Survey Paper on Internet of Things Architecture

Saptarashmi Bandyopadhyay
Department of Computer Science and Engineering
Pennsylvania State University
University Park 16802
U.S.A
(+1)8146992126
szb754@psu.edu

1. ABSTRACT

The objective of the CSE 530 class project is to survey the research literature on Internet of Things (IoT) [1], [2], [3], [4], [5] Architecture and its components [6], reference architecture for IoT infrastructure in the industry [7], [8], recognizing the issues in the implementation of IoT architecture in autonomous systems [9], [10], [11], [12], IoT architectural framework for connection and integration of heterogeneous IoT devices and systems [13], [14], [15], addressing the security concerns in cyber-physical systems [16], [17], [18], [34], [35], [36], [37], [38], [39], challenges of efficient power utilization in embedded IoT systems [19], [20], [21], [22], [40], [41], [42], [43], [44], cloud customer architecture of IoT [23], studying predictive solutions to the IoT architecture [24], software architecture for IoT applications [25], IoT architecture for scalable management and implementation of blockchain [26]. Various tools [28] which can be used to simulate and implement the IoT architecture have been studied. The Distributed Services Architecture (DSA) for IoT applications [45] has been used on real-time weather data to demonstrate the collaboration among the underlying components of the IoT architecture [46], [47], [48]. In view of the exponential increase in IoT devices [30], a new horizon of modern Instruction set architecture (ISA) will emerge to provide efficient service [29].

2. INTRODUCTION

Internet of Things is an emerging area of research which is in immense need of an efficient architectural framework in view of the rise in the number of smart systems and IoT devices [30]. Noted computer architects and 2017 A.C.M. Turing award winners, Prof. John L. Hennessy and Prof. David A. Patterson have spoken of an upcoming Golden Age of Computer Architecture with focus on cost, performance, energy and security in their Turing lecture [29] and emphasized on the need on fundamental changes in the ISA to service heterogeneous IoT devices.

The most noted conferences in computer architecture like International Symposium on Computer Architecture (ISCA) and others have started holding workshops and symposiums [22], [27], [29], [31] on IoT architecture and its applications like in mobile and embedded systems.

A total of 48 research papers, articles, manuals and conference proceedings have been studied for the class project. The evolution and paradigms of Internet of Things have been discussed in this paper [3], [4], [5], [32], [33]. 10 areas of research about the IoT architecture and its components and implementation issues over heterogeneous IoT systems have been elaborated in the following sections of the paper along with an overview of

some practical tools [28] and use of the DSA platform for IoT services [48].

3. EVOLUTION OF INTERNET OF THINGS

The term IoT was devised in 1999 by Mr. Kevin Ashton, who was one of the co-founders and an executive director of the Auto-ID Center at Massachusetts Institute of Technology (MIT) [3]. IoT can be considered to be a general infrastructure across the globe which provides specialized services by a combination of physical and virtual elements which follow interoperable information and communication technologies [5], [33]. It is a combination of several technologies that work together [4]. One of the objectives of IoT is to improve the detection and understanding of information by a computer by decreasing human mediation [1]. The present evolution of the Internet as a network of interconnected objects has led to a focus of perceiving the information, improving the command and control system for better interaction with the smart environment and to use the Internet standard for providing several services like data transfer, analytics and communication [1].

A smart environment can be considered to be a physical world which is closely and inconspicuously intertwined with sensors, actuators, display units and other computational objects which are ubiquitously embedded in regular life objects and connected continuously and are connected continually over large networks [32]. IoT has developed over the last 19 years with large-scale applications like healthcare, supply-chain management [1], transportation, logistics and social networking [2]. The data streams in IoT are real-time in nature which includes complexity in processing and in the underlying architecture..

4. PARADIGMS OF IoT

The RFID (Radio-frequency identification) group has defined IoT to be a worldwide network of interconnected objects that are uniquely addressable and follow a set of standard communication protocols [1]. IoT can be envisioned in three different paradigms [2] which are represented as follows:

i) Internet-oriented: It emphasizes on the middleware. This perspective of IoT consists of elements like the Internet, Web of Things and IPSO (Internet Protocol for Smart Objects).

ii) Things-oriented: It focuses on integrating generic objects like RFID (radio frequency identification), sensors and actuators on a common framework.

iii) Semantics-oriented: This view of IoT provides importance on the knowledge. It has emerged to address the challenges of the unique addressing of generic objects and about the storage and information of exchanged data. It has the benefit of supporting different devices, clouds or gateways by being compatible to their standardization initiatives [12].

