ANALYSIS OF IOT DESIGN AND TECHNOLOGY

[1] S.Hendry Leo Kanickam, [2] A.Preethijeralinhilda,
[1]Assistant Professor, [2]Student,
[1] Department of Information Technology,
[1] St.Joseph's College, Trichy, Tamilnadu, India

Abstract: The "Internet of Things" vision promotes the integration of smart devices into web applications, using newly technologies and protocols as underlying interaction mechanisms with smart devices without permissions. Technically many phones include various sensors and provide a large-scale sensing platform using into non sense able data nodes. To make this functionality available to a hug users of the web platform developers our research aims at easing the creation of issues applications that use mobile context data (e.g., vibrations ported communications). We present this paper using a sensing platform for sensor devices, called BREACH OF PRIVACY, which gathers and stores available information on a cloud platform and makes this information directly accessible via mobile services - locally and remotely used to end user. By using a concept of unpredictable sensing nodes , the platform supports the full development process, from the initial idea via adapting/extending the platform to incremental development of sensors networks and applications via Web portals controls. Hence, (web) developers can create arbitrary context-aware applications that make use of mobile hardware capabilities without touching mobile phone programming at all. In this paper we discuss the design issues and provide case studies to describe how this platform can empower the development of social networks, context-aware application.

IndexTerms **- Internet of things – challenges ports of IoT – mobile – web – context – web.**

I. INTRODUCTION

The Internet of Things marketplace is moving fast, with remarkable innovations becoming business as usual. To keep up, you may want to consider one of this year's IoT conferences. Not sure where to put your conference dollars? Here's a comprehensive guide to the best IoT events in 2018.Staying on top of technology trends within the sphere of the Internet of Things (IoT) is an ongoing challenge, given the industry's rapid-fire changes and how those changes affect other areas of IT. Topping the list this year in hot IoT topics are high-performance computing, edge computing, advanced analytics, machine learning, artificial intelligence, cloud computing, smart homes, and smart cities.The best technology conferences both teach the tools, processes, and tactics in use today and explore emerging IoT-related technologies. However, not all conferences are created equal. Some fall flat in content, and others are geared to specific use cases such as consumer IoT, smart cities, or health tech.

Fig -1 IoT classification

We're here to help you sort through which 2018 IoT conferences are worth your time and money. They are handily categorized as must attend, worth attending, or worthy mentions, although your individual mileage may differ. Each section is presented in chronological order. If a conference is aimed at a specific audience or industry vertical, it is noted in the description.

II. INTERNET OF THINGS

In general a real time application running in a web applications can be modeled as a directed communications for consisting of streaming the data and stream processing job tasks. Stream tasks are at the applications of the graph and streams are the edges connecting the devices. A stream is an unbounded sequence of events flowing through the edges mobile devices of the web port and each such event consists of data represented in some format frequency sensing data. We envision a middleware and online platform that provides reusable sensors, context, and activity information from a single phone as well as from a set of phones.. A distributed stream processing framework provides the necessary API and infrastructure to develop and execute such applications in a cluster of computation nodes. With the increasing pervasion of smart phones there is a clear trend towards continual mobile usage. Users set and share status updates explicitly and manually on their phones with others. However, sensors on these mobile devices allow implicit and automated communications, e.g., location and activity can be determined from the phone's sensors and be provided to friends via SNS.

2.1 Definition

In the next upcoming years , planet earth will don an electronic skin. It will use the Internet as a scaffold to support and transmit its sensations. This skin is already being stitched together. It consists of millions of embedded electronic measuring devices: thermostats, pressure gauges, pollution detectors, cameras, microphones, glucose sensors, EKGs, electroencephalographs. These will probe and monitor cities and endangered species, the atmosphere, our ships, highways and fleets of trucks, our conversations.

2.2 How IOT works

For Example Smart Home technology is the future of residential related technology which is designed to deliver and distribute number of services inside and outside the house via networked devices in which all the different applications & the intelligence behind them are integrated and interconnected to the devices. These smart devices have the potential to share information with each other given the permanent availability to access the WiFi internet connection. Hence, Smart port Technology has become part of IoT (Internet of Things). In this work, a home model is analyzed to demonstrate an energy efficient IoT based smart home. Several Multi level simulations were carried out focusing on the kitchen of the home model. A motion sensor with a surveillance camera was used as part of the home security system.

Coupled with the home light and sensor control systems, the smart system can remotely control the lighting and heating or cooling when an occupant enters or leaves the kitchen moving the sensing cloud platform used in data centers .

