Middle-East Journal of Scientific Research 24 (9): 2739-2751, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.09.23920

A Systematic Exposition of Internet of Things (IoT) and Security Issues

[1]S. Sreega, [2]S. Kannimuthu, [3]D. Bhanu and [2]Ms. K.S. Bhuvaneshwari

[1]Department of EEE, Karpagam College of Engineering, Coimbatore, India
[2]Department of CSE, Karpagam College of Engineering, Coimbatore, India
[3]Department of IT, Karpagam Institute of Technology, Coimbatore, India

Abstract: Internet of things abbreviated as IoT is a fuzzword which is pre-eminent in today's research field. It's a virtual world connecting electronic devices and internet. IoT was introduced for easy end-to-end communication. Even though it lays its helping-hand in the field of communication still it faces crisis in the field of security and researchers instead of tiptoeing round the problem are still confronting it. This paper will display an overview, attacks and contributions in IoT. It will also suggest ideas put forward for implementation of security in IoT.

Key words: Attacks · Security Framework · Internet of Things · Security · Wireless Sensor Networks

INTRODUCTION

In today's world as the population is increasing, the demands of the people are also increasing. As years pass, new technologies are evolved and people with these new technologies try to satisfy consumer needs. IoT was one such technology that was coined in the year 1999 by a British entrepreneur, Kevin Ashton while working at auto-id labs.IoT that is internet of things by its name tells some things or gadgets are connected to internet. That 'some' things or gadgets are the electronic devices like sensors, actuators etc that sense data from physical devices like home, buildings, vehicles etc. These sensed data are processed using Softwares and then stored. You might think where these large processed data are stored…? These data are stored in cloud-a virtual storage. The recipients receive there message from the cloud. A framework for IoT is shown in Figure 1.

The middle ground between sensor and cloud follows the wireless sensor network (WSN) or wired sensor network. Even though the security of data is the main problem in IoT, it's still flowering in many areas for developing applications. According to Gartner report, 6.4 billion IoT devices will be in use worldwide and 5.5 things will be connected every day in the current year respectively. It will reach 20.8 billion by 2020. By 2025 all the devices will be connected to our life was stated by US national intelligence council [1]. Many organizations are putting there hands together to make IoT applications to reach the pinnacle. Some organization and companies that are giving importance for this technology are NASSCOM, Cisco, IBM and many more. Even though many companies use their own secured measures, hackers still attack the system. So to eliminate forging and morphing of the data and bringing security into role can be achieved by analyzing and providing a lightweight algorithm from a hacker's perspective.

The paper is categorized into following sections. Section II tells about the IoT architecture. Section III displays the types of attack on IoT devices. Section IV briefs the contribution by various companies. Section V discusses about IoT in various fields. Section VI exhibits literature survey of security in IoT, Section VII exemplifies security requirements in IoT. Section VIII presents challenges in IoT. Section IX wind-ups the paper.

IoT Architecture: The architecture is of four levels [2]. They are:

- Perception layer
- Network layer
- Middle-ware layer
- Application layer

Perception Layer: In this layer, sensors are installed in a WSN. Wireless sensor network is a group of transducers with communication services. The network consists of distributed sensor nodes which are small,

Corresponding Author: S. Sreega, Department of EEE, Karpagam College of Engineering, Coimbatore, India.

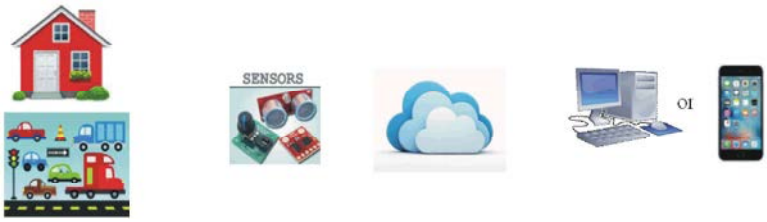

Fig. 1: A framework for an IoT based system

mobile, lightweight to sense data like temperature, pressure, speed, body conditions etc. The sensor nodes communicate with each other to transfer the data. A sensor node is also known as mote especially in North America. A node consists of the following:

- Controller
- Transceiver
- External memory
- Power source
- Sensors

Controller: The controller carries out the role, processes the data and controls the operations of other devices in the sensor node. The generally used controllers are microcontrollers. Other than this, microprocessors, field-programmable gate arrays (FPGA), application-integrated circuits (ASIC). Microcontroller is mostly used as it is economical, easily programmable and easy to connect with devices and less power expending. Microprocessors are not preferred as it consumes more power.

Transceiver: A Transceiver is combination of radio transmitter and receiver respectively. They are used for communicating information between nodes and base station. Present pandits are trying to find a WSN node consuming less power because each node runs on battery which is not reliable. If a battery fails it has to be replaced by someone leading to rise in maintenance cost. Transceiver consumes majority of power free to a sensor node for transmitting packets [3]. The energy consumed by WSN transceiver is known by a) active state,b) sleep state and c) transition states.

Memory: In WSN [4, 5], memory is used for storing application related data and program for the device. The contemporary WSN nodes consist of a)RAM(random access memory) for swift data storage,b)EEPROM for storing raw facts,c)internal flash for storing code and d) external flash for constant data. EEPROM and Flash memory are same but the only difference is that EEPROM data is erased and rewrote one byte at a time whereas in flash the process takes place in entire blocks hence making it speed memory. Flash and RAM memory is non-volatile in nature.

