**7th Feb 2022**

**CSCI 594 GRADUATE SEMINAR**

SHUBHAM DESHMUKH

(202006307 – x2020gfv)

**A RESEARCH REPORT ON:**

**INTERNET OF THINGS**

INSTRUCTED BY: DR. IKER GONDRA

DEPARTMENT OF COMPUTER SCIENCE

**St. FRANCIS XAVIER UNIVERSITY**

**Abstract**

Internet of things or IoT can be described as a network of multiple physical devices (embedded with sensors, power, and processing power) running on the same or different network which may or may not be connected to the internet [3][26]. It is also popularly known as IoT and are mostly portable small-sized devices doing a minimal but continuous fixed set of operations. The devices at their early stages were mostly wired but now it's mostly wireless because of the technological advancements but this has posed so many challenges like power, connectivity, etc. This paper will discuss some of the prominent solutions to these challenges, the existing solutions, and architecture.

1. **Introduction**

Internet of things (IoT) has seen massive expansion around the globe. The rise of the internet, computers and the global reach of technology has made this possible. IoT has become a separate vertical in the IT industry and has now been applied in every industry, now the consumer market the also increasing exponentially in fact it predicted that there will be around 1.1 billion wearable devices in the world by 2022 from 325 million in 2016 [1]. The IoT industry has been growing at an exponential rate and is expected to grow even more to about 75 billion connected devices by 2025 [2], however, one thing that remains common in the devices over the years are the constraints or problem faced by the devices or the IoT endpoints. The solutions have been better now than five years back however the problems still exist which are some major research points in the industry. IoT devices are more data/purpose-driven industry now and require even more precision in terms of solutions. The paper will talk about the existing architecture & working of the IoT devices in different industries and applications and discuss some of the solutions to the existing problems. etc.

Diagram, text

Description automatically generated

Fig 1. A generic architecture of IoT devices and Networks.

1. **Initial Implementations**

The first concept of the smart device came in 1982 when a modified version of the Coca-Cola vending machine was installed in Carnegie Mellon University it was able to identify if the stocks are low and whether the drinks were cold or not. "Internet of Things" as a term was first introduced by Peter T. Lewis at a speech in 1985. Kevin Ashton of Procter & Gamble invented the term "Internet of things" independently in 1999, however, he prefers the phrase "Internet for things" He related radio-frequency identification with the word IoT. According to Cisco Systems, the Internet of Things was born between 2008 and 2009 [3]. By 2013 IoT saw significant innovation and advancement and now had become a system of several technologies coupled together, from wireless communication to consolidated battery packs, from the microprocessor to embedded system, the embedded system also became smaller and smaller. Even the traditional system like home (doorbells, fans, switches), control systems, GPS, smartwatches, bikes, etc. all support and became a part of IoT.

1. **Existing Implications**

IoT devices have been here for almost two decades now, the advancements in the technologies used have upscaled the industry, and also the expectation has largely increased but the problems remain the same, even though the capabilities has increased but the challenges haven’t been solved just yet and the field still eyes so many research work on a topic like Energy harvesting, Security & Privacy, Data-Driven IoT, IoT searching, Service-oriented IoT, Social IoT, Edge Computing and IoT. These are some aspects where the devices and the architecture need improvements.

1. **Energy Harvesting**

The ever-increasing network for IoT devices and networks has resulted in a massively dispersed network of smart things and objects with different parameters like storage, functionalities, and networking. These networked things or IoT devices communicates with each other primarily to share a wide variety of data that has a direct impact on improving the standard of everyday lives by allowing smooth access to smart services wherever and at any time. These devices often are of different shapes and sizes due to different physical constraints. Due to the size and sometimes weight restrictions, the IoT sensors and the embedded systems have a certain life span, most importantly the batteries, since the majority of the IoT devices now run wirelessly the scope for power delivery has been restricted because of the use of a battery. The battery has a certain life span as well and needs to be changed from time to time, which directly impacts the life span of the IoT device because changing the battery from time to time is not possible or extremely expensive and laborious. The devices usually have size constraints so a bigger battery is not usually an option in most cases. One way to increase the overall battery life is to build your device in such a way that its hardware components consume lesser energy, however, that’s not always possible since the hardware components are already so optimized and efficient, making them less energy consumable is a daunting task. Smarter energy management like energy harvesting/ energy scavenging is the only way for IoT devices to be energy efficient.

Energy harvesting is a process that converts easily accessible energy from natural or manmade sources into electrical energy that may be used. Energy harvesting has the ability to considerably extend the total system lifespan. Energy harvesting has four stages i.e., choosing the best and most readily accessible energy source, transforming, storing, and consuming it. [Fig 2.].