2.3 Analysis of Drawbacks of IOT

Overcoming the drawbacks of sensors UHF radio frequency identification (RFID) a shift of the backscatter communication principle use to mm-wave frequencies is desirable. With the significant reduction of the transponder data and wider communication bandwidth, many new applications become possible to accessing security issues. Demonstrating the feasibility, we implemented a fully functional hardware system in the bounding ported . Both, the base station and spectrum analysis for communications models the transponder are investigated and their performance is presented in a system applications.

2.4 Research plan for Robust Open Sources IoT

QoS demands it as for example when monitoring shows that applications initial task is devices. This as-needed replication will directly reduce overhead from time cases in many open sources. We will dynamically identify with out collusions tasks that require research planning at the task level rather than at the streaming application level. This dynamic replication of data tasks will be implemented for Gateway Storm described above.

2.5 Raspberry on IoT

Security in data transmission is one of their biggest problems. the evaluation of VPN QoS parameters over a Wireless Network (WLAN), using different Raspberry Pi models. Additionally, we analyzed the QoS parameters with different traffic conditions and the CPU consumption in the VPN

Fig-2 Raspberry on IoT architecture

III. NEW THINKS OF IOT

3.1 IoT and Big Data

Big data appeared long before the IoT. But the whole concept of the Internet of things is about data gathering and processing. IoT devices are built on the basis of special chips which main purposes are to track users' activity. unidirectional storage devices. The accuracy and through put can be improved with parallel processing elements which are involved in super scalar architectures.

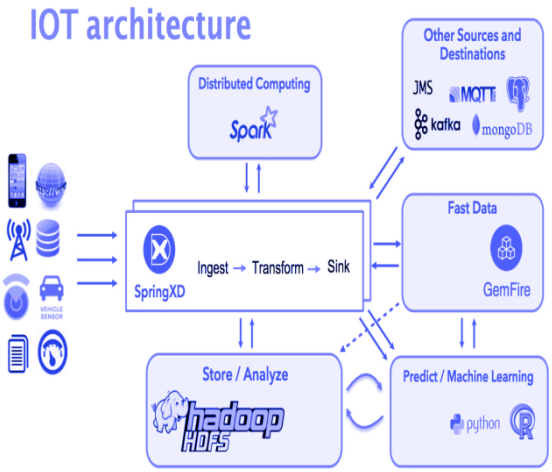

Fig – 3 Iot of big data Architecture

3.1.1 **IoT and machine learning**

As IoT devices collect so much data why not to use it to teach the system? IoT boost brings more and more devices into our lives, and as a result machine to machine, communication has to become more and more advanced. Machine learning is needed to make better predictions about the outcome of different situations. **It is a matter of life and death** if we apply it to medicine or road traffic safety. Usual analytics are static,

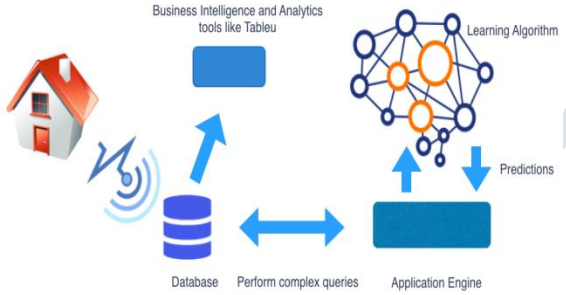

Fig – 4 Machine Leaning neural Networks

whereas Machine Learning algorithms constantly improve. The ability of IoT devices to interact with other appliances makes it even easier because of training one, you train them all. This fantastic **ability of IoT devices to get smarter** over time is extremely useful for businesses. The system is able to detect minimal deviations from the norm long before a human eye could detect them. For some companies that use expensive equipment, which breakages lead to millions in expenses, precise maintenance prediction means huge cost savings.

3.1.2 IoT and Blockchain

Because data gathering is so essential in IoT work, it means that this data has to be protected throughout its life cycle. Data management under all these conditions is a very difficult task as it will flow across many boundaries with different policies. This complexity shows all the challenges to keep IoT protected.