5. INTERNET OF THINGS (IoT) ARCHITECTURE

The multiplication in the number of smart devices, enabled by ubiquitous computing has led to the creation of IoT [2,3] in a communicating-actuating network where the sensors and actuators together work seamlessly with the environment and the data generated by these devices are shared across platforms to give a common operating picture (COP) [1]. IERC (Internet of Things European Research Cluster) has established the IoT architecture(IoT-A) project to establish an architectural reference model [1] for the interoperability of IoT systems. IoT architecture can be considered as physical or virtual or a

combination of the both [5] which can be categorized into the following components [1]

i) hardware consisting of sensors and actuators for embedded communication

ii) middleware which stores on demand and carries out data analysis

iii) presentation which ensures easy presentation and visualization of the architecture.

The basic IoT architecture is layered consisting of three layers which are the perception layer, the network layer and the application layer which are in a stacked order [4]. The perception layer collects data from sensors and actuators which are then processed and communicated in the network layer [4]. The application layer provides services to the user based on multiple applications [4].

Domain specific IoT architecture like RFID [5], cloud or fog-based architecture [4], [5] which use the generic 5 layer IoT architecture [4] consisting of the perception layer, transport layer, processing layer, application layer and business layer. The transport layer communicates data from perception layer to processing layer and vice-versa [4]. The processing layer stores, analyzes and processes data from the transport layer [4]. The business layer is responsible for managing the whole IoT system like applications, business models and protection of the privacy of users [4].

The layers of IoT architecture can also be represented as [6] Device Access Layer, Device Management Layer, Data Warehouse, Behavior Management Layer, IoT Layer and Service Integration Layer. The Device Access Layer identifies the device, executes communication and control protocols using device drivers and communicates among devices [6]. The Device Management Layer controls the devices based on their status information [6]. Data warehouse stores large amounts of heterogeneous data which can be used by multiple IoT applications and services [6]. The behavior management layer satisfies the commercial requirement of the users based on situations and rules from a pool of actions [6]. IoT layer communicates among objects, matches suitable actions and discovers the mechanisms and also tags the systems [6]. The service integration layer ensures the interconnection of the users with the services [6]. Performance can be enhanced by management mechanisms like caches and the security extends through the entire network, although it is implemented differently in different layers [6].

The Unifying Sensing Platform (USP) allows the seamless integration of a number of dissimilar objects efficiently in a reusable and context aware way [5]. The USP architecture can be stratified into the sensor framework, resource framework, observation framework and context framework [5]. Efficient sensor-oriented usage is ensured by the control methods using contextual observations towards the upper level of applications [5].

6. REFERENCE ARCHITECTURE FOR IoT INFRASTRUCTURE

Intel has defined the system architectural specification (SAS) to connect any types of IoT devices to the cloud irrespective of native internet connectivity in view of 50 billion IoT devices in the next 2 years [7]. This architectural framework facilitates secure, scalable and interoperable IoT operations, allows seamless data ingestion and device control, provides provisions of automated discovery of edge devices, gives analytics infrastructure for customer satisfaction and monetizes the IoT infrastructure with services [7]. There are two versions of Intel's SAS where the latest version is specialized for the smart connected objects [7]. The reference architecture is layered with the communications and connectivity layer, data layer, management layer, control layer, application layer and business layer [7]. All the layers interact with the developer

enabling layer [7]. A security layer is executed in runtime which secures all the above layers [7]. The application and business layers are user layers whereas the communications and connectivity layer, data layer, management layer and control layer are executed during runtime [7].

The IIRA (Industrial IoT Reference Architecture) consists of models, definitions and a clearly defined set of ontology to provide basic standards for all IoT systems in frame development, documentation, communication and deployment [8]. The Industrial IoT Architecture has been viewed by the IIRA from the perspective of the stakeholders and these viewpoints are bound to the lifecycle process [8]. The systems can be classified into controls domain, operations domain, information domain, application domain and business domain [8]. The architecture can be categorized into the edge tier performing device management, the platform tier which comprises of the service platform and the application tier which deals with the domain applications [8]. These tiered architecture can be mapped to the specified functional domains [8].

7. PROBLEMS IN IMPLEMENTING IoT ARCHITECTURE

A single reference architecture cannot be used in the description of IoT architecture as it encompasses a variety of technologies and varied states of implementation [9,11]. It is not clear whether a single addressing format or a single addressing model can be applied in the IoT architecture and a centralized architecture can be a security concern [11]. The networking challenges of scalability, multi-tenancy, open network interfaces, low power-communication and security challenges plays a significant role on investment on the technology if the risks of such challenges are significantly high [9], [12].

