link budgets and thus significantly enhanced ranges. IEEE802.15.4e standard is very suitable for a protocol stack for IoT because it is latest generation of highly reliable and low-power **MAC** protocol.


APPLICATION LAYER
IETF COAP

TRANSPORT LAYER
IETF COAP

NETWORK LAYER
IETF 6LOWPAN

MAC LAYER
IEEE 802.15.4E

PHYISICAL LAYER
IEEE 802.15.4-2006

Fig 3 b. IOT Protocol Stack .

From a networking perspective, the introduction of the IETF 6LoWPAN protocol family has been instrumental in connecting the low power radios to the Internet and the work of IETF ROLL allowed suitable routing protocols to achieve universal connectivity. From the transport layer and an application perspective, the introduction of the IETF CoAP protocol family has been instrumental in ensuring that application layers and applications themselves do not need to be re-engineered to run over low-power embedded networks .

Applications of IOTs:

A survey done by the IoT-I project in 2010 identified IoTs application scenarios which are grouped in 14 domains viz; Transportation, Smart Home, Smart City, Lifestyle, Retail, Agriculture, Smart Factory, Supply chain, Emergency, Health care, User interaction, Culture and tourism, Environment and Energy. This survey was based on 270 responses from 31 countries and the scenarios attracting the most interest were: smart home, smart city, transportation and health care .In this paper, the focus will be briefly on the IoTs applications in medical (health care), smart home, intelligent community security system (smart city).

We measured three things: What people search for on Google, what people talk about on Twitter, and what people write about on LinkedIn. The highest score received a rating of 100%, the other Internet of Things applications were ranked with a percentage that represents the relation to the highest score (relative ranking).

1. IoT in Smart Home

Now a days, smart homes are becoming more and more cost-effective and intellectualized with continued progress and cost reduction in communication technology, information technology, and electronics, which connects the Internet with everyday devices and sensors for connecting virtual and physical objects through the data capture and communication capabilities development.

Reading of remote meters can be attained through these smart home systems. That implies, the data related with home power, telecommunications, gas and water can be sent automatically to their corresponding utility company to enhance the efficiency of the work. In addition, by virtue of smart home systems, windows, home ventilation, doors, lighting, air conditioning etc., can be controlled by remotely. Each electronics devices such as refrigerator, washing machine, oven etc., can be manipulated by remote platforms or programs. Entertainment equipments like radios and televisions can be connected to common channels which are in remote. In addition, home security and healthcare are also important aspects of smart homes. For instance, health aid devices can help an elder individual to send request or alarm to a family member or a professional medical center. In the smart home design, the house and its different electrical appliances have been equipped with actuators, sensors as shown in Fig. 4. The home devices functions in a local network but on certain occasions connected to a remote management platform in order to do processing and data collection.

