Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 6, Issue 06, June -2019

Internet of Things in the field of Asset Tracking

Anilavo Datta[1], Dhanashri Kulkarni [2]

[1] *Computer Engineering, D.Y. Patil College of Engineering*
[2] *Computer Engineering, D.Y. Patil College of Engineering*

Abstract - *The Internet of Things could be a novel paradigm shift in IT arena. IoT is one of the most researched topics in the field of Information Technology and Communication, for this technology possesses the potential of transforming the real-world objects into smart virtual objects. While the previous era was about connecting people; this era looks forward to connecting things and unifying them into a single infrastructure. More than a billion devices would be connected worldwide in the next two years. The paper attempts to provide a holistic view of the IoT technology, right from the basic architecture to the future scope of this technology. Initially, the paper outlines the basic architecture of IoT, explaining how various devices or "things" are connected to the network/internet, which in turn connects it to the IoT Application. Various types of sensors, actuators, network technologies and protocols, have been elaborated upon to evaluate the different parameters that can be monitored. By focusing on a few use cases for vehicle tracking, school children safety, temperature monitoring, etc., a walkthrough of a typical IoT application, its analytics and reporting, has also been discussed upon.*

Further focus is on explaining how key architectural directives are set, the methodology behind selection of the architecture type, the pain points while architecture deployment, etc. How various systems are integrated with one another and with the application, as well as how the application is integrated with sensor-embedded devices has also been taken into account. While exploring more technical details of the application, various different Application enablement platforms, different protocols for device and system integration, etc. are found out. As already mentioned, the technology of IoT has immense potential to revolutionise industry automation, lifestyle, healthcare, entertainment, etc. While expanding horizons and a rational extrapolation, an attempt has been made to visualise a holistic view of the IoT technology of tomorrow, of what it brings to the table.

Keywords – *IoT, Asset Tracking, Autonomous Vehicle, Vehicular Communication, Machine to Machine Communication*

I. INTRODUCTION

The net may well be a made of interconnected laptop networks that use the standard web protocol suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of immeasurable non-public, public, academic, business, and government networks, of native to international scope, that square measure connected by a broad array of electronic, wireless and optical networking technologies. While returning to the items, which will be any object or person which might be distinguishable by the $64000 world.
Everyday objects such as food, clothing; and furniture; materials, parts and equipment, merchandise, etc. That means here things can be both living things like person, animals, plants, etc. and non-living things. So at this time, things square measure real objects during this physical or material world.

The growth of the Internet of Things (IoT) has been catalysed by the requirement of large organisations to automate their business processes and be able to follow all objects throughout the commodity chain, they are embedded in. The ability to program objects have made it possible for the companies to reduce error, be more efficient, speed up processes and improve security.

The IoT is expected to transform how human beings live, work and play. From factory automation and automotive connectivity to wearable body sensors and home appliances, the IoT is set to touch every facet of our lives. Our lives will change with networks around us that constantly change and evolve based on our surroundings and inputs from other systems. It will build our lives safer with cars that sense one another to avoid accidents. It will build our lives additional inexperienced with lighting systems that change supported the number of daylight from windows. It will make our lives healthier with wearable that can detect heart attacks and strokes before they happen. There is a protracted road ahead to the IoT.

M2M is associate word form for Machine-to-Machine, the term is related to telecom industry and it refers to the communication between different devices. The connection can be either wired or wireless. The M2M was originated in 1960's once caller ID was being developed. Internet of Things, on the other hand, is a bit different than M2M. IoT is a term which is not concentrated on telecom networks solely. Rather, the IoT specialize in connecting multiple devices and pc applications with one another. Both IoT and M2M talk to some devices being connected and transferring knowledge with one another. However, however the communication is completed is totally different for each, IoT and M2M.

In case of IoT, devices area unit continuously connected to web either victimization wired or wireless web. The property to net is for process knowledge and delivering it through a middle layer that is hosted within the cloud. As explained in above reasons, M2M can be thought as a subset of IoT. M2M is like a line connecting 2 points and is like large network that consists of a lot of M2M network along with other devices and computer systems.
Now that both technologies are discussed and how they are different in working, let's take a look at practical applications of both. M2M is once associate worker uses associate card to unlock a door. When the card is swiped, the detector inside the lock will receive the ID and unlock it if the ID is valid.