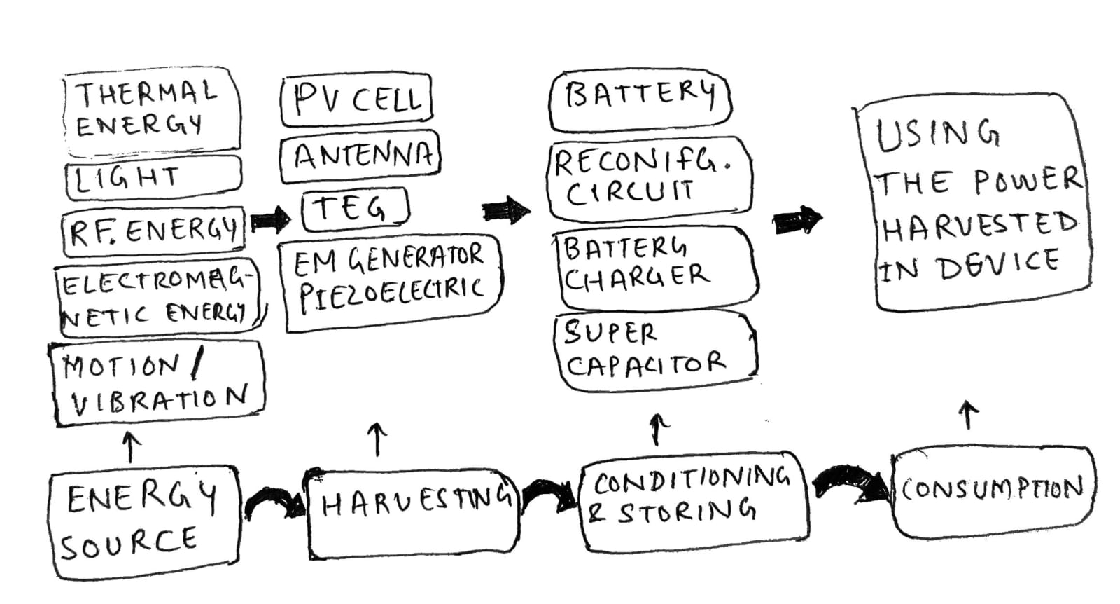


Fig 2. System of Energy Harvesting IoT Device.

The first phase is the transformation phase where the energy from the ambient or natural sources such as thermal energy, electromagnetic energy, light waves, radiofrequency energy are identified. The energy is then transformed into electrical energy using transducers and harvesters like PV cells, Antenna, Electromagnetic generators & piezoelectric, etc. The stage is conditioning and storing the energy in rechargeable batteries, supercapacitors, etc. the final stage is using the energy in the IoT device and application for its functioning. Despite the advanced techniques, there are still underlying challenges that loom over the energy harvesting solution. for example, Because conventional IoT object plans can't handle major differences in an item's hardware because the amount of energy sent to an IoT device is closely related to the availability of energy, which might be inferior to or superior to the power requirements of the item's electronics. As a result, software that is intelligent enough for IoT harvesting systems must be built which can tolerate energy disruptions for a shorter time period, allowing any job to be restarted rather than starting over, preventing loss of data. Lastly, both supercapacitors and rechargeable batteries have intrinsic limitations that make designing a battery that is highly efficient, cost-effective, compact, and long-lasting challenges.

* 1. **Harvesting Energy**

This is the initial and the most important part of the system, Energy harvester is a device that generates electrical power from natural sources like light, Radio Frequency waves, motion, electromagnetic waves, etc. Harvesting energy through the process of photovoltaic from solar energy is the best promising and researched technology of all, in part because of its higher power density than other ambient energy sources. Any device or a system that has substantial access to light can have solar harvesting as its prominent source, there are IoT devices that are mostly outdoors and remote areas with no access to electricity, using a solar harvester in these types of devices can be significantly useful. There are studies in which a photovoltaic cell is integrated into clothing which can give a new rise of smart wearables and consumer IoT devices like smart jackets etc. [6]. Radiofrequency waves are also a potential source of energy for IoT devices, Radio Frequency harvesters convert energy from incoming radio frequency waves. The source of power can be radio frequency signals transmitted from the existing system for transfer of data like the TV remote, etc. or there can be a dedicated power source like wireless charging emitting radiofrequency waves. this technique is already used in RFID systems like ID cards, keys, tracking cards, etc. Although the quantity of gathered electricity is frequently tiny, energy harvesting from Wi-Fi network signals has been demonstrated [8]. Electromagnetic Induction or piezoelectric effect [7] are some of the phenomena which are used for generating electrical energy from motion or vibration (mechanical energy), these types of harvesters are called kinetic energy harvesters, this way of harvesting energy can be useful for smart wearable or devices where the power/energy can be extracted from routine human activities like walking, running or exercising, etc. also it can benefit devices which operate in fast-moving or vibrating conditions like motors or engines which have high vibrating surfaces. Thermoelectric generators turn a temperature difference between two surfaces into an electrical potential. Thermo electrical generators can be used to power the IoT devices that are adjacent to heat sources, like hot water pipes, etc. They may also be used as a power source in wearable IoT devices, such as wearables, where the temperature difference between the ambient source and body surface is used. Finally, every harvesting mechanism depends on the energy constraints, functioning environment, and size of every IoT device.