There are problems of performance, evolution, complexity and quality of services in the IoT architecture which needs to be addressed [9]. Recovery mechanisms have to be instituted in the IoT architecture from a known good state if it is compromised by the distributed ubiquitous devices [9]. The small devices may not be supported by continuous power sources [9]. The capability of shared and virtual resources and infrastructure have to be provided to support multiple IoT applications [9]. The virtual resources have to be mapped to the underlying shared physical infrastructure [9]. The architecture should be able to support the capability of the IoT devices to have customized network interfaces, operating systems and programming models with an optimal usage of the computational resources and energy [9]. With a varied set of semantics and access in open environments, more complex dependencies need to be supported by the IoT architecture [9]. Real-time analysis of data requires improved synchronization mechanisms with high timing precisions [9].

The IoT architecture has to be flexible and adaptive to the changing user requirements like by introducing new devices or new functionality [12]. A flexible distributed IoT architecture [12] can bind similar uses together and separate orthogonal features along with a hierarchical structure of the functionalities [12]. It supports the architecture with the functionalities of heterogeneity, scalability, configuration and inter-operability [12]. The lack of appropriate evaluation of performance affects the processing speed, communications speed and memory requirements of multiple components in the different layers of IoT architecture [12].

Redundancy in IoT architecture will support resilience to ensure that critical devices and services can be provided [12]. Caching and tunneling supports the mobility of the IoT based services [12].

There are challenges in IoT architecture development like data management, data mining, privacy and accuracy [10]. The architecture of the data center needs to deal with large amounts of heterogeneous data [10]. The design of IoT architecture needs to incorporate uniform standards across multi-purpose collaborative devices [10], [12].

8. IoT ARCHITECTURAL FRAMEWORK FOR INTEGRATION AND INTERCONNECTION OF DEVICES AND SYSTEMS

IoT architecture provides on-demand and scalable services which can be shared and these services are provided by the cloud which highlights the importance of the successful dynamic data integration of the heterogeneous IoT devices and systems to the cloud [13]. The components of IoT architecture and cloud computing to be integrated on the cloud platform are batch processing, distributed databases, real time processing, distributed queries and management and deployment of the clusters [13]. It provides storage, processing and improved scalability which were restricted by the limitation of components in the IoT architecture [13]. Integration of the cloud infrastructure will facilitate the interconnection of multiple data centers and access of the data by secure abstraction mechanisms [13]. Middleware for IoT can be designed using layered container-based architecture comprising of a virtual sensors manager, query manager, configuration notification manager and an interface layer [13].

An IoT integration framework has been proposed which uses an intelligent API (Application Program Interface) layer by working with an external service assembler, service auditor, monitor and router to coordinate the publication of services, subscription, decoupling and service combination inside the IoT architecture [14]. It overcomes the weakness of Service Oriented Architecture to provide proper integration, scaling and resilience to IoT system architectures [14]. The micro-services architecture ensures the deployment of services independently along with atomicity of services, resilience to single point failure, synchronization of IoT services and security transaction management [14].

The functional requirements of IBM's IoT reference architecture, based on which many IoT devices are connected, are easy usage, robust device management, easy sharing of data, enterprise and home networks [15].

9. SECURITY ISSUES IN THE ARCHITECTURE OF CYBER-PHYSICAL SYSTEMS

Security hazards exist in cyber-physical systems due to many reasons like scalability, constrained resources, heterogeneity, interoperability, latency constraints etc. [17]. Distributed servers collect data from the Internet by linking and cross-linking using the Object Naming Service (ONS) allowing third party access to the information which makes the access points vulnerable [36]. A large number of IoT nodes do not store the metadata or the temporal data which makes it difficult to track the origin of information, thus making the security susceptible [37]. Cyber forensics in IoT systems without properly documented methods and tools makes it difficult to ensure a safe logging and monitoring system to preserve and analyze cyber-physical systems data due to deficit attribution of malicious activities [37]. A secure IoT architecture needs to ensure absolute perception, reliable transmission, intelligent processing, The security problems and possible measures to solve

these problems in the different layers of IoT architecture can be categorized as follows [35]:

1. Perception Layer

A. Security challenges [35]: RFID readers and other devices collect data using wireless signals which are exposed in public places. This makes them vulnerable to attacks like Differential Power Analysis (DPA), node capture where primary nodes are taken over as gateway nodes, fake node and spurious data consuming energy from nodes and potentially destroying the network, Denial of Service (DoS) attack, timing attack from analysis of the execution time of encryption algorithms routing threats, replay attacks in authentication processing, Side Channel Attack (SCA) causing unnecessary time or power consumption and Mass Node Authentication problem. As IoT devices support low power, sleep deprivation attacks stop the sleep routines which would have reduced the power consumption [38].