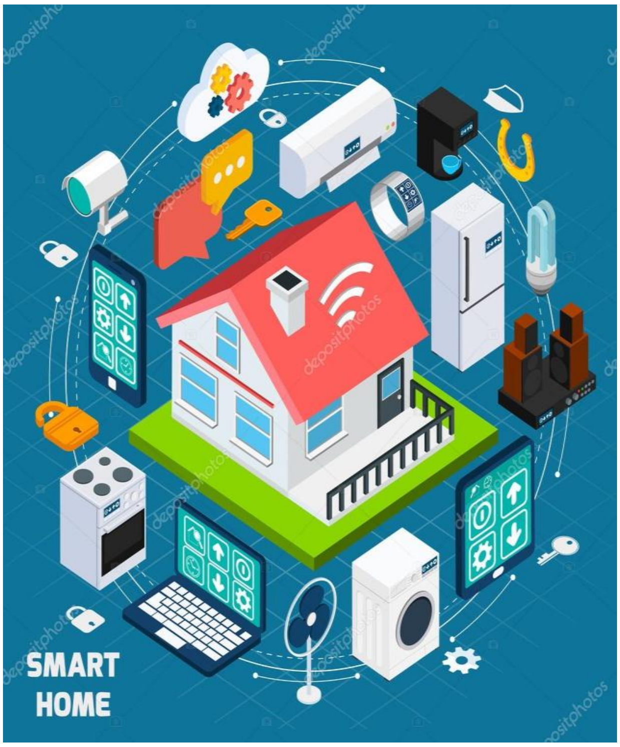


Fig 4: smart home

2. Wearables

Wearable remains a hot topic too. As consumers await the release of Apple’s new smart watch in April 2015, there are plenty of other wearable innovations to be excited about: like the Sony Smart B Trainer, the Myo gesture control, or Looksee bracelet. Of all the IoT startups, wearables maker Jawbone is probably the one with the biggest funding to date. It stands at more than half a billion dollars!

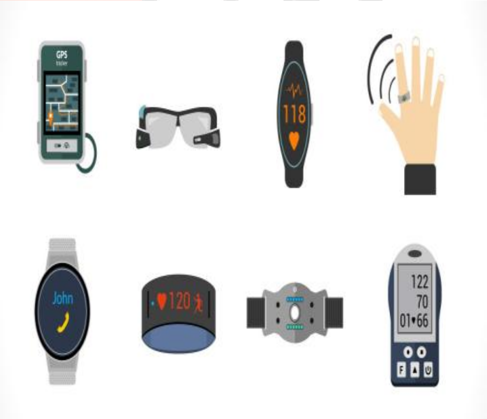
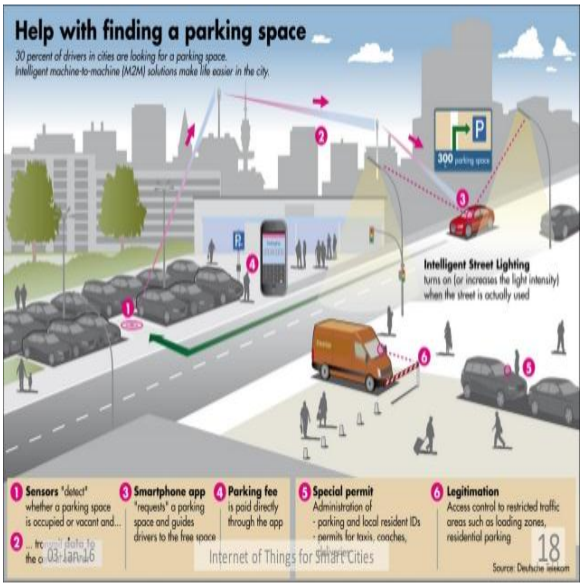


Fig5. w**earables**

3. Smart City

Smart city spans a wide variety of use cases, from traffic management to water distribution, to waste management, urban security and environmental monitoring. Its popularity is fueled by the fact that many Smart City solutions promise to alleviate real pains of people living in cities these days. IoT solutions in the area of Smart City solve traffic congestion problems, reduce noise and pollution and help make cities safer.


Help with finding a parking space
30 percent of drivers in cities are looking for a parking space.
Intelligent machine-to-machine (M2M) solutions make life easier in the city.
300 parking space
Intelligent Street Lighting
turns on (or increases the light intensity) when the street is actually used
1 Sensors "detect" whether a parking space is occupied or vacant and...
2 ... transmit data to the c...
3 Smartphone app "requests" a parking space and guides drivers to the free space
4 Parking fee is paid directly through the app
5 Special permit Administration of - parking and local resident IDs - permits for taxis, coaches, deliveries
6 Legitimation Access control to restricted traffic areas such as loading zones, residential parking
03-Jan-16
Internet of Things for Smart Cities
18
Source: Deutsche Telekom

4. Smart grids

Smart grids are a special one. A future smart grid promises to use information about the behaviors of electricity suppliers and consumers in an automated fashion to improve the efficiency, reliability, and economics of electricity. 41,000 monthly Google searches highlight the concept's popularity. However, the lack of tweets (Just 100 per month) shows that people don't have much to say about it.