Power Source: In WSN node battery is used as power source. All the components of a sensor node need power to sense, process the data and communicate the data. Most of the power is consumed for data communication. Since the sensor nodes placed in remote places, rechargeable and non-rechargeable batteries are used. The power consumption can be reduced by DPM and DVS. In DPM (dynamic power management) the unactive part of a node is shut off. In DVS (dynamic voltage scaling) the voltage level is increased and decreased along with frequency, leading to power consumption. Nowadays great scholars are trying to find batteries of small size with enhanced performance. A pandit found a way to deposit a thin film lithium battery on the chips [6].

Sensors: Sensor is a hardware device that sense physical condition like temperature, pressure, people presence etc. The data sensed which is analog is converted to digital by analog-to-digital converter (ADC) and then is transferred to microcontroller for processing. Sensors are small in size, low power consumption and work at high volumetric energy densities. Each node has certain area it covers for which the observed data can be reported.

Network Layer: The objective of this layer is to transmit the sensed data from perception layer to particular data processing system through available network. The data can be transferred through LAN (WiFi, Ethernet), PAN (ZigBee, Bluetooth, 6LowPAN). Sensors that need not require connectivity to a LAN can be connected directly to WAN through internet. These are known as Gateways. Routing of packets occur here.

Middle-ware Layer: In this layer, information processing system is present. The data is sent to be processed and the system links with the database to store the data. It's of four types.

- Interface protocols
- Device abstraction
- Control and management
- Application abstraction

Application Layer: In this layer, the IoT understands the need of data and transfers to the recipient like mobile, computer etc.

Attacks on IoT Device: IoT devices are increasing in production due to the contribution of many companies. The devices are used in many fields where data security in a must. But as IoT devices are connected via internet, anyone can hack or read others data leading to no privacy of data. In recent survey, it was found that in 2015 the attacks on IoT devices have doubled. Due to this china has prohibited armed forces to use internet connected devices. The percent attack on devices and systems in 2014 and 2015 is listed below.

Table 1: The percent attack on devices and systems in 2014 and 2015

	Devices attack (in percent)			
Year	Mobile devices	Embedded systems	Consumer technologies	Operational systems
2014	24	13	11	10
2015	36	30	29	26

Erven and his team in 2014 unfolded two years research study on defenceless of medical devices. They noticed that anyone could change the dosage levels remotely. The researches also told that by plugging laptops plug into diagnostic ports, one can control the steering wheel, break system and headlight. In the crux, IoT devices can be attacked in various ways. They are listed below [7, 8].

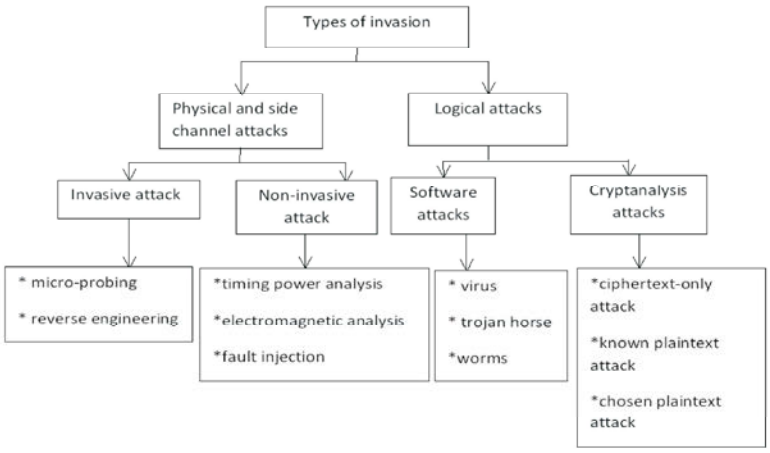

Fig. 2: Taxonomy of Invasion

Physical Attacks: Hardware along with software runs most of the application. Nowadays physical attacks on devices are increasing.

Invasive Attack: It refers to physical attack of the system by irreversibly changing the properties of the chip. The objective of this attack is to capture data in the memory or flowing through the bus, register. Types of invasive attacks are listed below.

Micro-Probing: Its direct access to chip surface to observe, manipulate or tamper the system working.

Reverse Engineering: Its understanding the structure and working of the semiconductor device to create a replica of it.

Non-Invasive Attack: This attack does not need the device to be opened. But this attack needs time and creativity and is cheap when compared to invasive attack. The encrypted devices provide radiation, power consumption, timing and so information that are easily measurable. This attack uses this information to recover the key of the device. Types of non-invasive attacks are listed below.

Timing Power Analysis: Here power consumption is measured in time. To measure power consumption in time, a PC with an oscilloscope and a resistor in small size is placed in power supply line. Its were difficult to say whether its in W/O process. But the inner data is useful. To perform this, a little knowledge in electrical engineering and signal processing is enough. It has two basic methods. They are

Simple Power Analysis (SPA)
Differential Power Analysis (DPA)
Electromagnetic Analysis: Here emissions are measured. Its same as power analysis but the only difference is that instead of resistor, a small magnetic coil is positioned over the chip. It also has two basic methods. They are

Simple electromagnetic Analysis (SEMA)
Differential Electromagnetic Analysis (DEMA): Fault Injection: Its cost is typically low. For this detailed knowledge of circuit is required. It has many methods. They are

Thermal Glitching: In this, the chip is cooled or heated beyond operating limits. As it is hrad to control, it is mostly not used.

Voltage Glitching: Here the powers supply is made to drop below minimum. The contents of SRAM may be corrupted and RC propagation delay increases. It is commonly used for attacking,

Temperature Glitching:
Clock/Timing Glitching: Here a short clock pulse is sent. It can be controlled and is commonly used.

Radiation Glitching: In Radiation Glitching, the device is irradiated using X-rays, Gamma rays, UV/visible light/IR, alpha particles, neutron etc.