* 1. **Energy Conditioning and Storing**

The need and requirement of energy conditioning come from the fact that the energy harvest from multiple sources is highly fluctuating which depends on the source of the ambient power supply, however, to avoid the risk of the hardware getting blown up, any IoT device requires a steady direct current voltage supply to work and function correctly. Thereby a proper mechanism is needed to convert the unstable power to a stable and consistent voltage supply before storing it or feeding it to an IoT device’s circuit. The harvester's output power is relatively low, generally only a few megawatts, due to the small/tiny building restriction in mostly all the IoT devices. The conditioning circuit needs to send as much energy to the IoT device as feasible with the least amount of loss, which necessitates careful design. To add up, there are some energy harvesters, such as thermoelectric generators in body-worn devices, that produce merely tens of millivolts at their output. In these situations, a boost regulator with a very low input voltage is necessary. Energy conditioning is vital for boosting harvester's efficiency. The maximum power point on which an energy harvester's power output is maximal is considered the optimal operating point for the harvester. Keeping the MPP tracking, which is referred to as MPP tracking, is imperative since MPPs change dynamically according to ambient conditions. Commercial power conditioning integrated circuits have MPP tracking as a feature. Without a dedicated power conditioning unit, MPP tracking is accomplished by altering the IoT device's average power consumption, some design considerations are mentioned in detail in the papers. [9] [10].

In IoT devices that don't have ambient power, the energy collected using harvesters is unstable and unpredictable, and energy storage elements must be present to ensure uninterrupted operation. A high energy density energy storage element requires a priority, to maximize the IoT device’s span and reduce its size since the storage material or the battery is mostly the heaviest part of an embedded IoT system. Batteries are the most common and most prominent things which are used to store energy in IoT devices like in every other electronic device such as phones, EV cars, etc. However, IoT devices can benefit greatly from solid electrolyte batteries that use solid electrolytes, they are known as solid-state thin-film batteries [11]. Despite its low power density, it has a high energy density, so it can be best used in low-power and long-lasting IoT applications, they are thin and bendable which makes it ideal for using it in size-constrained devices [12]. Manufacturing solid-state batteries as a traditional battery pack or incorporating them into the circuit is possible, incorporating them into the circuit saves even more space, which helps in a significant reduction of the size of the circuit and the integration cost of the circuit. Supercapacitors have a substantially greater cycle efficiency and a lot longer cycle life than batteries. They do, however, need power conditioning equipment that can handle their huge voltage variations, particularly the very low voltage during cold boot. which can make the device costly as well. the use of dynamic reconfiguration of numerous supercapacitors can help to alleviate the problem. Improve cold boot speed by addressing voltage fluctuation, some details of arranging multiple supercapacitors are mentioned in the paper [13]. Another type of supercapacitor is one that is based on a thin film substrate and is flexible, making it excellent for wearable applications, which have also been enabled by recent breakthroughs in nanotechnology [14].