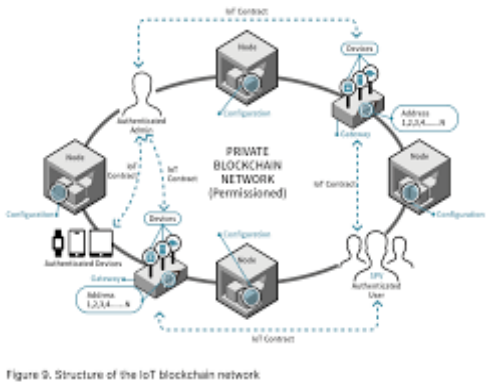

Fig – 5 IoT of Block chain

3.2 IoT platform Technology

Interoperability between IoT devices, and making easily use of IoT devices. The proposed platform technology provides semantic-based IoT information services, and semantic interoperability of IoT devices. This service platform can be applicable to a lot of semantic IoT services: collecting invisible information in real environment by smart devices, providing smart life services by sharing, participating, distributing open sensing information .

3.3 Territory IoT monitoring

IoT devices can do lots of tasks. They can measure the soil humidity and control the water supply. They can control how ripe fruit and vegetable are and inform the farmer about harvesting time and so on. Smart approaches reduce costs and advances forecasts, planning and harvesting processes.

Infrared cameras and air filters can save our forests in summer time. These appliances are commonly used in countries where this problem is not an empty phrase. If we combine and improve weather forecast systems with these sensors we can do the same.

3.4 Deployment of IoT Wireless Conversions

Wireless energy transfer technologies have played an important role in the development of Internet of Things (IoTs). Most of previous studies focus on scheduling mobile chargers efficiently for rechargeable sensor nodes. In this concepts, we consider optimizing the deployment for Wireless Charging Stations (WCSs) in urban area. We respect the users detouring cost, when they need move to the candidate WCSs. Given a number of WCSs and users trajectories, we aim at optimizing the WCSs deployment to maximize the number of users for recharging with guaranteed probability. We convert our deployment problem into the weighted maximum coverage problem, which has been proved to be NP-hard.

3.5 Smart Controllers Urban Areas

The developed the structure and described work algorithm of data collection controller automated processing systems for Data traffic of the “smart” city public transport survey the ported into Smart controllers, built and examined the controller model, based on Petri networks, which allowed to develop recommendations concerning technical means choice for implementation automated processing systems for passenger traffic of “smart” city public transport..

Advantages of Iot Technology :

IoT is tagging our day-to-day objects with machine-readable identification tags. Sensors may be a couple with these tags to collect more information about the condition the everyday objects and those present around them. The time is not that far when you are out of home and your computers at home contact you to let you know that your medicines have expired or that the milk is over or you need more pepper. This isn’t just a fantasy but soon to be a reality due to the amazing possibilities of the Internet of Things (IoT).

Data : The more the information, the easier it is to make the right decision. Knowing what to get from the grocery while you are out, without having to check on your own, not only saves time but is convenient.

Tracking: The computers keep a track both on the quality and the viability of things at home. Knowing the expiration date of products before one consumes.

Figure - 6 : IoT Round Of year Productivity Improvements

Time : The amount of time saved in monitoring and the number of trips done otherwise would be tremendous.

Money : The financial aspect is the best advantage. This technology could replace humans who are in charge of monitoring and maintaining supplies.

Drawback of IoT issues :

Compatibility : As of now, there is no standard for tagging and monitoring with sensors. A uniform concept like the USB or Bluetooth is required which should not be that difficult to do.

Complexity : There are several opportunities for failure with complex systems. For example, both you and your spouse may receive messages that the milk is over and both of you may end up buying the same. That leaves you with double the quantity required. Or there is a software bug causing the printer to order ink multiple times when it requires a single cartridge.

Privacy/Security : Privacy is a big issue with IoT. All the data must be encrypted so that data about your financial status or how much milk you consume isn't common knowledge at the work place or with your friend.

Safety : There is a chance that the software can be hacked and your personal information misused. The possibilities are endless. Your prescription being changed or your account details being hacked could

put you at risk. Hence, all the safety risks become the consumer's responsibility

IV. Issues of IoT data Sciences

The realization of IoT systems will enable seamless integration of the cyber world with our physical world and will fundamentally change and empower human interaction with the world. A key technology in the realization of IoT systems is middleware, which is usually described as a software system designed to be the intermediary between IoT devices and applications. In this concepts , we first motivate the need for an IoT middleware via an IoT application designed for real-time prediction of blood alcohol content using smart watch sensor data. This is then followed by a survey on the capabilities of the existing IoT middleware. We further conduct a thorough analysis of the challenges and the enabling technologies in developing an IoT middleware that embraces the heterogeneity of IoT devices and also supports the essential ingredients of composition, adaptability, and security aspects of an IoT system.