5. Industrial Internet

The industrial internet is also one of the special Internet of Things applications. While many market researches such as Gartner or Cisco see the industrial internet as the IoT concept with the highest overall potential, its popularity currently doesn't reach the masses like smart home or wearables do. The industrial internet however has a lot going for it. The industrial internet gets the biggest push of people on Twitter (~1,700 tweets per month) compared to other non-consumer-oriented IoT concepts.

6. Connected Car

The connected car is coming up slowly. Owing to the fact that the development cycles in the automotive industry typically take 2-4 years, we haven't seen much buzz around the connected car yet. But it seems we are getting there. Most large auto makers as well as some brave startups are working on connected car solutions. And if the BMWs and Fords of this world don't present the next generation internet connected car soon, other well-known giants will: Google, Microsoft, and Apple have all announced connected car platforms.

7. Connected Health (Digital health/Telehealth/Telemedicine)

Connected health remains the sleeping giant of the Internet of Things applications. The concept of a connected health care system and smart medical devices bears enormous potential, not just for companies also for the well-being of people in general. Yet, Connected Health has not reached the masses yet. Prominent use cases and large-scale startup successes are still to be seen.

8. Smart retail

Proximity-based advertising as a subset of smart retail is starting to take off. But the popularity ranking shows that it is still a niche segment. One LinkedIn post per month is nothing compared to 430 for smart home.

9. Smart supply chain

Supply chains have been getting smarter for some years already. Solutions for tracking goods while they are on the road, or getting suppliers to exchange inventory information have been on the market for years. So while it is perfectly logic that the topic will get a new push with the Internet of Things, it seems that so far its popularity remains limited.

10. Smart farming

Smart farming is an often overlooked business-case for the internet of Things because it does not really fit into the well-known categories such as health, mobility, or industrial. However, due to the remoteness of farming operations and the large number of livestock that could be monitored the Internet of Things could revolutionize the way farmers work. But this idea has not yet reached large-scale attention. Nevertheless, one of the Internet of Things applications that should not be underestimated. Smart farming will become the important application field in the predominantly agricultural-product exporting countries.

III SECURITY AND PRIVACY CONCERNS IN IOTS

Security Concerns in IoTs:

Internet of Things virtually is a network of real world systems with real-time interactions. The development of the initial stage of IoT, is M2M (Machine to Machine), having unique characteristics, deployment contexts and subscription. Unattended operation without human intervention is possible for long periods of time by the wireless area network (WAN)

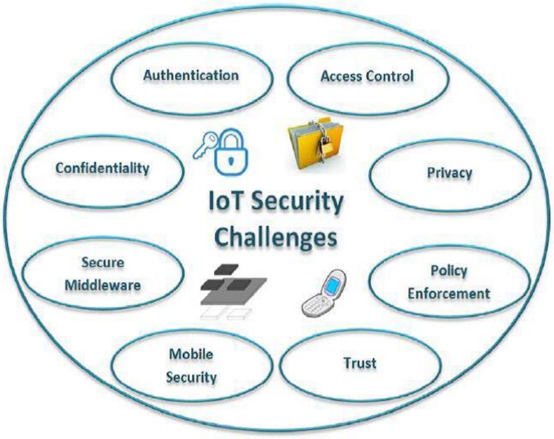


Fig.5.1. Main security issues in IoT.

IoT security requirements: authentication, confidentiality and access control

Authentication

Confidentiality

Access control

with a special focus on IoT systems. IoT, in fact, enables a constant transfer and sharing of data among things and users in order to achieve particular goals. In such a sharing environment, authentication, authorization, access control and non-repudiation are important to ensure secure communication.

Authentication

As regards authentication, the approach presented in makes use of a custom encapsulation mechanism, combines cross-platform communications with encryption, signature, and authentication, in order to improve IoT applications development capabilities by establishing a secure communication system among different things.

It is introduced the first fully implemented two- way authentication security scheme for IoT, based on existing Internet standards, specifically the Datagram Transport Layer Security (DTLS) protocol, which is placed between transport and application layer. The extensive evaluation, based on real IoT systems, shows that such an architecture provides message integrity, confidentiality, and authenticity with enough affordable energy, end-to-end latency, and memory overhead.