Semi-Invasive Method: This method also includes opening of the chip to get data like invasive attack. The cost is less and can be performed in a short time. This attack can be done using X-rays, UV rays etc.

Logical Attacks: Softwares that are used to destroy a computer is called malware. This is of two types.

Software Attacks: In this kind of attack, malicious software is used to interrupt operations of the computer, get the data and display unwanted ads and access to private computers. In 2011, most of the threats were due to worms and Trojan horse. The examples are virus, worms, Trojan etc.

Cryptanalysis Attack: The Cryptanalysis aim is to decrypt the ciphered data. There are four types. They are listed below.

Ciphertext-only: The cryptanalyst has access only to the ciphered text. This attack is kind of difficult.

Known-Plaintext: In this attack, the cryptanalyst gets the ciphered text and plaintext of it as well.

Chosen-Plaintext: In this attack, the attacker can choose any quantity of plaintext then gets the ciphered encrypted texts. It is of two types.

Batch Chosen-Plaintext: In this, the attacker chooses all the plaintexts before being encrypted.

Adaptive Chosen-Plaintext: In this, the attacker chooses the plaintext dynamically and change the opinion based on previous encryptions.

Chosen-Ciphertext: In this attack, the attacker selects one ciphered text and receives a decrypted plaintext of it. It is of two types:

Indifferent Chosen-Plaintext: It is also known as"lunchtime" or "midnight" or "indifferent" attack. Here the attacker can make adaptive chosen-ciphertext queries but only up to some time. After that the attacker must show some ability to attack the system.

Adaptive Chosen-Plaintext: In this the attack, the cryptanalyst chooses his ciphered text by sending all these text for decryption. After decryption, the results are used to select the desired cipher text.

These are network attacks that occur in data transition. They are listed below.

Spoofing/Poisoning: Here the data is made to appear to have come from somewhere it is not or be something that it is not. The attackers do it by changing IP source address, MAC address and DNS info.

Man-in-the-middle: The two end people think they are communicating with each other. But the attacker intercepts their communication without the two's knowledge.

Replay: During the transmission the data is captured by the attacker and is send off later.

For example, Consider A and C wants to communicate. To do that A decides to authenticate and send the user name and password to C. But the person in the middle that is B seizes the user name and password of A and keeps a copy of it. So A and C communicates with B in the middle. When A disconnects, B uses the user name and password to connect with C.But c is unaware of it. This is told replay.

Denial of Service (DoS): In this the attacker overloads the web server by loading large amount of data. This crashes one operating system and slows down the internet.

Distributed Denial of Service: In DDoS, the attacker through other computer attacks the victim. The intermediate computers do not know that their sources are used for this. After completion of the work, the details of intermediate computers are deleted so that no one will doubt.

Contribution: For a technology to proliferate, great pandits or organizations aid must be the main requisite. Even users play an important in the rise of a technology. For the IoT technology to develop many organizations or companies helped. They are as follows:

- Google's IoT home connects is android at home platform coming out to the world in the year 2012. In that respective year it was a deadly new to the humanity. We might have heard different ways of controlling a device. But this platform led the world to a different path to control things. With the help of this platform, people can control household devices using voice. But this failed as they were not able to find manufacturers who could adopt their hardware standards.
- CISCO introduced fog computing (router +server). In the current iot trend, the sensed data is processed and sent to the cloud. The sensed data may include wanted and unwanted information. As this unwanted data also gets stored along with wanted information, more space is occupied in the cloud. As a result, the cost is increased. To overcome this problem, fog computing came into role. They created a router architecture called 'Iox' which combines router and server. For example, there is a chemical in a room which is very temperature sensitive that is for high temperature it can be dangerous. So a temperature sensor is fixed in the room to keep an eye on the room temperature.when the temperature is normal it will send a 'normal' message continuously to the server. This can lead to server hanging as the data keeps on occupying more space.so no need of sending this millions of 'normal' message to the cloud server. It is enough for the router to concede these messages. In case the room temperature extends the constraint, then the message will be sent to the cloud server via router to alert the user. But this still has not been implemented.
- Nasscom [9] promulgated the India's first centre of excellence (CoE). Under p3 the governmnent has planned to help them. Even other industries are ready to join their hands with Nasscom to support IoT industry.The CoE is a joint ventureof the Department of Electronics and Information Technology, education and research network and the IT industry body.The centers will be placed in major cities to support people's innovative ideas.It will also provide equipments, kits and everything required to build an IoT application. They have planned five centers with lab, office infrastructure and other necessities. The credits for initiating CoE go to minster of information technology, Ravi Shankar prasad.
- Cisco was the first company to help the iot field to grow. The company has invested 100 million dollars for IoT startup companies to improve the IoT and their hardware business.
- Xoriant, an American based software product engineering and service company through its IoT centers of excellence (CoE) has great skills in m2m (machine-to machine) communication, cloud, analytics, mobile. The company has also the skill to designed the next generation OS (operating system) for IoT.
- IBM Watson is a technology platform that included natural language processing and machine learning to provide correct data. IBM in thought of making its cognitive computing system more useful for IoT, joined with Cisco to take Watson out of the clouds and place it near all machines and sensors collecting raw facts.now IBM Watson and its BA (business analytic) can run on Cisco's gateway gear for which no internet connection is required. It's for business operation in remote location were internet connectivity is not reliable.
- Intel Company introduced new platform, related software and services for security, scalability, manageability and interoperability of data. The IoT platform includes modernize of Intel gateway, edge management middleware from Wind River, increased McAfee security and application program interface and traffic management tools. Dell, Accenture, TCS, Wipro and others have joined with Intel to work on this new IoT platform.
- Intel introduced Quark,a series of low power microcontroller chips to increase its cloud computing processors.
- Libelium on 21st June 2016 introduced ten new kits for the IoT Marketplace.