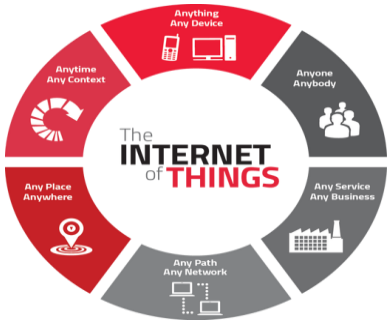

Fig -7 Places issues of IoT in the world

4.1 Automated Tools Of IoT

- Communication: IoT system increases and encourages machine to machine communication (also known as M2M). Because of this ingenious innovation, physical devices stay in touch with one another leading to greater efficiency and higher quality. It also allows full transparency.
- Automated: Due to the overall wireless infrastructure of these smart devices, it requires little to no human intervention, being able to pretty much operate on their own. This allows for greater control and automation leading to more operating efficiency.

- Information: IoT systems have allowed a greater flow of information which in turn allows people to make better decisions. It can be as simple as Siri informing you that you are out of groceries to more complicated decisions at work. As people say knowledge is power! The systematic use of information also allows you to save time and work in an effective manner.
- Money: IoT systems thrive on efficiency thus, when machines communicate with each other, not only does it save time but also money and resources. For instance your oven or kitchen electronic gadgets now have the ability to turn off themselves once the work is done. This makes the IoT system more environmental friendly as the system operates on minimum resources. Another way which this system saves money as it immediately informs its owner of any breakdowns or other technical problems with the system or anything else in the work or home environment. Hence, this immediate correspondence helps save time and money.
- Comfort: We live in a century where people have such hectic schedules that they just don't have the time to worry about small things. Hence this is where the IoT system comes in; greater convenience, comfort, time management and overall a better standard of living.
- Use of IoT in different systems: Using IoT in systems such as healthcare or security can generate excellent results. For instance, by implementing chips in patients, doctors can monitor their patient's vital signs and respond immediately in case of an emergency. Moreover, it can increase monitoring patients at homes, allowing for more free space in hospitals for serious cases. In case of security, police can use the IoT system to monitor the street cameras and improve the law and order system.

IoT systems in businesses: IoT systems would prove to be extremely advantageous for businesses; it would allow them to monitor consumer trends and respond to the demand changes in a timely manner. This could lead to greater sales which lead to greater profits and revenues.

4.2 Devices and portable uses

IoT stands for internet of things. IoT is a network of all physical, tangible items such as devices, cars, buildings and anything that has software or sensors in them which allow us to automate everything. In this day and age IoT play a huge role in our lives as most of our daily activities involve the use of internet and collecting or exchanging data. The main aim of IoT is to automate our lives which could make it more efficient but at the same time could lead to some major privacy issues. Every day we see new gadgets and innovations in the market; with just a command we can control all our gadgets and other electronics at home without having to get up and physically turn on and off things. The use of word 'smart' has become something of a brand name where you have smart phones, smart TVs, smart washing machines and in essence now you can have smart homes.

4.3 IoT device used for air pollution

One of that priorities is to improve cycling habit within the society. This project was intended to motivate people to do more cycling by creating awareness about air pollution issues. The utilization of Internet of Things (IoT devices), secondary data analysis and physical data visualization were methodology approaches used in this project. This paper explains workflow of the project, including data collection and analysis, participatory design workshop, field measurement and physical data visualization. Based on the analysis of data in this research, a series of physical installation was deployed as the outcome of this research.

4.4 Energy efficient green-IoT network

especially sensor devices are mostly deployed in an extremely resource constrained environment and thus pose the necessity to extend the capability and life expectancy of these kind of devices in terms of energy consumption. Since, the devices in IoT have limited energy sources they often run on battery with a certain energy capability, the deployment of green communication and system model in IoT has been a core challenging issue. addresses the energy efficiency issues across diverse IoT driven networks by proposing a system model for G-IoT and energy efficient scheme for the IoT devices to extend the life expectancy of the whole IoT network.