As regards confidentiality and integrity, in it is analyzed how existing key management systems could System (KMS) protocols in four major categories: key pool framework, mathematical framework, negotiation framework, and public key framework. In authors argue that most of the KMS protocols are not suitable for IoT. In fact, key pool ones suffer insufficient connectivity; mathematical ones make use of the deployment knowledge to optimize the construction of their data structures, but such an approach cannot be used in IoT since client and server nodes are usually located in different physical locations; combinatory-based KMS protocols suffer both connectivity and scalability/authentication; negotiation ones make use of the wireless channel and its inherent features to negotiate a common key, be applied to the IoT context. It is possible to classify the Key Management however they cannot be suitable for IoT because client and server nodes usually belong to different networks and they should route the information through the Internet in order to be able to talk with each other. Hence, the KMS protocols which might be suitable for some IoT scenarios are the Bloom and the polynomial schema, whose computational overhead is quite low in comparison to Public Key Cryptography (PKC) operations (i.e., public key framework). However for such schemes, several counter- measures are required in order to manage device authentication and face man-in-the-middle attacks. The encrypted data are decrypted at each routing node, until the Local Information Server of Things (L-TIS) receives the plain text. Meanwhile, the nodes can check the integrity of received data and the creditability of routing path in the transmitting procedure. Such a transmission model results very weak in terms of attack-resistance due to the adoption of hop-by-hop encryption/decryption behavior.

It appears that a unique and well-defined solution able to guarantee confidentiality in a IoT context is still missing, as also asserted in. It is worth to note that many efforts have been conducted in the WSN field, but several questions arise:

Network layer handles authentication like

It is feasible to reuse the traditional security mechanisms (e.g., encryption algorithms)

Handle the different keys.

key distribution mechanism is the most suitable.

It ensures an end-to-end integrity verification mechanism in order to make the system more resilient to malicious attacks

For example, an authentication protocol for IoT is pre-sented in, using lightweight encryption method based on XOR manipulation for anti-counterfeiting and privacy protection, in order to cope with constrained IoT devices.

Starting from WSN context, an user authentication and key agreement scheme for heterogeneous wireless sensor networks is also proposed in. It enables a remote user to securely negotiate a session key with a sensor node, using a lean key agreement protocol. In this way, it ensures mutual authentication among users, sensor nodes, and gateway nodes (GWN), although GWN is never contacted by the user. In order to apply such a scheme to resource- constrained architectures, it only uses simple hash and XOR computations, as in.

The authentication and access control method presented in aims at establishing the session key on the basis of Elliptic Curve Cryptography (ECC), another lightweight encryption mechanism. This scheme defines attribute-based access control policies, managed by an attribute authority, enhancing mutual authentication among the user and the sensor nodes, as well as solving the resource-constrained issue at application level in IoT.

These preliminary answers partially address afore- listed questions because they specifically target the problem of lightweight cyphering in pervasive environments. Further efforts are required to complement these lean mechanisms with standardized protocols for authentication and a clear definition of one or more authorities aimed at guaranteeing the expected confidentiality within the IoT infrastructure.

Confidentiality:

When we talk about confidentiality of information, we are talking about protecting the information from disclosure to unauthorized parties. Information has value, especially in today’s world. Bank account statements, personal information, credit card numbers, government documents. Every one has information they wish to keep a secret. Protecting such information is a very major part of information security. A very key component of protecting information confidentiality would be encryption. Encryption ensures that only the right people (people who knows the key) can read the information. Encryption is very widespread in today’s environment and can be found in almost every major protocol in use. A very prominent example will be SSL/TLS, a security protocol for communications over the internet that has been used in conjunction with a large number of internet protocols to ensure security.