B. Solutions [35]: i) Access control [35,36]: It protects the data in the RFID tags and covers label failure, chip protection, antenna energy analysis. ii) Physical security scheme [35]: DPA, a type of SCA can be prevented by hiding and masking. Hiding removes data dependencies of energy consumption. Masking randomizes the intermediate values in the encryption devices.

iii) Physical security design [35]: The security of node design has to be ensured which involves security measures in hardware structure design, chip selections, chip connections, radio-frequency circuit designs and data acquisition unit design. Antenna design has to satisfy the communication distance requirement along with high stability and adaptability.

iv) Data encryption [35]: A non-linear key algorithm using displacement calculation ensures high security and high speed data transfer with small power consumption.

v) IPSec security channel [35]: It ensures authentication [36], [37] and encryption of data.

vi) Key management [35]: Key generation and update algorithms need to incorporate forward privacy, backward extensibility, prevention of collusion attacks and source authentication.

vii) Intrusion detection system [35]: The periodic monitoring of the behavior of IoT nodes ensure security of the system.

viii) Better cryptography technology scheme [35]: It protects user privacy and authenticity and integrity of the RFID systems.

2. Network Layer

A. Security challenges [35]: The internet security architecture faces challenges of compatibility during communication among machines. This leads to a split of logic relationship between IoT machines which along with multiple access methods of the access network and heterogeneous nature of IoT devices makes security and interoperability [36] vulnerable. Authentication [36], [37] in a cluster of IoT devices leads to large-scale network congestion which can cause security concerns. Sinkhole attacks can take place when a compromised IoT device can claim to support high amount of power, leading to other devices connecting to this node for forwarding purposes thereby increasing the data flow in the compromised sink node [38]. Wormhole attack is achieved by two collaborative malicious IoT nodes by falsely reducing the forwarding hops leading to more data to be transmitted to these nodes [38]. Other problems lie from eavesdropping data, privacy and confidentiality disclosures due to unauthorized data access, man-in-the-middle attack [38], exploit attack and virus invasion.

B. Solutions [35]: Several mechanisms need to be enforced like end-to-end authentication, cross-domain authentication, cross-network authentication, key agreement mechanism, Public key infrastructure (PKI), security routing, onion routing [36] and intrusion detection. Network virtualization technology ensures simple network management and helps in prevention of error. Implementation of IPv6 layer as a transport carrier

network in IoT also increases the security of the IoT devices.

3. Application Layer

A. Security challenges [35]: User access, identification and data protection can suffer attacks due to spurious information. Mass nodes management which require large scale of data transfer and fast processing and adaptability can lead to data loss if the requirements are not met. Software vulnerabilities in the application layer due to non standard programming like vulnerabilities can be misused to compromise the application layer in IoT architecture.

B. Solutions [35]: i) Across Heterogeneous Network Authentication and Key Agreement can be ensured by symmetric key crypto-system and certification transfer technology.

ii) Private data can be protected by fingerprint technology, digital watermarking and anonymous authentication.

iii) Information security management, which involves management of resources and physical security needs to be strengthened,

System auto-configuration and automatic update of system software and firmware ensures secure operations even for resource constrained IoT devices by using the gateway architecture for high system availability [16].

A reference framework to ensure security in IoT architecture has been developed by Symantec [18] that mitigates malicious data by host-based protection and security analytics. Communication is protected by mutual authentication and encryption leveraging Ellyptic curve cryptography (ECC) based algorithms for resource constrained IoT devices [18].

Microsoft Azure IoT reference architecture carries out threat modeling in the design phase to address the threats in the areas of devices, data transfer, device and event processing and presentation [34]. It addresses the threats of spoofing, tampering, denial of service, information disclosure and elevation of information privilege [34]. The cloud gateway that ensure remote communication among IoT devices provides security to the exposed endpoints by the Security Development Lifecycle [34,39].