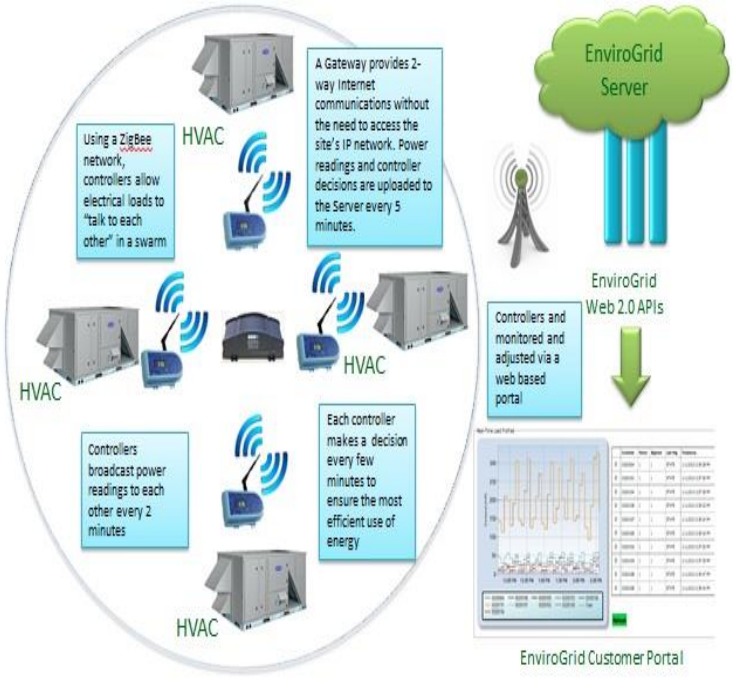

Fig -8 Energy Efficiency in IoT

VI. FUTURE WORK

We propose a novel security method for security modeling and analysis of such environments. This method aims to support the development of secure IIoT environments at the modelling and simulation level. As future work, we plan to examine the applicability of our proposed security analysis method to other complex environments, such as connected cars and homes, and wearable devices. This will allow us to understand in depth the challenges that these environments face, the peculiarities that have to be addressed, in order to protect the exchanged information of the distributed devices and the service provision of all relevant actors, limiting the number of incidents that can affect negatively the entire IIoT environment. We also aim to extend our work by including privacy requirements during the modeling and the analysis of such systems. Through this extension we will be able to preserve privacy on users' data and identify the critical paths
that might have impact on users' privacy requirements, such as anonymity, unlink ability, un observability, un detectability, and so on. Finally, we plan to enhance the simulation level with game theoretic approaches, so we can better identify mitigation techniques for the identified attack paths.

References

[1] Statista. (2017) Internet of things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). [Online]. Available: https://www.statista.com/statistics/471264/
iot-number-of-connected-devices-worldwide/

[2] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–
2243, 2014.

[3] A. Jacobsson, M. Boldt, and B. Carlsson, "On the risk exposure of smart home automation systems," in Future Internet of Things and Cloud (FiCloud), 2014 International Conference on. IEEE, 2014, pp. 183–190.

[4] V. Mookerjee, R. Mookerjee, A. Bensoussan, and W. T. Yue, "When hackers talk: Managing information security under variable attack rates
and knowledge dissemination," Information Systems Research, vol. 22, no. 3, pp. 606–623, 2011.

[5] R. H. Weber, "Internet of things–new security and privacy challenges," Computer law & security review, vol. 26, no. 1, pp. 23–30, 2010.

[6] A. Cui and S. J. Stolfo, "A quantitative analysis of the insecurity of embedded network devices: results of a wide-area scan," in Proceedings
of the 26th Annual Computer Security Applications Conference. ACM,
2010, pp. 97–106.

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

[8] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in Design Automation Conference
(DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015, pp. 1–6.

[9] C. Alcaraz, R. Roman, P. Najera, and J. Lopez, "Security of industrial sensor network-based remote substations in the context of the internet of
things," Ad Hoc Networks, vol. 11, no. 3, pp. 1091–1104, 2013.

[10] A. N. Duc, R. Jabangwe, P. Paul, and P. Abrahamsson, "Security challenges in iot development: a software engineering perspective," in
Proceedings of the XP2017 Scientific Workshops. ACM, 2017, p. 11.

[11] M. S. Moganedi and J. S. Mtshweni, "Beyond the convenience of the internet of things: Security and privacy concerns," 2017.

[12] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and
privacy issues," International Journal of Computer Applications, vol. 90,
no. 11, 2014.

Mr.S.Hendry Leo Kanickam working as a Assistant Professor in Department of Information Technology , St.Joseph's College(autonomous) Trichy, India. He received his M.Phil Degree in Bharathidasan University in 2008 and also He is pursuing Ph.D (Computer Science) in Bharathidasan University.

Ms.A.Preethijeralinhilda is studying II M.Sc Computer Science in the Department of Information Technology ,St. Joseph's College (autonomous) Trichy, India