- IZOT platform is an IP enabled and software manager that helps in development of industrial IoT devices.
- A project of O' Reilly Media has made the data sensing lab to deploy 500 sensor motes at important locations around the Moscone West center. Some of these sensors measure noise, temperature, noise, humidity and light levels [10].
- Lively is a new upcoming IoT company funded by VC firm. It was launched in 2013.

Since these companies laid an helping for IoT, it has flourished in various areas.The status of IoT in various categories is listed below.

Category	Status
Agriculture	Matured
City and building	Matured
Automotive	Matured
Industrial	New
Corporate	Matured
Security	New
Retail	Matured

IOT in Various Fields

IoT in Home Automation: There have been many new and wonderful products evolving and still evolving from this field which has made most of the task automatic, simple and faster. They have reduced the man power needed. According to Forbes, ATM was the first IoT objects.Some of the IoT products are discussed below.

IoT or smart refrigerator [11]: In 2000, LG introduced IoT refrigerator but it was not successful as people thought it was exorbitant and its introduction was obscure. But nowadays in abroad countries iot refrigerators are used. In India IoT refrigerator is rarely used. At CES 2016 in Las Vegas Samsung will be exhibiting its next generation refrigerator called as 'family hub' [12]. IoT refrigerator senses the products stored in the fridge and checks if any shortage of groceries occurs. If it happens it sends a message to the recipient or calls to the nearby store and requests for home delivery.

3D Printing: 3D printing also known as additive manufacturing is a process to create objects in no time under computer control irrespective of its shape. The process issued in various fields like medical, food, research, apparel, vehicles, construction, art etc. Using 3D printing,a house can be constructed in 3-5hrs.IoT field uses this process for creating objects.[13] For example,two professors of King Abdullah university,Saudi Arabia thought of creating a wireless sensor network to create a smart city. So they made mobile sensors using 3d printing.In medical, it is very helpful in planning for surgeries [14].

IoT or Smart Light Bulbs: Smart light bulbs are light emitting diode bulbs (LED) that are enabled with Wi-Fi. It is often sold in kits. They allow controlling the brightness of light and also provide various colour [15]. Philips hue is a wireless LED lighting. It is sold online.

Smart Washing Machine: Smart washing machine works on WiFi making it easy for users to wash their clothes irrespective of the place where they are present.It user's right amount of energy and water by monitoring the weight of clothes loaded. Many companies like Samsung, LG and IFB have launched their own smart washing machines.

Smart Thermostat: Nest Learning thermostat is a brilliant IoT device which saves billions of kilowatt hours of energy. Its senses the temperature and maintains it. It even understands your likes of temperature and alerts if the home temperature is too hot or cold. It also turns off itself when no one is at home and can even set temperature from any place. We can also see how many energy we have used everyday and we can also know how to use less. Even the payment process is done by itself.

Air Quality Egg: Air Quality Egg is used to measure the nitrogen dioxide and carbon monoxide content in the air. It helps in telling the quality of air and it's very low cost. It can be done using DIY sensors.

Amazon Echo: Amazon Echo is a product developed by Amazon. It consists of 7 microphones in an array. It works on voice. By saying Alexa, you can enable it. If we have many echo, we can name wake works like 'amazon' or 'echo'. With the help of this we can listen to anything we want. It can sense your voice even when the music sound is high. It can also control other smart devices at home. It charges the room with 360 degree omni-directional audio. AWS IoT Button: AWS Iot Buttons are used to order goods online just by pressing a button. It comes in packs. After receiving, they compute each button to order the specific product. Configure them and stick it near the product. For example if your washing powder is out of stock, by pressing the button on the washing machine is enough. next minute the commodity will be at the door step.

Smart Heater: Holmes smart WiFi enabled smart heater allows us to control the heater from our mobiles.

Motorola Moto 360: It is a wearable and provides chance to work without phone. It helps by sending all important data to Moto 360 from your phone directly. So even if he or she forgets the phone, it won't be a problem as Moto 360 is there.

IoT in Agriculture: Agriculture is the source of food for all living beings in the world. Many years ago, 90 percent of the population in USA did agriculture to feed themselves. But nowadays only 2% of the population is doing agriculture also providing fruits, meats and dairy products. This drastic reduction of people in food production is due to technology development. Farmers make use of the technology to increase the food productivity for the emerging world. Due to technology growth, a farmer feeds nearly 155 people today. In the crux, less population provides food for a big population by use of motorized equipment's. It has been 16 years since IoT came into introduction. From then till now, many have been trying to implement IoT in agriculture for increasing the productivity, quality of crops and also saving water and time.A smart water saving irrigation system was proposed by three Chinese scholars. It was used to measure moisture content and height of water in soil. It was implemented in congyu vegetable fields of Guangzhou and was found suitable for rice growth [16]. In [17], soil moisture sensor and temperature sensors were placed in the soil. The data was then transmitted to the web application. In microcontroller an algorithm was written to measure the threshold values of two sensors used to control water quantity. Solar panels were used for power. Then the data were inspected and schedule for irrigation was done through a webpage. This method was tried for 136 days and 90 percentages was saved when compared with normal irrigation. When agricultural fields are located in remote areas, it becomes very costly to send people out to the fields. If the fields are vast then watering and taking care of the field also becomes expensive. To overcome these issues some IoT products for agriculture are listed below.

Rachio is a smart sprinkler that works on WiFi. The gateway for rachio is the controller. Android app or iOS app must be downloaded. Rachio studies the soil, amount of sun exposure; weather ans so on and decides when to water, how much to water. Rachio helps in saving water and money. Skydrop smart watering sprinkler controller is another product same as rachio.In agriculture it can be implemented but its costly.