IoT is more powerful than that, once implemented; IoT can turn on lights, change the temperature on thermostat and even print out today's appointments for the employee once he has unlocked the door with his Identity Card. For associate autonomous vehicle to control safely and effectively, an accurate and robust localisation system is essential. While there square measure a spread of car localisation techniques in literature, there is a lack of effort in comparing these techniques and identifying their potentials and limitations for autonomous vehicle applications. Hence, this paper evaluates the progressive vehicle localisation techniques and on autonomous vehicles. The analysis starts with discussing the techniques that just use the knowledge obtained from on-board vehicle sensors. It is shown that though some techniques are able to do the accuracy needed for autonomous driving however suffer from the high price of the detectors and additionally sensor performance limitations in different driving scenarios (e.g. cornering, intersections)

II. IOT IMPLEMENTATION FOR ASSET TRACKING

Real-time location systems (RTLS) are used to track and identify the locations of objects. In healthcare applications, RTLS tracks the treatment process securely, and helps to reconfigure the health- care system based on the distribution of available resources. The most important RTLS is the Global Positioning System (GPS), which is a satellite-based navigation system to locate objects under all weather conditions as long as unobstructed lines of sight can be received by four or more satellites. For a healthcare system, a satellite-based positioning system can be used to locate ambulances, patients, doctors, etc. It is noteworthy that the accessibility to the systems like GPS or Beidou System (BDS) of China in an indoor environment is generally poor, because the construction structure hampers the transmission of satellite signals. Since GPS is insufficient to build an effective healthcare system, it is necessary to compensate GPS with local positioning systems (LPSs) to enhance location accuracy. An LPS locates an object based on the measurement of radio signals travelling among the objects and an array of the pre-deployed receivers. The above mentioned short-distance communication technologies are essential to implement LPS. For example, UWB radio has a fine temporal resolution, which enables a receiver to estimate the arrival time accurately. Therefore, UWB is an ideal technology for radio-based high-precision positioning - implemented the UWB localization by Time Difference of Arrival (TDOA). Based on the measured time of arrival (ToA), an "indoor GPS" system has been realized. With the measurement of round trip time of flight, a UWB ranging technique was developed. An indoor GPS system with the Root Mean Squared (RMS) accuracy of 3–5 feet in an open space cargo was also introduced. Other UWB based indoor positioning systems demonstrating good performances are reported in. For the implementation of an indoor positioning system, a combination of high bandwidth wireless communication with a GPS or BDS has provided numerous possibilities in developing smart networks

Sensing technology is pivotal to the acquisition of numerous physiological parameters about a patient, so that a doctor can adequately diagnose the illness and recommend the treatments. Furthermore, new progress of sensing technologies allows a continual data acquisition from patients, facilitating the improvement of treatment outcomes and the reduction of healthcare costs. In this section, some exemplifying devices for data acquisition in the IoT-based healthcare system are discussed, as listed. Pulse oximeter was invented in the early 1970s and it has become one of most widely used instruments for diagnosis. Two health indices that are particularly critical for the emergence service, heart rate and blood oxygen saturation can be reliably obtained by a pulse oximeter. A mote-based pulse oximeter was introduced in. The standard digital signal processing (DSP) technique can be used to calculate heart rate and blood oxygen saturation from the waveforms of light transmission. Motion analysis sensor is a complicated device composed of different sensors. For example, the instruments such as accelerometers, gyroscopes, and surface electrodes for electromyography recording are often used collectively for a motion analysis. A triaxial accelerometer can detect the orientation and movement of each segment of the body, while a gyroscope can measure the angular velocity. A combination of both can thus tell the dynamic pose of a limb accurately. The electrodes of EMG gather the statistical information from action potential (AP) generated by excited muscles. EMG signal has been widely applied in the estimation of muscular fatigue, prediction of muscle contraction, and the identification of motion patterns during clinical rehabilitation. All the acquired data related to health conditions of patients can be converted into the digital form and be transmitted to the network immediately. The applications of wireless sensors have greatly simplified the processes of data acquisition, and have made it feasible for patients to wear portable sensors for a longer period of time without bulky data logger. The rising IoT introduces several new challenges that can't be adequately addressed by today's Cloud and host computing models. Here, we discuss several such fundamental challenges.