10. POWER UTILIZATION IN EMBEDDED IoT ARCHITECTURE

Energy dimensioning of IoT devices to meet the application requirements is an uphill task [22] when the reliability of industry applications have become uncertain due to energy harvesting [19]. Model energy consumption of wireless IoT devices takes into account many application parameters that affects the energy live-cycle [19]. The increasing scale of industrial IoT (IIoT) systems has led to large amounts of energy consumption [40]. Traditional IIoT systems not only have the capability of increasing carbon footprint but also limits their continuous operations due to support by low-powered devices.

IoT software architecture can be designed with reusable components which improves the energy efficiency of such devices which comes at a cost of performance like late response time [20]. A methodology to select the energy efficient components from a repository and calculate the energy required for the services provided by the IoT software architecture can ensure the goal to save power [20]. Energy profiling of the re-usable software components can lead to quicker and accurate development of the IoT architecture [20]. Energy consumption due to hardware units is dependent on the clock speed of the CPU and memory size which can be controlled the software components in the architecture [20]. Energy utilization is also dependent on the version of Operating System, code optimization policies of the compiler and the interface [20]. An IoT

framework uses smart location-based automated and networked energy control in smart-phones and clouds which uses multi-scale energy proportional to the area of application [21].

An energy efficient IIoT architecture comprises of the sense entities domain, RESTful service hosted networks, cloud server and user applications [40]. A three-layer hierarchical framework in the sense-entities domain for the deployment of IIoT nodes saves energy and increases network lifetimes [40]. The smart devices in this domain are categorized into sense nodes (SNs), gateway nodes (GNs) and control nodes (CNs) for energy optimization [40]. SNs transfer the information to GNs as relay nodes based on a trigger or periodically and direct communications between SNs are prohibited, thereby saving energy [40]. Energy consumption due to data processing by SNs can be limited by sleep scheduling when some nodes are switched off if they are inactive [40]. GNs forward the data to the cloud servers through CNs [40]. The sleep interval of a SN which transfer data to a GN can be estimated by prediction from the usage history of SN [40]. Thus GNs can alter the state of SNs which can lead to effective energy consumption [40]. An activity scheduling mechanism is maintained alongside it to switch the nodes to sleeping and waking up mode based on the requirement [40]. The RESTful web services are hosted in networks which connects the objects in the sense entities domain to the cloud server [40]. The cloud server employs the virtualization environment which is then transferred to the application layer and interfaces thereby improving the processing capabilities [40]. System development constraints like energy consumption limits of data transfer are limited by the size of the data, radio electronics and the distance between the source and the final nodes [40].

The design of nodes should be modular to save power [41]. The requirement of low energy consumption of sensors leads to distributed intensive processing of the data [41]. Cloud resource provide the computing capacity and elasticity to satisfy the energy requirement also on the service-side [41]. Use of connectionless protocols in the gateways of the IoT architecture will decrease the consumption of power due to data transmission [41]. Each IoT node can have its own power management unit which will lead to elimination of the standby energy of the system when individual nodes are not being used [41]. The gateway architecture can be customized by combining the functionality of a general purpose microprocessor with an extremely low power controller which helps in simplifying the software development effort and ensures flexibility [41]. Only the radio module has to be kept switched on always as the microcontroller can wake up once a packet arrives to the radio module and the microprocessor can stay switched off unless data collection is being done [41]. However, the shortcoming is that the gateway may not always be available for reconfiguration from the Internet side [41].Such architectures can be applied in data intensive applications like preservation of cultural heritage [41].

A balance has to be maintained between the quality of data processed by the IoT nodes and the power consumption of the nodes [42]. Quality of information can be ensured if more data is harvested at shorter sleep intervals but it comes at the cost of spending more energy [42]. The coverage area of multiple sensors can overlap which can control the power consumption of these sensors [42]. Energy can be saved in the information processing layer of the IoT architecture by using an energy-efficient resource allocator (eRA) which allocates hardware resources for processing information based on the requirement of information [42].