OpenIoT's Phenonet [18] is a network of wireless sensor nodes which senses various data of the crops in the field, processes and analyzes the data to find the best varieties of crops to increase the yield. The sensor detects air temperature, humidity and soil temperature. OpenIoT [19] is an open source middleware which got awarded as the best open source platform of IoT in 2013. It was also awarded as "best semantic interoperability" in 2014 at IoT hackaton.

When the elevator loads the silos with grains using the conveyors, there are possibilities for bearings catching fire. Even the grains in the silos can be infected due to bacteria and moisture leading to fire. The fire due to dust produced during loading in to silos is also hazardous. In response to these issues, Tempu Company which provides software and hardware for farms with elevators with the help of GE Company introduced Temputech's wireless sensor monitoring system which connects all the sensors helping the farmers. There is an arrangement to stop the conveyor belt if the bearings become hot or the belt is slow. There is also a monitor in the control room which displays the sensors deployed. If any problem occurs, it lets the farmer know which part of the system has gone wrong[20]. The message is sent to mobile as well as to their emails making it easy for the grain breeders [21].

CLASS is an agricultural machine manufacturing company. Claas Company is joining with 365farmnet-a program using which the whole agricultural land can be monitored from home by using computers or mobiles. It combines GPS and GPRS. The SIM they use are produced by Wireless Logic of United Kingdom. These SIM help in data flow from machine to internet through mobile network [22].

In 2009, CleanGrow an company in Ireland unfolded a nanotube or ISE sensor to check the nutrients level in the water so the farmer can change the maturity rate and colour of production of crops. CleanGrow device houses 6 sensors.

PrecisionHawk, a commercial drone company located at North Carolina developed unmanned air vehicles. When these UAE's are ready to take off, the farmer tells which field is to be surveyed, from which height the images must be captured or elevation. The drones detect the best path for flight as they can sense the climate conditions by artificial intelligence. It can also measure wind pressure and speed. During the flight, these drones capture thermal, multispectral and thermal images of the land for one centimeter per pixel. During landing,it lands at the same place from where it took off.

Yamaha, Japanese manufacturing company has created unmanned vehicles which are used for spraying purpose for agricultural lands. In japan, these drones are used for spraying rice fields. Even they have decided to supply for farmers in USA.

In Italy, tobacco production is prime. For tobacco's growth, certain climate conditions are required. To ovecome this issue, TeamDev -an Italian based software company placed Libelium's Waspmote Plug and Sense platform to gather weather conditions that will be favourable for tobaccos growth [23]. By seeing this, Senseye, a UK software company thought of adopting this method in UK fields. This protected the plants from pest infestations. The devices communicated with Senseye's cloud via GPRS.

IoT in Health care: Uro Sense: The product is used to measure the urine output and core body temperature automatically on catheterized patients. The continuous monitoring of these two things help the patients in prior to know the state of their kidneys and heart so that the patients can have treatment and diagnosis for tumors,heart and kidney failures,infectious disease,diabetes,hypothermia and sepsis. It can report the data directly to the nursing station from anywhere through WiFi.

Philip's Lifeline: Philip has developed a 24/7 hours around the clock facility for people using this product to monitor the user's condition every second. It can be put around the neck like a pendent. When the user falls off, by pressing the button we can call an ambulance or someone for help. Also when a person becomes unconscious, it will automatically make a call without pressing the button. It also helps to connect with trained personnel response associate.

Philips Medication Dispenser: It is for those who take many medicines and have difficulty in remembering. It consists of a dispenser with 60 cups. It schedules medicines for 40 days. The medicines to be taken are loaded in the cups. When we hear the remainder, press the button. The medicines loaded will be dispensed. If the medicines are missed, the cup will go to the medicine missed storage bin. It works only for solid medicines.for liquid medicines there's a remainder. If the user forgets to take the medication, then the user receives a call.

Masimo Radical-7: It is a health monitoring system that sends a detailed picture of status of the patients to the personnel doctors. The doctors can review the status from anywhere as it uses wireless connection.

Home Health Hub: Freescale's Home Health Hub is on which gets health data from commercials devices like pulse oximeters, blood pressure meters and so on through wired or wireless connection. The data received is stored in the cloud securely and is sent to the caretaker or recipient who is monitored. This platform helps in achieving telehealth. Telehealth means doctor monitoring and advising the patient from anywhere through wireless connection.

Jawbone UP2: It is a band that tracks our day to day activity, sleeping patterns and food logging. It is available in many colors and styles and is wearable.

Fitbit Charge HR: Its a band tracker that tracks one's sleeping pattern, heart rate, workout. Its also gets notification calls.

IoT in Retail: In retail domain, IoT is a game changer. Present companies are trying to implement IoT in retail area to engage customers. By doing this companies sales increases leading to less operating cost. Automated retailing alone in US is forty two billion dollar opportunity.The products to captivate the consumers are listed below.

Intel's Digital Signage: It provides a greater experience of shopping. For example: Intel's digital signage Pepsi machine. It is a interactive machine with touch screen. Consumers can choose type of drink and bottles respectively then touch to vend. While enjoying the drinks, consumers can continue to interact with the machine in a more one on one fashion. They can watch videos and play games and get the gifts if they have chosen. They can also send the gifts to people across the world where they are sent a promo code with their email address and then they can take that to the machine and redeem it. It is available in five big malls in United States of America.