2.1. Stringent latency requirements

Many industrial management systems, such as manufacturing systems, smart grids, oil and gas systems, and goods packaging systems, often demand that end-to-end latencies between the sensor and the control node stay within a few milliseconds. Many other IoT applications, such as vehicle-to-vehicle communications, vehicle-to-roadside communications, drone flight control applications, virtual reality applications, gaming applications, and real-time financial trading applications, may require latencies below a few tens of milliseconds. These needs fall way outside what thought Cloud services can do.

2.2. Network bandwidth constraints

The speedily growing variety of connected things is making knowledge at an exponential rate. A connected automotive, for example, can create tens of megabytes of data per second. This will include data about the car's mobility such as its routes and speeds; the car's operating conditions such as the wear and tear on its components, the car's surrounding environment such as road and weather conditions, and videos recorded by the car's safety cameras. An autonomous vehicle can generate even a lot of knowledge, which was estimated to be about one gigabyte per second. The North American nation good grid is anticipated to come up with one thousand petabytes of information annually. Sending all the info to the Cloud would force prohibitively high network information measure. It is often unnecessary or sometimes prohibited due to regulations and data privacy concerns. ABI analysis estimates that ninetieth of the info generated by the endpoints are keep and processed regionally instead of within the Cloud.

2.3. Resource-constrained devices

Many IoT devices will have severely limited resources. Examples include sensors, data collectors, actuators, controllers, surveillance cameras, cars, trains, drones, and medical devices embedded in patients. Many resource-constrained devices won't be ready to believe only on their own restricted resources to meet all their computing desires. Requiring all of them to act directly with the Cloud are costly in addition, as a result of such interactions usually need resource-intensive process and complicated protocols. For example, the multitude of microcomputers on a contemporary vehicle would like microcode updates, however requiring every of those resource-constrained devices to perform the serious cryptanalytic operations and complex procedures required to obtain firmware updates from Cloud services will be impractical.

2.4. Cyber-physical systems

As a lot of cyber-physical systems square measure connected to the IoT, the setup between the "brick" versus the "click" is getting down to swing back toward the "brick" once more, wherever interactions, and often times shut integrations, between cyber systems and physical systems have become progressively vital and produce new business priorities and operational necessities. Examples of cyber-physical systems embrace industrial management systems, good cities, and connected cars and trains. In such systems, uninterrupted and safe operation is usually the highest priority. Taking a system offline for any reason will cause important business loss or intolerable client inconvenience, and thus should be planned days, weeks, and even months earlier in some cases . For example, requiring cars to be brought to repair shops just to install software update packages can cause intolerable inconvenience and result in heavy cost to both car owners and carmakers. A reactor usually runs on 18-month cycles and any period will cause tens of thousands of bucks. Many alternative industrial management or producing systems, such as car assembly plants and electrical power generators in the energy grids, have similar requirements for uninterrupted safe operations and require weeks to months lead times to set up for system down times. Many time-critical management applications, which need to be updated over time, cannot be moved to the Cloud due to delay, bandwidth, or other constraints. Therefore, a brand new computing and networking design are required to cut back the requirements for the hardware and software system in mission-critical systems to be updated over time.

2.5. Uninterrupted services with intermittent connectivity to the Cloud

Cloud services can have problem providing uninterrupted services to devices and systems that have intermittent network property to the Cloud. Such devices include vehicles, drones, and oil rigs. For example, AN oil rig within the ocean and much off from shore could have solely satellite communication channels to attach to the Cloud. These satellite channels will suffer wide unsteady quality and intermittent accessibility. However, applications like knowledge assortment, data analytics, and controls for the oil rig have to be available even when the rig does not have network connectivity with the Cloud. As another example, once an automotive traverses a region wherever it loses web property, several services and applications for the devices and other people within the automotive should still be on the market. When an automotive breaks down in such a region and wishes to own one among its electronic management unit (ECU) replaced before it will run once more, the new European should be authenticated to prevent any unauthorized and potentially malware-infected ECUs from being installed on the vehicle. However, Cloud-based authentication services will not be available in this scenario.