1. **Security & Privacy**

The proliferation of the IoT industry has eased and helped the way we live however, there is another aspect to it, with the ever-increasing IoT devices, the privacy of the users & data is at stake and posing a threat to the security of the devices. The main challenge of an IoT network has always been the lack of power and energy, which in turn deprive these devices of using high and cryptographic techniques for data encryption and decryption, therefore posing a high range of security threats against it like denial of service (DoS), data sniffing, data stealing and even dysfunction of the device. There has been a never-ending research work going on securing and privacy issues, despite that there is still a long way to go in terms of finding a robust security mechanism for IoT devices and networks, the research work at the current moment doesn’t give solutions to every aspect of the system instead they can come up with a solution for a few needs like authentication, secure routing, confidentiality, etc. a complete security solution is yet to be proposed which gives complete security of the data and minimizes the number of interferences to the network while integrating several solutions. As of now, none of the offered research methodology or industrial solutions provide a secure solution that is free of security attacks. fine-grained accessibility and conditional nameless authentication, The IoT infrastructures and devices will employ resource-constrained control mechanisms. The security of IoT infrastructure faces a variety of issues but is not restricted to DoS, scalable security or data upload, and interoperability. One of the most important requirements for IoT systems is scalability. Such a need can be satisfied by securely outsourcing costly cryptographic computations to a cloud-based system, some of the details of cloud-based IoT are mentioned in detail in the research paper [15]. To overcome the present security concerns of IoT systems, there is a pressing need to investigate clever solutions to combine IoT with cloud and edge computing. Additionally, in IoT security research, cryptographic methods with minimal communication cost, like constant size Attribute Base Encryption approaches, should be studied. Some details about Attribute encryption techniques are mentioned in [16]. Non-repudiation is also required for IoT infrastructure, particularly for systems involving human interaction. To prohibit users from contesting the service's use or previous data uploads, non-repudiation should be enforced. Due to privacy considerations, non-repudiation is not taken into account in the majority of existing implementations. Several approaches, such as conditional anonymity, can ensure the privacy of both users and devices while implementing nonrepudiation, a technique that can provide conditional anonymity can be a group signature but with the very limited research work and resources in the IoT infra, they require high research work for implementation. In addition, with IoT device heterogeneity, interoperability is an important requirement of IoT infrastructure. Creating IoT interoperability standards and backward compatibility requires a great deal of effort and cooperation from government and non-governmental agencies. These standards should also be incorporated into Privacy Management to maintain user privacy. In the IoT world, trust is also a must-discuss subject. As with most present security procedures, do not deal with foreign people's subjective opinions. In the presence of inside infection, IoT objects are particularly vulnerable. Attackers are attempting to undermine the network's trustworthiness. Interactions between IoT devices When it comes to the security and trust paradigm, that is, security and trust, Mechanisms for a barrier, a lock, and an entry form When, where, and why they should be placed in a matter. Overcome the IoT ecosystem's obstacles, locks, and gates. In terms of how well IoT objects work together and integrate. Security based on trust There is now a system in place to boost overall security. IoT based on a trust and reputation paradigm cooperation should be improved, and trustees should be chosen. Service providers are chosen depending on the QoS and IoT based on service-oriented architecture. The relevance of trust management in many types of networks has lately been examined. For extremely dynamic and dispersed networks, reliability assessment is critical. We can't always guarantee a constant infrastructure in certain situations. For public-key cryptography, this is important. Computing trust, on the other hand, has its own set of difficulties. That is, utilizing event/time-driven characteristics depending on the context of a specific application, and trust aggregation purposes by assigning suitable weights to these attributes. Set the appropriate trust criteria and discriminate between nefarious and non-nefarious nodes before deciding whether or not to trust updates. To sum up, developing a resilient IoT network capable of meeting the severe application requirements necessary to fulfill the goal of high-security digital communities demands a combination of security, privacy, and trust.

* 1. **Authentication**

Granting access to authorized persons by recognizing users in a network in non-manipulated equipment is known as authentication. There are some attacks in the IoT system that may have been prevented with authentication, Authentication remains one of the easiest ways to hack a system and get into the application layer of an IoT infrastructure. TSL or Transport layer security along with TSL-PSK, RSA, and DH key exchange is the most common cryptographic methods that are used in IoT. Mutual authentication is expected between the two entities in this approach, they must first justify themselves by communicating secret information (pre-shared key). Because the authentication procedure employs just symmetric key encryption, this approach is suited for constrained devices such as sensors. Asymmetric crypto-based protocols, symmetric crypto-based protocols, and hybrid crypto-based protocols are the three types of authentication protocols currently being researched for IoT [17]. Customers and gadgets in an IoT environment produce mutual communication, therefore there may be mutual communication between the tool and the servers as well. In addition to sending data to the server, the utility will collect, and handle statistics sent through the server. As a result, in an IoT machine, reciprocal authentication is essential to confirm that both the tool and the server are real. lightweight authentication and encryption have seen a rise in have demand in recent times, as they provide controllable and consistent communication. Different techniques to achieve IoT authentication's purpose include multi-element authentication using bio-hashing and anonymity.

* 1. **Encryption**

End-to-end security is ensured by encrypting nodes. However, because IoT systems are heterogeneous, certain nodes may be able to incorporate a general-purpose microprocessor. Only application-specific ICs can be implanted if resources are constrained, and devices are limited. As a result, classical cryptographic primitives are unsuitable for intelligent devices with limited resources, because of some of the constraints with IoT devices’ built. As a result, for these devices, lightweight encryption is a good option. Effective end-to-end communication has been achieved by using IoT encryption while using as little power as possible, symmetric and asymmetric lightweight IoT algorithms have been developed to meet these requirements. In both the physical and network arenas, the focus of research has been on developing low-cost, lightweight encryption. An attribute-based decryption system, on the other hand, is proposed to facilitate user revocation [18].