Integrity:

Integrity of information refers to protecting information from being modified by unauthorized parties. Information only has value if it is correct. Information that has been tampered with could prove costly. For example, if you were sending an online money transfer for $100, but the information was tampered in such a way that you actually sent $10,000, it could prove to be very costly for you.As with data confidentiality, cryptography plays a very major role in ensuring data integrity. Commonly used methods to protect data integrity includes hashing the data you receive and comparing it with the hash of the original message. However, this means that the hash of the original data must be provided to you in a secure fashion. More convenient methods would be to use existing schemes such as GPG to digitally sign the data.

Availability:

Availability of information refers to ensuring that authorized parties are able to access the information when needed. Information only has value if the right people can access it at the right times. Denying access to information has become a very common attack nowadays. Almost every week you can find news about high profile websites being taken down by DDoS attacks. The primary aim of DDoS attacks is to deny users of the website access to the resources of the website. Such downtime can be very costly. Other factors that could lead to lack of availability to important information may include accidents such as power outages or natural disasters such as floods.

How does one ensure data availability? Backup is key. Regularly doing off-site backups can limit the damage caused by damage to hard drives or natural disasters. For information services that is highly critical, redundancy might be appropriate. Having a off-site location ready to restore services in case anything happens to your primary data centers will heavily reduce the downtime in case of anything happens.

Access control:

Access control refers to the permissions in the usage of resources, assigned to different actors to IoT network. Users and things, as data holders, must be able to feed data collectors only with the data regarding a specific target. At the same time, data collectors must be able to identify or authenticate users and things as legitimate data holders, from which the information are collected.

It presents an identity based system for personal location in emergency situations. It consists of: registration, users authentication, policy, and client subsystems. The system confirms the identity of the user through the user authentication subsystem and gets the level of the emergency through the policy subsystem. Then it can make sure that user’s location information can be accessed only by some authorized user and only when it is needed.

In a security architecture is developed, which aims at ensuring data integrity and confidentiality, starting from a prototype query processing engine for data streams, called Nile. Such a mechanism is based on FT-RC4, an extension of the RC4 algorithm, which represents a stream cipher encryption scheme, to overcome possible decryption fails due to de-synchronization problems.

Privacy in IoT:

IoT finds application in many different fields, for example: patients remote monitoring, energy consumption control, traffic control, smart parking system, inventory management, production chain, customization of the shop-

related to their movements, habits and interactions with other people. In a single term, their privacy should be guar- anteed. In literature, there are some attempts to address such an issue.

Secure middlewares in IoT:

Due to the very large number of heterogeneous technologies normally in place within the IoT paradigm, several types of middleware layer are employed to enforce the integration and the security of devices and data within the same information network. Within such middlewares, data must be exchanged respecting strict protection constraints. Moreover, in middleware design and development, the different communication mediums for wide scale IoT deployments need to be considered; in fact, while many smart devices can natively support IPv6 communications, existing deployments might not support the IP protocol within the local area scope, thus requiring ad hoc gateways and middlewares.

This solution provides two core features: (i) it is designed to be simple, modular and extensible and (ii) it runs in different computational platforms, including Java SE and Android. The underlying interface is based on HTTP and uses a REpresentational State Transfer (REST) interface. Different implementations can provide only certain features (e.g., data access) and still interact with each others. In this way it is possible to embed it in other devices. This gateway platform only supports Python and requires a partial ad hoc implementation. It uses a TSC (Triple Space Computing), that is a coordination paradigm which promotes the indirect communication style and uses semantic data. The way it works is simple: each application writes semantically annotated information in a shared space, and other applications or nodes can query for it. As regards security, given the data-centric nature of the framework, there are mainly two core requirements: (i) a data provider may only grant access to certain data to a certain set of users and (ii) a data consumer may trust only a set of pro- viders for certain set of acquired data.

A derived issue is how to authenticate each other in such a dynamic scenario. In order to support the first requirement, an OpenID-based

Mobile security in IoT:

Mobile nodes in IoT often move from one cluster to another, in which cryptography based protocols are required to provide rapid identification, authentication, and privacy protection. An adhoc protocol is presented in exploited when a mobile node joins a new cluster. Such a protocol contains a valid request message and an answer authentication message, which rapidly implements identification, authentication, and privacy protection. It could be robust towards replay attack, eavesdropping, and tracking or location privacy attacks. Compared with other similar protocols such as basic hash protocol, it has less communication overhead, more security and more privacy protection properties.