Smart Vending Machine: Intel and N&W together designed an IoT based vending machine. It has a transparent glass screen which plays videos. On the right

side are button like images for choosing beverages, snacks and camera. The camera senses the age, gender and the time the user spent interacting with it and these data are stored in the clouds. By this the owner can know who all used it. Since a real integrated sensor camera is present, just by gestures on can select the snacks, beverages or lunch one wants to have. It can be used in places where it is crowded or in sterile environments like hospitals. It can also be operated using mobile. By 2016, five thousand vending machines will be produced.

Yourcegid Retail: It is a cloud based retail management and POS solution for specialty retailers. It is quick to deploy and easy to scale. The owner can have a track of the sales across all his stores all over the world so he can know which of his product sales is high and increase that product sale. In 2014, TCI Company implemented this software in its 28 Australian stores and planned to deploy this in Asia and America.

POS Mobiles: Shopkeeps POS mobile is cloud based point of sales system. All their registers run on iPad and iPad Mini and the rest works on clouds. For example using iPad Mini you can order any product from anywhere. It is portable. One can call customers also. It is useful for quick survey retailers. This iPad has mac tech's dynamo and Star Micronics mobile printing.

ELO Tablet: It is same like POS mobiles. It has smart card readers. It is equipped with WiFi and Bluetooth. In offline there is no problem in printing. It is also equipped with NFC and RFID. This helps consumers to purchase on spot quickly. It runs Microsoft windows on Intel processor. It has integrated MSR and smart card readers to easily get paid by anyone, anywher and anytime. Its touch screen and has camera for scanning.

Cegid's innovations store has all latest innovation. It uses POS mobiles, Yourcegid cloud based management, digital signage and so on.

IoT in Smart Cities: In 2015, the Prime minister of India, Narendra Modi launched smart city concept in order to make many states in India a smart one. A smart city is one which makes good use of the upcoming new technologies and makes products that help in conserving energy, provide proper solid management, providing transport and electricity facilities in urban areas. There are some smart products that are listed below.

Bigbelly Smart Waste and Recycling: Its solar powered which is used in waste managing. When the waste keeps on filling the bin, a sensor measures the capacity and a compactor presses down the waste in the bin so that it can swallow eight times more waste than a standard bin before it fills up. Then its sends a email saying when how much full it is and when it has to be emptied. It has proved to reduce the number of collection by up to 88%. it also reduces collection cost by 75%. It also reduces emmision of carbon-di-oxide, leading to fuel saving. It uses cloud driven technology and smart data to make all countries smart across the world.

CitySense Plus: It is automatic street light control. It reduces light brightness based on the presence of people and vehicles. If any interference, its filtered out. The brightness is 100 percent, when the system fails. It ensures that the street is not completely dark. So it reduces the light intensity to 20 percent. It is combined to the CitySense software. The energy is efficiently used and low carbon-di-oxide emissions occur. Nuenen is a small town in Netherlands[23]. The town inhabits around 22,500 people and roughly. There was not much light at night. So the city council approached Tvilight to install their CitySense. After it was installed the people are happy as it is not too dark at night [24].

Libelium Smart Parking System: It is a automatic car parking system with LoRaWan and Sigfox helping one to detect accessible parking spots. The features are that it is small in size, provides high accuracy, low cost and easy installation respectively and fast detection. It's placed on road surface. The special feature is that it can work in both the radio technologies simultaneously or switch from one to another through cloud easily.

IoT in Automotive or Transportation: GE Evolution series tier 4 locomotives: It's loaded with 250 sensors arranging 150,000 data in a minute. When the data combine with other incoming data from operating and informational system helps in foreseeing events and taking driving lessons in real times. Normal train uses 3000 hundred gallons of fuel. But this uses only 10 percent of it.

Caterpillar's New Machine: It helps its dealers to achieve industrial analytic through IoT. So it collects data from locomotives like machines, tools and engines and shares those data with the customers. So this helps them to know where the fault is present, schedule maintenance, manage them.

IoT in Industrial Automation: Smart Structures embedded data collector: In industry it's very important to tell the quality of cement. This is done by the embedded data collector. Here the sensor is embedded in the concrete during pouring and curing. So now it becomes permanent part of the building. It tells the strength and quality of the concrete to the workstation of Smart Structure directly.

Iot in Energy Management: Smart metering: It helps in easier energy management and was produced byLandis+Gyr. It helps consumer in knowing their energy needs and also helps in load management.

Smart Grid Management: It's also established by Landis + Gyr Company. This works with metering ad sensor networks for load management, distribution automation and energy storage.

Literature Survey on Security: In [25], they proposed a framework for embedded security for IoT devices. The terms performance, cost and security are contradictory to one another. That means, when the performance is high, the cost is also high. But if the cost decreases, then security and performance both decreases. Through this framework these three can be brought on par with one another that is at a low cost a system can achieve both performance and security. The framework is a combination of hardware and software with three layered architecture consisting of hardware, software with lightweight protocols and MAC layer.

In [26], they implemented optimized DTLS on the MagoNode, a low power, tinyOS compatible fully designed wireless sensor node for security purpose. It operates in ISM 2.4Ghz band. The OS they used was TinyOS 2.x. Using nesC programming language they developed their solution. Using optimized DTLS, they reduced execution time and memory operations. Experimental results showed increased network lifetimeby a factor of up to 6.5. Security was established through CoAP.

In [27], they proposed a security model for IoT. They chose a cube structure for security, privacy and trust. As cube has three dimensions, the convergence of security,trust and security is depicted clearly. So to grant/reject access of data is difficult. So to overcome this, it must address: authorization (security), respondent (privacy) and reputation (trust) that is the convergence of these three terms.