* 1. **Routing in IoT**

In an IoT network, sensors and actuators are critical components. These gadgets are self-organized and communicate information while being low-powered and resource-restricted. They can also be used to store data and perform calculations at the same time. As a result, every routing system must have scalability, autonomy, and energy efficiency. Because IoT networks are becoming more widespread, IPv6 is the protocol that is used by these devices' for IP addresses. 6LoWPAN allows internet protocol communication across lossy networks while using the least amount of power. There is a chance of security breach if (6LoWPAN) is not present. In an IoT network, sensors and actuators are critical components. These gadgets are self-organized and communicate information while being low-powered and resource-restricted. They also execute some computations and store some data at the same time. For any routing system, energy efficiency, autonomy, and scalability become critical. The sensor nodes function as border routers, establishing a connection between the internet/LAN and the low-powered lossy networks. All of these devices are based on the IPv6 protocol because of the increasing extent of IoT networks. An IETF IPv6 adaption layer that facilitates communication across lossy networks with minimal power is an adoption over IPv6. Route optimization techniques that are both safe and efficient have been presented. The proposed protocol intends to improve on the existing Proxy Mobile IPv6 routing technology for smart home networks. Mutual authentication, key exchange, complete transfer secrecy, and data protection are all supported by this protocol. Based on the trust mechanism, a new Secure trust enabled RPL routing protocol has been designed and built [19]. The suggested protocol tries to prevent ranking and an improvement in network speed is seen courtesy of Sybil attacks. Especially for large-scale IoT, a time synchronization technique was developed and it was very secure, in this technique the nodes use their parent and grandfather nodes to identify rogue nodes. A suggested technique for preventing black hole attacks on AODV-based MANETs is a safe and trust-based solution, but it may not support the main features of the IoT systems: scalability and mobility.

* 1. **Recent Works**

There are two kinds of emerging technologies that have recently gotten a lot of attention. One of the most popular new technologies to connect with IoT security solutions is Software Defined Networking. it’s based on the principle of separating network and data control. As a result, network management that is both centralized and dynamic can handle IoT environment issues like resource allocation for IoT devices. It can also effectively handle some of the present IoT concerns, such as dependability, security, scalability, and quality of service. Cryptocurrencies are built on blockchain technology. Process decentralization private & secure transactions, as well as communication, are all used in IoT-based applications. The application has had a lot of success in financial applications thus far. Decentralization, pseudonymity, and safer transactions come out to be some of the advantages of IoT blockchain technology. To deal with non-patchable vulnerabilities, A SDN-based cloud solution was proposed to provide safe transmission of data with QoS [20]. A proposal around blockchain technology was made where virtual zones are created which are secure and can be easily identified and trusted, further details are mentioned in [21].

1. **Searching in IoT**

The network of IoT devices are widespread across the world and contains billions of devices of different shapes and sizes with different functionality but all of them are generating data that are of some use or other, searching in these devices can be a major challenge, and finding relevant pattern can be even more tedious since the searching methodologies in the web document is different from the once which can be used in IoT, because of the nature of IoT devices and restrictions like sticking to a particular context and absence of having a generic index for all the devices and networks, also the ever-changing technology poses a severe challenge. Searching on the web is super easy and convenient, reusing the same technology for searching in IoT can be very beneficial [22]. This leads to the development of search engines for Web of Things (WoTSE), which use Web technologies to retrieve information and services from physical devices via the Internet of Things. Each physical object in World of Warcraft has a digital equivalent known as a "Digital Twin." These digital twins were accessible via hypertext transfer protocol using the RESTful APIs and were using the Representational State Transfer (REST) architecture. Steady growth has been seen in WoTSE research after being started in the 2000s. It may be divided into three categories: functionality search, sensor search, and object search[23]. WoTSE was frequently used in early projects to locate physical objects with active sensor nodes or RFID tags. One of the works from Dyser looks for physical entities depending on their true state as determined by sensor readings [24]. Also, research work on sensor search is done by cassaram [25]. It retrieves sensors using WoTSE, which is based on circumstances like cost & reliability, and their meta-data. Each variant of WoTSE has its unique characteristics, however, they might all be based on the unified search architecture proposed in [23].