IoT infrastructure, a security and privacy mechanism is proposed. From trustworthiness point of view, service providers have to get authentication from a public authority, which is also responsible for handover cryptography credentials to each actor, in order to allow a secure communication among the end-devices and the application brokers; the goal is to establish a trusted IoT application market, where information on end-devices can be exchanged to establish a secure connection among market and users.

In, a security architecture deployable on mobile platforms is defined for mobile e-health applications.

Conclusion:

The IoT technology draws huge changes in everyone's everyday life. In the IoTs era, the short-range mobile transceivers will be implanted in variety of daily requirements. The connections between people and communications of people will grow and between objects to objects at anytime, in any location. The efficiency of information management and communications will arise to a new high level. The dynamic environment of IoTs introduces unseen opportunities for communication, which are going to change the perception of computing and networking. The privacy and security implications of such an evolution should be carefully considered to the promising technology. The protection of data and privacy of users has been identified as one of the key challenges in the IoT.

References

[1] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.

[2] D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, Survey internet of things: vision, applications and research challenges, Ad Hoc Netw. 10 (7) (2012) 1497–1516.

[3] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, M. Dohler, Standardized protocol stack for the internet of (important) things, IEEE Commun. Surv. Tutorials 15 (3) (2013) 1389–1406.

[4] B. Emmerson, M2M: the internet of 50 billion devices, Huawei Win–Win Mag. J. (4) (2010) 19–22.

[5] D. Boswarthick, O. Elloumi, O. Hersent, M2M Communications: A Systems Approach, first ed., Wiley Publishing, 2012.

[6] O. Hersent, D. Boswarthick, O. Elloumi, The Internet of Things: Key Applications and Protocols, second ed., Wiley Publishing, 2012.

[7] L.A. Grieco, M.B. Alaya, T. Monteil, K.K. Drira, Architecting information centric ETSI-M2M systems, in: IEEE PerCom, 2014.

[8] R.H. Weber, Internet of things - new security and privacy challenges, Comput. Law Secur. Rev. 26 (1) (2010) 23–30.

[9] H. Feng, W. Fu, Study of recent development about privacy and security of the internet of things, in: 2010 International Conference on Web Information Systems and Mining (WISM), Sanya, 2010, pp. 91–95.

[10] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Networks 57 (10) (2013) 2266–2279.

[11] J. Anderson, L. Rainie, The Internet of Things will Thrive by 2025, PewResearch Internet Project, May 2014. <http://www.pewinternet.org/2014/05/14/internet-of-things/>.

[12] S. Bandyopadhyay, M. Sengupta, S. Maiti, S. Dutta, A survey of middleware for internet of things, in: Third International Conferences, WiMo 2011 and CoNeCo 2011, Ankara, Turkey, 2011, pp. 288–296.

[13] M.A. Chaqfeh, N. Mohamed, Challenges in middleware solutions for the internet of things, in: 2012 International Conference on Collaboration Technologies and Systems (CTS), Denver, CO, 2012, pp. 21–26.

[14] S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, Proposed embedded security framework for internet of things (iot), in: 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2011, Chennai, India, 2011, pp. 1 – 5.

[15] M.C. Domingo, An overview of the internet of underwater things, J. Network Comput. Appl. 35 (6) (2012) 1879–1890.

[16] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.

[17] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for internet of things, J. Network Comput. Appl. 42 (0) (2014) 120–134.

[18] Y. Zhao, Research on data security technology in internet of things, in: 2013 2nd International Conference on Mechatronics and Control Engineering, ICMCE 2013, Dalian, China, 2013, pp. 1752–1755.

[19] https://cfs22.simplicdn.net/ice9/free_resources_article_thumb/Applications_of_big_data_infog raphic.png

[20] https://mapr.com/hadoop-security-and-big-data-governance-mapr/