2.6. New security challenges

Existing cyber security solutions for today's web, designed primarily for protecting enterprise networks, data centers, and consumer electronics, have focused on providing perimeter-based protections. In particular, a system or an individual device under protection is placed behind firewalls that work with intrusion detection and prevention systems to prevent security threats from breaking through the protected perimeters. Some resource-intensive security functions also are being emotional to the Cloud. Existing Cloud-based security services still target providing perimeter-based protection, such as redirecting email and web traffic to the Clouds for threat detection, and redirecting access control requests to the Clouds for authentication and authorization processing. This existing security paradigm cannot be adequate for addressing several new security challenges within the rising IoT. Here, we discuss several such challenges.

2.7. Keeping security credentials and software up to date on a large number of devices

As the variety and type of the connected devices increase, a growing challenge will be how to manage the security credentials on these devices and how to keep the security credentials and security software on the devices up to date. Requiring every device to connect to the Cloud to update its security credentials and software will be impractical.

2.8. Protecting resource-constrained devices

Many resource-constrained devices within the IoT won't have sufficient resources to shield themselves adequately. These devices may have very long lifespans, and the hardware and software on them can be impractical to upgrade. Yet, these devices can get to stay secure over their long lifespans. For example, replacing any hardware on cars, which have already been sold to consumers, can create significant inconvenience to vehicle owners and result in heavy costs and reputation damages to carmakers. However, over a car's long lifespan that averages about 11.4 years, security threats will become significantly more advanced, many new threats will appear, and the mechanisms required to combat the growing threats will need to be enhanced and upgraded accordingly. Therefore, a basic question arises: a way to defend a really sizable amount of resource-constrained devices from security attacks?

IoT will support many large distributed systems. A connected transit, as an example, might have thousands of devices deployed throughout a town to regulate traffic signals and communicate with vehicles. A giant car maker can have to be compelled to make sure the security of tens of numerous cars on the road in a very large country like the USA. An oil and utility may have to interconnect many remote sites like oil rigs, exploration sites, refineries, and pipelines. A smart grid can incorporates networked subsystems for metering, data collection, data aggregation, energy distribution, and demand response in multiple geographical areas.

Therefore, the flexibility to inform, in a trustworthy manner, whether a large number of distributed devices and systems are operating securely, will be essential. However, standard approaches have problem meeting each the measurability and therefore the trustworthy observation needs at identical time. Today's security health observation systems have faith in grouping security standing messages and log information from devices. Adversaries also can simply use these compromised devices to make a neighbourhood majority in several IoT situations. For example, they may compromise the majority of the smart meters in a house, a building, or even an entire region. As a result, existing mechanisms for detecting false information, which typically rely on the majority of the data sources to be honest (i.e., uncompromised and not malfunctioning), will no longer be adequate. Attackers will compromise a cyber-physical system and injury the physical instrumentation whereas keeping the messages to and from the system seem traditional. A prime example is the attack on the Iranian nuclear facility - the worm attack by sending normal status messages to the system administers while spinning the nuclear reactor out of control.

To increase the trustworthiness of security status monitoring, remote attestation mechanisms allow a device to cryptographically prove its trustworthiness to a remote verifier. A device makes a claim concerning bound properties of its hardware, software, or runtime atmosphere to the admirer and uses its security credentials (e.g., a hardware-based root of trust and public key certificates) to vouch for these properties. The verifier then cryptographically verifies these claims.

However, existing remote attestation strategies have centred on a personal device to attest to its own trustiness. Many resource-constrained devices within the IoT won't be ready to support processing-intensive remote attestation. Even when they can, forcing a large number of devices to perform remote attestation can result in prohibitively high cost and management complexity.

Today's incident response solutions trust predominately on brute force mechanisms like motility down a doubtless compromised system, reinstalling and rebooting its software, or replacing its components and subsystems. Such extremely troubled responses, which largely disregard how severe the compromises actually are, can cause intolerable disruptions to mission-critical systems. For example: an electrical power generator is also infected by a malware that just seeks to steal power for unauthorized use. Shutting down the power generator could cause severe disruptions to the smart grid and excessive power outages.