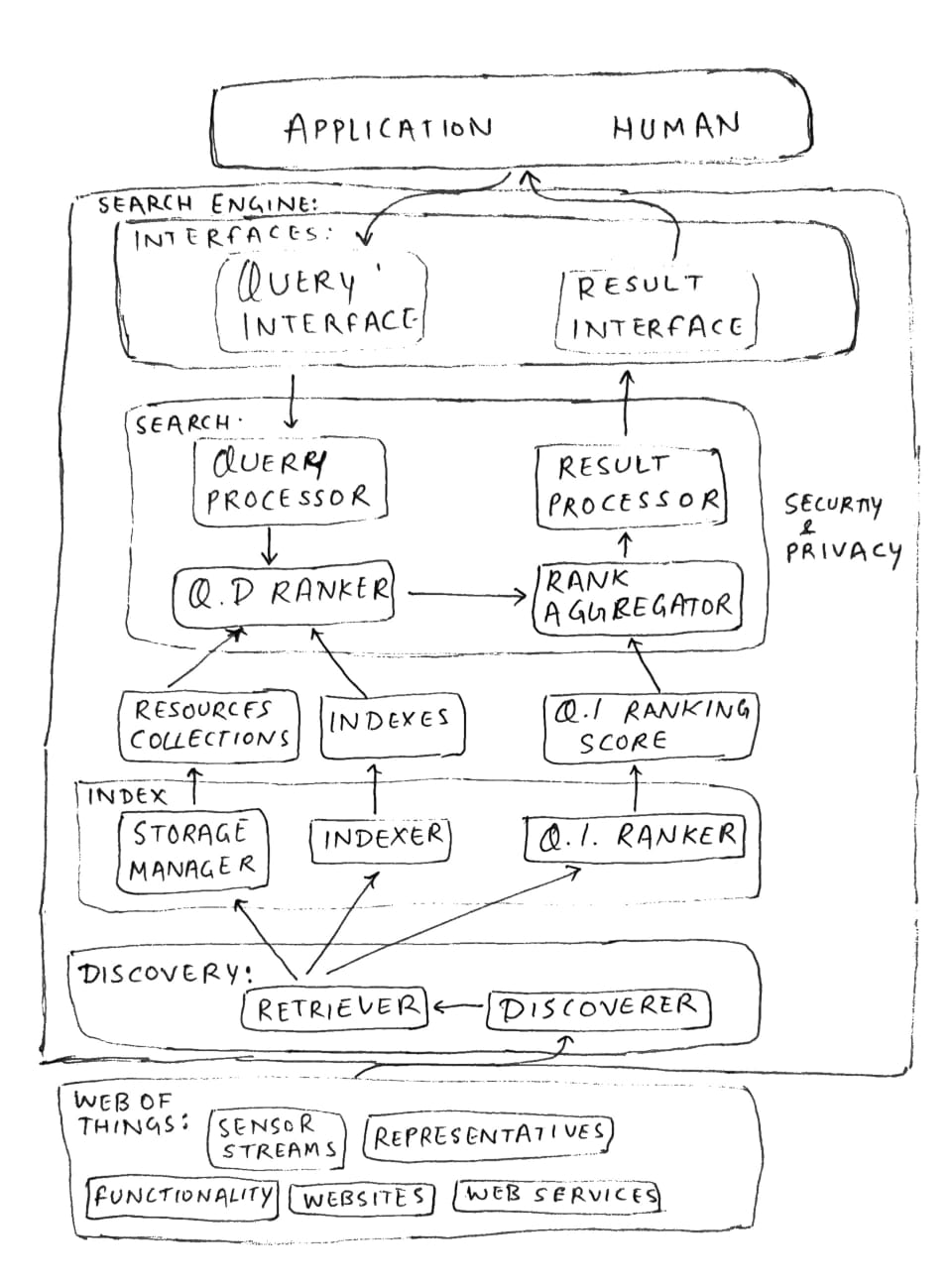


Fig 3. An architecture Searching in IoT.

A generic architecture and different layers are shown in the figure [Fig 3]. The lowest two levels are in charge of the discovery, while the upper two layers are in charge of the search. Two sets of levels are associated with the resource collection and index storage modules. Security, privacy, and reliability assessment methods are organized in vertical levels to secure the entire system. Several online resources like webpages, etc are served by the discovery layer in particular and act as a gateway between the two. The Indexer modules and Collection manager are used by the index layer to store and index resources. Resources are also arranged at this level. The query resolution procedure is handled by the search layer. A module that converts the user request into a format that can be processed by the system is called the query processor module. The query resource discovered in the connection to the user is assessed by the Query-dependent marshaller and finds the relevant result resource using the recorded linkages between the resources. Query Detector and Query Indexer ranking are merged by the ranking aggregator module to generate a single resource. To provide search results, the results processor gathers and combines information from matched sites. WoTSE is connected to the user through the user interface (UI) layer. It has two interfaces for accepting queries and producing search results: a query interface and a result interface. The modular design serves as a benchmark against which previous WoTSE implementations may be compared. Examine how each module is supported by current work and how it is implemented in general. WoTSE's purpose is to create a search engine. Whatever information is available on the internet of things. To achieve this aim, efficient and appropriate solutions to various issues are required. Because of the dynamic and varied nature of IoT data, crawling and indexing huge volumes of it for search purposes is intrinsically difficult. It's also difficult to find valuable web resources connected to things because the language of interpretation is available in a variety of ways.