In [28], a security architecture IPM for U2IoT model. The U2IoT heterogeneous system comprises of Unit IoT and Ubiquitous IoT. Unit IoT comprises IoT network and sensors, distributed motes and centralized, management data center. Ubiquitous IoT comprises the centralized and management data center for local, national and industrial IoT's. The objective was to provide integrated security architecture taking cyber -physical- social world into consideration. The three dimensional model IPM is addressed as information, physical and management security respectively. The perspectives for information security are security layer and requirement respectively. Artificial immunity is used for physical security. Through series of social strategies, management security is achieved.

In [29], two Chinese authors proposed a fast and efficient algorithm to detect integrity of commodities and secure the data of owner based on IoT and Chinese Remainder Theorem (CRT). They then conducted experiments to compare the properties of their algorithm with TRP and their algorithm proved to be good.

In [30], authors designed an algorithm to monitor the structure of the Tsing Ma Bridge. By monitoring with 128Hz from the end nodes the wireless sensor network achieved the frequency analysis of the bridge. Moreover using ARM Cortex M3 processor, a local-data-processing node was developed to increase the potential of the system.

Due to lack of cryptography in RFID, in [31] authors designed an algorithm based on XOR operations. They found that using this algorithm the flaws or weakness in RFID can be improved. It can be also used to establish mutual authentication in RFID.

In [32], a highly strong and efficient lightweight algorithm ESLRAS for authentication in RFID was developed. To increase the efficiency, the key k is selected to reduce the hash computing occurring in the database. To prevent the synchronization and tracking attack the tag is placed in the database and constantly updated. The reader and tag generate random numbers which is used to protect the replay attack. The algorithm correctness was proved by GNY logic.

In [33], the authors proposed a new protocol by combining Physical Unclonable Functions (PUF) and Physical Key Generation (PKG) to overcome anti-counterfeiting problem. These two are based on physical properties of the digital circuits.they evaluated their idea by using generalized architecture of a smart home

network. By using the two methods they could say that the overall cost of the system decreased and provided authentication.

The present authenticating schemes do not seem to be lightweight and secure and due to the presence large number of heterogeneous devices, there's a need of a scalable authentication scheme. To provide this, in [34] authors introduced the TCGA (Threshold Cryptography based Group Authentication) scheme. This scheme was proposed using Paillier Threshold Cryptography. It also generates a secret key at end of a group session, does encryption, hashing and is implemented in WiFi environment. In this paper, the authors compared TCGA with Group Authentication Scheme (GAS) based on number of handshake in Group Authority (GA) and between devices, computational time and TCGA was proved to perform better. The scheme also eradicates replay and man-in-the-middle attack.

In [35], the authors proposed a lightweight RFID mutual authentication with cache in the reader (LRMAPC). It reduces the transmission and computational cost when large number of tags needs to be authenticated. The correctness of this scheme was proved using GNY logic. When compared with other works, it proved to be of higher efficiency and strong security. But the cost was a bit more for storage space ie cache in the reader. The cache is used to store recently visited keys of tags, so that the tags can be authenticated directly in the reader.

In authors proposed lightweight authentication scheme which was employed in e-Health application and it was found suitable. HMAC, nonces and masked identity codes were used for dissimilar exchanges. They concentrated on the power consumption. When compared with available exchange techniques, its of low cost computation and communication with high security. Due the use of nonce cryptography, replay attacks are avoided.

Security Requirements for IoT: Following are the security measures to be followed.

User Identification: The user authenticates before using the system. Along with password and username, the image of the person also must be sent to the recipients system or mobile. When one enters and tries to connect with other system, the camera in PC must capture the persons face and send it to the receiver end so the receiver can decide to let access or deny.

Tamper Resistant: Even when the device falls in hands of attackers, the data can still be protected. To overcome timing attacks or side channel attacks, assembly language can be used. Instead of using microcontroller in sensor node, microprocessor can be used. Even if the energy consumption is more, their processing speed is high and they occupy less memory. For example, there were two projects of same topic. One was done using microcontroller while other one was done using microprocessor.the memory space occupied by the code in microprocessor was 624 bytes/8000bytes and another one's memory space used was 2900/8000 bytes. Since electronic equipment's have less space, microprocessor can be used. The lightweight algorithm must be developed using assembly language as the hacker needs programming knowledge.

Secure Content: The content transferred must be protected. This can be achieved through DRM approach.

Secure Network: In secure network, the net access is provided if the device is authorized.

Secure Data Tranfer: here the data communicated must be protected. For this lightweight algorithm can be used in which the key once used can't be used the next time. The user must once again generate. Cryptographic nonce can be implied.

Challenges in IoT: According to reports, 91% of data is unstructured. So there is a scope to convert the unstructured data into structured or valuable one.

There is no technology that provides 100 percent data accuracy. There is some loss of data over transmission. So there is a room to manoeuvre data accuracy.

There is no technology that can provide 100 percent security and privacy to the devices connected to the network. But the number of attacks can be reduced.

Interoperablity is also a great challenge in IoT. Different devices can be connected to one another in absence of human.

To reduce the overall cost, energy consumption must be low. But during data transfer losses occur. Hence the percentage loss can be reduced.

CONCLUSION

In this paper, a survey on attack in IoT and the percentage attack is presented. It displays the architecture

of IoT. The paper briefs on IoT in various field like agriculture, industry, retail, home automation etc. It also exemplifies the security requirements, literature review and challenges in IoT. It is believed that in the future we can access connectivity at anytime from anywhere to anyone.