Industrial management systems typically have very little tolerance for down time. Manufacturing operations can also have critical safety implications. This means that hardware and code updates will solely be put in throughout a system's regular down times, which have to be short and far between, rather than every time any security compromise is detected. A connected car can be infected by malware that can become active while the car is in motion. While the malware can do a range of damages to the vehicle and can put the driver and passengers in harm's way, abruptly shutting down the engine each time any malware is detected could be an even quicker and surer way to cause deadly traffic accidents.

A server in a data center may be infected by a spyware that seeks to steal commercial secrets. While allowing such a compromised server to continue to operate could give the attacker access to some sensitive data, it may not directly impact the data-centre's mission-critical services. If we shut down the server, or halt the execution of the malware-infected files to wait for the malware to be removed, the system downtime could cause significantly more damage, including causing vast economic losses to the data center operator, business disruptions to those who count on the data centers to operate their businesses, and inconvenience to other users of the data center. Therefore, today's extremely troubled incident response paradigm can now not be adequate for securing the various mission-critical systems within the rising IoT.

III. RESULTS & CONCLUSION

A customer is on boarded post analysis of their business requirements. Once the customer profile is ready their assets are boarded. According to the customer needs relevant IoT devices and needful sensors are on boarded. Assets are further mapped with relevant devices so that they can be tracked. On successful mapping the customer assets can be tracked and monitored live.

Customers can get dashboards customized to their requirements for tracking and managing their on-field assets which may be fixed or mobile. Customized graphs of sensor monitoring data are made available according to the range needed by the customer. A customer mobile asset's trip can be geo-fenced to prevent unplanned travel or even theft or tampering of the asset.

Consumers have already got connected things like thermostats, energy meters, lighting management systems, music streaming and management systems, remote video streaming boxes, pool systems, and irrigation systems with additional to come back. Most of these systems have some connectivity through a Web site so that a user can manage them through a standard Web browser or a smartphone app. While each the commercial and client situations are exciting, deployment is not simplified since they are all disparate vertical systems. The systems might use the precise same protocols and OS underpinnings, but the communications layers are inconsistent. Each conjointly uses open application programming interfaces (APIs) while not a horizontal affiliation, which would lead to easier cross-application integration.

Take for example a sprinkler control system. It will have tier of intelligence thus it is aware of once to water supported sensors and net weather information beneath programmable management. However, it doesn't recognize something concerning motion sensors around a house which may indicate a reason to delay the zone to avoid wetting the dog or youngsters. There are no motion sensor inputs on the sprinkler controller, so other motion control vertical integration needs to be used to transfer data to another cloud server. Then the 2 cloud servers ought to be "glued" along somehow. However, hope isn't an honest word in electronic systems. An additional vertical application written in Perl, Python, PHP or another programing language on a server will program an affiliation that enables motion to delay the mechanical device zone (or other logic the user may want). This is not easy unless someone is an expert and therefore will not lead to rapid deployment.

The IoT is a subject of increased interest and enthusiasm, and much of it is warranted. Connected devices and products offer new possibilities for everything from pre-emptive maintenance to new services and business models. The IoT is not a homogeneous concept or paradigm, but rather a buffet of possibilities from which each actor can peruse and assemble an approach that is right for their strategic interests and business requirements. In this article, we draw upon existing research as well as observations from the field and present a number of fundamental questions that each and every actor looking to implement the IoT needs to address before making any decisions or investing a single cent. The results of the collaborative venture demonstrate that a financially sustainable solution needs to have the full support of all participants in order to enable the right preconditions for value creation. Although unique skill sets are part of the rationale behind business ecosystems, these in and of themselves are not sufficient. Unless complemented by suitable forms of communication, coordination, and trust between parties, disparate skill sets are just as likely to create confusion and conflict as they are to yield synergies. In order to prepare for what is coming, managers need to consider their digital strategy in relation to their own business and the ecosystem of partners, as well as emerging technology.