1. **Other Research**

IoT has several other shortcomings or areas where research work is done, and improvements are to be done like recommendation systems in IoT. Because of the IoT ecosystem's exponential data explosion searching in IoT networks, accessing data in IoT networks, or connecting between different devices is never been as difficult as it is today. As a result, rather than looking for a suitable IoT device, proactively locating one is a preferable paradigm. Instead of requiring the user to trawl the internet for suitable gadgets to satisfy their needs, the autonomous IoT system may now propose and send appropriate resources to the user based on her previous choices. This IoT recommendation technique, which we call the thing-of-interest (TOI) suggestion, is an essential study issue for future IoT applications, TOI has its few challenges on its own due to the IoT environment. Also, Conversational IoT has been thriving with the launch of smart assistants like Google Assistant, Alexa, Siri. Conversational IoT is reading and understanding the human language, this technique seeks for understanding the human languages/words and replying to them just as a human being. This can be text-based or voice-based as well, making the whole experience very personal for the user. There has been a lot of research around this area and improving the IoT part to get a better experience in understanding human language and emotion. Service Computing-based IoT, service-based applications are a huge success in the field of software applications, it changed the way how an application is made, delivered, and used. It is based on service-oriented architectures where everything is based on different collections of services that can be used modularly to develop applications and cut the cost of development. RESTful services are an example of SOA-based applications. A similar thing can be implemented in IoT and can be used to solve problems in IoT using the same service-oriented architecture, coupling an existing service architecture with the IoT architecture can be difficult because of the constraints of IoT devices, also the existing service-oriented application mostly is of single layer and contains only services however IoT devices contain multiple layers of components, hardware, ICs and services which poses another problem for SOAs for IoTs. Several research is done to make services available for IoT devices. Semantic annotation, Open IoT project, Semantic sensor networks, Hydra project, etc. There are a few other research works that are in done, including data-driven IoT, Social IoT, Edge Computing and IoT, etc.

1. **Summary**

The Internet of Things has been an extremely busy field in terms of innovation and research, the technology is new when compared with others in computer science, there are several shortcomings like energy harvesting, security & privacy issues, and searching in IoT that we discussed in the paper are significantly improving and showing its potential to change how the technology operates. Due to the security & privacy concerns, the directness, diversity, and size of IoT networks and devices, many challenges are still open for discoveries. We have discussed only some of these major challenges in the paper.

**References**

[1] https://www.statista.com/statistics/487291/global-connected-wearable-devices/

[2] https://internetofthingsagenda.techtarget.com/feature/Future-of-IoT-6-trends-and-predictions-to-watch

[3] https://en.wikipedia.org/wiki/Internet\_of\_things

[4] W. E. Zhang et al., "The 10 Research Topics in the Internet of Things," 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC), 2020, pp. 34-43, doi: 10.1109/CIC50333.2020.00015.

[5] Hrishikesh Jayakumar, Kangwoo Lee, Woo Suk Lee, Arnab Raha, Younghyun Kim, and Vijay Raghunathan. 2014. Powering the internet of things. In Proceedings of the 2014 international symposium on Low power electronics and design (ISLPED '14). Association for Computing Machinery, New York, NY, USA, 375–380. DOI:https://doi.org/10.1145/2627369.2631644

[6] Jiang, C.Y. & Sun, X. & Tan, K. & Lo, G. & Kyaw, Aung & Kwong, D.. (2008). High-bendability flexible dye-sensitized solar cell with a nanoparticle-modified ZnO-nanowire electrode. Applied Physics Letters. 92. 143101-143101. 10.1063/1.2905271.

[7] https://revibeenergy.com/piezoelectric-electromagnetic-harvesting/

[8] Hawkes, Allen & Katko, Alexander & Cummer, Steven. (2013). A microwave metamaterial with integrated power harvesting functionality. Applied Physics Letters. 103. 163901-163901. 10.1063/1.4824473.

[9] Younghyun Kim, Naehyuck Chang, Yanzhi Wang, and Massoud Pedram. 2010. Maximum power transfer tracking for a photovoltaic-supercapacitor energy system. In <i>Proceedings of the 16th ACM/IEEE international symposium on Low power electronics and design</i> (<i>ISLPED '10</i>). Association for Computing Machinery, New York, NY, USA, 307–312. DOI:https://doi.org/10.1145/1840845.1840909

[10] Yoon, E.-J. et al. (2013) “Micro-scale Solar Energy Harvesting System with a New MPPT control,” Journal of the Korea Institute of Information and Communication Engineering. Korea Information and Communication Society, 17(11), pp. 2627–2635. doi: 10.6109/JKIICE.2013.17.11.2627.