REFERENCES

1. Luigi, A., I. Antonio and M. Giacomo, 2010.The Internet of Things: A survey. Science Direct journal of Computer Networks, 54: 2787-2805.
2. Farooq, M.U., Muhammad Waseem, Anjum Khairi and Sadia Mazhar, 2015. A Critical Analysis on the Security Concerns of Internet of Things (IoT), 111(7).
3. Odey, A.J. and Daoliang Li, 2012. low power transceiver design Parameters for Wireless Sensor Networks, 4: 243-249.
4. Prof. Manjiri Pathak, 2013. An approach to Memory Management in Wireless Sensor Networks, 4: 1172-1176.
5. http://rsta.royalsocietypublishing.org/content/370/1958/68.
6. Bates, J.B., N.J. Dudney, B. Neudecker, A. Ueda and C.D. Evans, 2000. Thin-Film Lithium and Lithium-Ion Batteries, ELSEVIER, 135: 33-45.
7. Ravi Srivaths, Anand Raghunathan, Paul kocher and Sunil Hattangady, 2004. Security in embedded systems:Design challenges,Transaction on embedded computing system(TECS), ACM, 3(3).
8. Kommerling Oliver and Markus G. Kuhn, 1999. Design Principles for Tamper-Resistant Smartcard Processors, USENIX Workshop on Smartcard Technology, Chicago, Illinois, USA.
9. http://www.nasscom.in/building-policy-framework-iot?fg=1149667.
10. Royer Michele, 2013. The internet of things,Bellevue College,A trends white paper,
11. Prapula, S.B, Dr G. Shoba and Dr T.C. Thanuja, 2015.smart refrigerator using internet of things, JMEST, pp: 2.
12. http://www.ibtimes.co.uk/ces-2016-samsung-showcase-internet-things-fridge-called-family-hub-1536010
13. http://3dprintingindustry.com/news/3d-printing-smart-sensors-34571/
14. Rengier, F., A. Mehndiratta, H. von Tengg-Kobligk, C.M. Zechmann, R. Unterhinninghofen, H.U. Kauczor and F.L. Giesel, 2010. 3D printing based on imaging data:review of medical applications, springer.
15. Kavehrad Mohsen, 2010. sustainable energy-efficient wireless applications using light,, , IEEE, 48: 66-73.
16. Kehui Xiao, Xiao Deqin and Luo Xiwen, 2010. smart water-saving irrigation system in precision agriculture based on wireless sensor network, transaction of the CSAE, 26: 11.
17. Gutierrez Joaquin, Juan Francisco Villa-Medina, Alejandra NietoGaribay and Miguel Ángel Porta-Gándara, 2013. Automated Irrigation System Using a Wireless Sensor Network and GPRS Module, IEEE.
18. http://www.csiro.au/en/Research/D61/Areas/Robotics-and-autonomous-systems/Internet-of-Things/Phenonet
19. Consortium OpenIoT, 2012. Open source solution for the internet of things into the cloud, January, http: //www.openiot.eu.
20. http://www.informationweek.com/big-data/software-platforms/ge-powers-internet-of-agriculture/d/d-id/1306646.
21. http://iotbusinessnews.com/2012/12/21/79411-global-agricultural-equipment-manufacturer-reaps-telematics-benefits-with-gprs-communications-via-wireless-logic/
22. http://www.libelium.com/increasing-tobacco-crops-quality-by-climatic-conditions-control/
23. http:// www.tvilight.com/ wp-content/ uploads/ 2015/12/CaseStudies_ResidentialArea_ENGLISH.pdf
24. Babar Sachin, Antonietta Stango, Neeli Prasad, Jaydip Sen and Ramjee Prasad, 2011. Proposed Embedded Security Framework for Internet of Things, IEEE, pp: 1-5.
25. Capossele Angelo, Alerio Cervo, Gianluca De Cicco and Chiara petrioli, 2015. Security as a CoAP resource:an optimized DTLS implementation for the IoT, IEEE, pp: 549-554.
26. Babar Sachin, Parikshit Mahalle, Antonietta Stango, Neeli Prasad and Ramjee Prasad, 2010. Proposed Security Model and Threat Taxonomy for the Internet of Things, Springer, pp: 420-429.
27. Ning Huansheng and Hong Liu, 2012. Cyber-Physical-Social Based Security Architecture for Future Internet of Things, Sci. Res., 2: 1-7.
28. Li Chaoliang and Guojun Wang, 2012. A Light-Weight Commodity Integrity Detection Algorithm Based on Chinese Remainder Theorem, IEEE, pp: 1018-1023.
29. Hsu Chia-Hao, Chih-Ting LinHui-Ping Tserng and Jen-Yu Han, 2014. An Implementation of Light-Weight Compression Algorithm for Wireless Sensor Network Technology in Structure Health Monitoring, IEEE, pp: 548-552.

30. Lee Jun-Ya, Wei-Cheng Lin and Yu-Hung Huang, 2014. A Lightweight Authentication Protocol for Internet of Things, IEEE, pp: 1-2.
31. Fan Kai, Jie Li and Hui Li, Xiaohui Liang, Xuemin Shen and Yintang Yang, 2012. ESLRAS: A Lightweight RFID Authentication Scheme with High Efficiency and Strong Security for Internet of Things, IEEE, pp: 323-328.
32. Huth Christopher, Jan Zibuschka, Paul Duplys and Tim Guneysu, 2015. Securing Systems on the Internet of Things via Physical Properties of Devices and Communications, IEEE, pp: 8-13.
33. Parikshit N. Mahalle, Neeli Rashmi Prasad and Ramjee Prasad, 2014. Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT), IEEE, pp: 1-5.
34. Fan Kai, Chen Liang,Hui Li and Yintang Yang, 2014. LRMAPC: a lightweight RFID mutual authentication protocol with cache in the reader for IoT, IEEE, pp: 276-280.
35. Khemissa Hamza and Djamel Tandjaoui, 2015. A Lightweight Authentication Scheme for E-health applications in the context of Internet of Things, IEEE, pp: 90-95.