IV. FUTURE SCOPE

The hotel where someone has a reservation knows the person is coming and the approximate time of his arrival because that person has allowed Apple and Google to track my location. It also knows that the person is hot and sweaty from my trip because of the temperature and moisture sensors that are part of my smart watch. The hotel room he will stay in is currently dormant (no lights, drapes closed, the temperature is at optimized dormant levels). He opens my door and the car adjusts the seat because it detects the valet. My preference is to carry my own bag, so he is not accosted by the bell captain. Once in proximity of the edifice lobby, a secure key app is available on my smartphone. By the time he reaches the elevator, the room temp has adjusted to coincide with my smart watch sensors. The room ambience is set to my choice. Because he is hot and sweaty the room also prepares hot water for a shower he will probably take after entering into the room. As he approaches, the secure key app unlocks the room door. Once I fall asleep – the rooms switches to sleep preferences of light and temperature.

In this situation, every room in this particular hotel chain has multiple sensors and actuators. Every rental car has multiple sensors and actuators. He is wearing multiple sensors and actuators, like a watch vibration for alerts. He is not interacting with my smartphone touchscreen constantly to direct these connected things to take actions even though it is one gateway for my activity. There will be millions of people doing this every day.
This vision of IoT will not happen right away. The scale needed can solely be achieved by making a lowest common divisor, simple messaging scheme that everyone on the planet will agree to. It will have to be digitally organic, imitating nature.

At present, technology protocols and information structures area unit restricted by their style quality moreover as security, extensibility, and much more. Our connected devices can need to become easier to use even if the quality of the devices can increase. The line between analog and digital will blur. Every person on the earth is able to “author” his or her own life setting, even though they know basically nothing about the underlying technology. Manufacturers have been connecting things to the Internet since the World Wide Web days. Current IoT device makers are desegregation Internet-connected systems into high-value plus following, alarm systems, fleet management and the like for more than 15 years. These IoT systems area units difficult to create even if some area unit supported trade normal protocols. However, it's getting easier to integrate M2M systems as further powerful processors unit incorporated into the tip nodes. And since these processors support high-level operating systems and languages, the platform can leverage intelligent frameworks. These systems are typically tied into high-end business service layers and are managed by a network operations centre (NOC).

While these business cases are designed to record quite simple data, a lot can be modified in this in order to automate processes; for example, replacing sensors with actuators, using digital fingers, etc. The Internet of Things (IoT) is a revolution that can conquer the future of computing and communication.

REFERENCES

[1] Sayidul Morsalin, Khizir Mahmud, Graham E. Town, “Scalability of Vehicular M2M Communications in a 4G Cellular Network”, IEEE Transactions on Intelligent Transport Systems, 2017
[2] Yasir Mehmood, Koojana Kuladinithi, Anna Fo¨rster, Carmelita Go¨rg, Safdar Nawaz Khan Marwat, Yasir Zaki, Andreas Timm-Giel, “M2M Potentials in logistics and transportation industry”, Springer Dynamics in Logistics: Digital Technologies and Related Management Methods, 2016
[3] In Lee, Kyoochun Lee, “The Internet of Things (IoT): Applications, investments & challenges for enterprises”, Elsiever, 2015
[4] Nallapaneni Manoj Kumar, Archana Dash, “The Internet of Things: An Opportunity for Transportation and Logistics”, IEEE International Conference on Inventive Computing and Informatics, 2017
[5] Mohammad Abdur Razzaque, Teesside University, Marija Milojevic-Jevric, "Middleware for Internet of Things: A Survey", IEEE Internet of Things Journal, 2016
[6] Yuehong YIN , Yan Zeng , Xing Chen, Yuanjie Fan, “The internet of things in healthcare: An overview”, Elsevier Journal of Industrial Information Integration, 2016
[7] DongBum Seo, You-Boo Jeon, Song-Hee Lee, Keun-Ho Lee, “Cloud computing for ubiquitous computing on M2M and IoT environment mobile application”, Springer Science and Business Media New York, 2016
[8] Rahul B. Pendor, P. P. Tasgaonkar, “An IoT Framework for Intelligent vehicle monitoring System”, IEEE International Conference on Communication and Signal Processing, 2016
[9] Jie Lin, Wei Yun, Nan Zhang, Hanlin Zhang, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications”, IEEE Internet of Things Journal, 2017
[10] Mohammad Abdur Razzaque, Marija Milojevic-Jevric, Andrei Palade, Siobhán Clarke, “Middleware for Internet of Things: A Survey”, IEEE Internet of Things Journal, 2016