[11] Notten, Peter & Roozeboom, Fred & Niessen, R.A.H. & Baggetto, Loïc. (2007). 3‐D Integrated All‐Solid‐State Rechargeable Batteries. Advanced Materials. 19. 4564 - 4567. 10.1002/adma.200702398.

[12] Gorlatova, M., Kinget, P.R., Kymissis, I., Rubenstein, D., Wang, X., & Zussman, G. (2010). Energy harvesting active networked tags (EnHANTs) for ubiquitous object networking. IEEE Wireless Communications, 17.

[13] Chien-Ying Chen and Pai H. Chou. 2010. DuraCap: a supercapacitor-based, power-bootstrapping, maximum power point tracking energy-harvesting system. In <i>Proceedings of the 16th ACM/IEEE international symposium on Low power electronics and design</i> (<i>ISLPED '10</i>). Association for Computing Machinery, New York, NY, USA, 313–318. DOI:https://doi.org/10.1145/1840845.1840910

[14] Fei Li, Yang Li, Jiang Qu, Jinhui Wang, Vineeth Kumar Bandari, Feng Zhu, Oliver G. Schmidt, Recent developments of stamped planar micro-supercapacitors: Materials, fabrication and perspectives, Nano Materials Science, Volume 3, Issue 2, 2021, Pages 154-169, ISSN 2589-9651,https://doi.org/10.1016/j.nanoms.2020.10.003.

[15] Lei Yang, Abdulmalik Humayed, and Fengjun Li. 2016. A multi-cloud-based privacy-preserving data publishing scheme for the internet of things. In <i>Proceedings of the 32nd Annual Conference on Computer Security Applications</i> (<i>ACSAC '16</i>). Association for Computing Machinery, New York, NY, USA, 30–39. DOI:https://doi.org/10.1145/2991079.2991127

[16] M. Fischer, A. Scheerhorn and R. Tönjes, "Using Attribute-Based Encryption on IoT Devices with instant Key Revocation," 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2019, pp. 126-131, doi: 10.1109/PERCOMW.2019.8730784.

[17] Ferrag, Mohamed Amine & Maglaras, Leandros & Janicke, Helge & Jiang, Jianmin. (2016). Authentication Protocols for Internet of Things: A Comprehensive Survey.

[18] Singh, S., Sharma, P.K., Moon, S.Y. et al. Advanced lightweight encryption algorithms for IoT devices: survey, challenges, and solutions. J Ambient Intell Human Comput (2017). https://doi.org/10.1007/s12652-017-0494-4

[19] David Airehrour, Jairo A. Gutierrez, Sayan Kumar Ray, SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things, Future Generation Computer Systems, Volume 93, 2019, ISSN 0167-739X, https://doi.org/10.1016/j.future.2018.03.021.

[20] Seokhoon Kim and Wonshik Na. 2016. Safe Data Transmission Architecture Based on Cloud for Internet of Things. <i>Wirel. Pers. Commun.</i> 86, 1 (January 2016), 287–300. DOI:https://doi.org/10.1007/s11277-015-3063-1

[21] Hammi, Mohamed Tahar & Hammi, Badis & Bellot, Patrick & Serhrouchni, Ahmed. (2018). Bubbles of Trust: a decentralized Blockchain-based authentication system for IoT. Computers & Security. 78. 10.1016/j.cose.2018.06.004.

[22] S. Duquennoy, G. Grimaud and J. -J. Vandewalle, "The Web of Things: Interconnecting Devices with High Usability and Performance," 2009 International Conference on Embedded Software and Systems, 2009, pp. 323-330, doi: 10.1109/ICESS.2009.13.

[23] N. K. Tran, Q. Z. Sheng, M. A. Babar, and L. Yao, “Searching the Web of Things: State of the Art, Challenges, and Solutions,” ACM Computing Surveys, vol. 50, no. 4, pp. 55:1–55:34, 2017.

[24] Ostermaier, Benedikt & Römer, Kay & Mattern, Friedemann & Fahrmair, Michael & Kellerer, Wolfgang. (2010). A real-time search engine for the Web of Things. 10.1109/IOT.2010.5678450.

[25] Perera, Charith & Zaslavsky, Arkady & Liu, Chi Harold & Compton, Michael & Christen, Peter & Georgakopoulos, Dimitrios. (2013). Sensor Search Techniques for Sensing as a Service Architecture for The Internet of Things. IEEE Sensors Journal. 14. 10.1109/JSEN.2013.2282292.

[26] B. Özdenizci Köse , "Towards Adoption of Blockchain Technology for Enhancing Communication in Smart Transportation", Avrupa Bilim ve Teknoloji Dergisi, no. 21, pp. 473-485, Jan. 2021, doi:10.31590/ejosat.823102