The technology of wireless energy harvesting (WEH) of IoT devices is simple, easy to implement and readily available [43]. It ensures prolonged battery longevity of these devices [43]. Energy harvesting from environmental resources

like solar and thermal is dependent on the presence of the energy resources which is not mandatory in case of wireless resources as the signals are readily available [43]. WEH unit in a sensor harvests the radio frequency energy, thereby producing a stable energy resource for the rest of the IoT device along with interface with the power management unit (PMU) [43]. High efficiency wireless energy harvesting rectifiers have to be used along with low power wake-up radio for the WEH unit in the IoT architecture [43]. Dedicated radio frequency resources can be optimized to satisfy the maximum energy requirements [43]. Harvesting of dynamic ambient radio frequency resources requires smart management of the WEH unit monitoring the channel at the access points to find the best possible moment to harvest energy [43]. The power consumption of the radio transceivers can be addressed by the wake-up radio scheme where the receiver switches between the listening and sleeping states by duty-cycling based on requirements [43]. The architecture of the PMU is able to detect and pre-empt node failure due to insufficient energy requirement by collaboration with the WEH unit [43]. A significant impact of this technology is to mitigate the impact on the users and on the environment [43]. Dynamic duty cycles in the sensors can lead to problems of synchronization and reliability in implementing the medium-access control (MAC) protocol design [43].

It has been envisioned that ubiquitous IoT architecture is being developed which is similar in structure to the social organizational framework [44]. The application of IoT architecture in social networks can lead to challenging requirements of energy [44]. Co-operative services, based on multiple objects like Bluetooth or low-power wireless personal area networks (WPANs) of sensors and actuators and RFID systems can reduce the energy consumption of wireless devices [43].

11. CLOUD CUSTOMER ARCHITECTURE OF IoT

The Object Management Group has specified a framework for cloud customer architecture in IoT which is presented as a three layered architectural pattern as defined by the IIRA [23]. The architecture has to comply with the norms and requirements of the industry [23]. The edge tier consists of proximity and public networks where data is collected from IoT devices, followed by the platform tier consisting of the provider cloud and the enterprise tier comprising the enterprise network [23]. The interconnection of the devices leave security issues to be considered [23]. The resilience of the architecture has to be ensured [23]. The user layer allows the customer to execute specific IoT applications and does not depend on the network domain [23]. Visualization and analytics is provided for the administrators and customers of the cloud based reference IoT architecture [23].

12.SOFTWARE ARCHITECTURE OF IoT

IoT application architecture is built over the hardware of sensors and actuators where the sensors generate data that are converted to understandable forms [25]. Network connectivity is provided by a wireless or a wired connection and security is ensured by data abstraction [25]. Edge computing allows transformation and analysis of the data after the information is stored and aggregated [25]. The analysis of the data helps in better decision making in the presentation layer which is followed by user interaction with such systems in the user interface layer [25].

13. PREDICTIVE ANALYTICS TO IoT ARCHITECTURE

Predictive analytics plays a significant role in the architecture of industrial IoT (IIoT) where the data is collected by conditions monitoring [24]. Estimation is done by machine learning techniques like polynomial regression to find the upper limit of the confidence band to fit the non-linear data while the lower limit is estimated by linear regression [24]. Implementation of the neural architecture across different IoT devices and systems is extremely challenging.

14. SCALABLE IoT ARCHITECTURE IN BLOCKCHAIN

The architecture is a distributed access control system for IoT built using the blockchain technology [26]. Bitcoin was one of the first applications of peer to peer trustless electronic cash and block chain is a secure distributed database which is the ledger of bitcoins [26]. A management hub obtains control data from the blockchain for the IoT devices [26]. The proposed architecture overcomes the limitations of centralized access management models which have technical problems in global management. This architecture is fully decentralized and scalable in specific IoT scenarios and facilitates easy integration of the IoT systems [26]. However there are limitations of crypto-currency fees and processing tines [26].

15. IoT ARCHITECTURE TOOLS

Some tools for simulation of IoT architecture like DSA (Distributed Services Architecture), an open source IoT platform which ensures communication among heterogeneous devices, Arduino Ethernet Shield and Intel Galileo which implements IoT systems and hazelcast in-memory datagrid were observed among other tools [28].

16. DISTRIBUTED SERVICES ARCHITECTURE

The Distributed Services Architecture (DSA) has three components [48]:

i) DSA-Broker which routes the incoming and outgoing data streams

ii) DSLinks that are connected to the DSA-Broker and originate the data-streams. They can be run on the same machine or on distributed machines.

iii) nodeAPI which ensures the communication among DSA nodes and maintains node compatibility along with bidirectional control and monitoring among connected components.

DSA is useful for distributing functionality among different computational utilities for architecting IoT based products [48].

DSA has been installed in Windows 8 to understand the architecture and services provided by the Distributed Services Architecture [45] . It can be launched from the command prompt by the command daemon.bat start. The server will be launched in localhost at port number 8080. As the port was already in use, the process ID using that port number was identified by the command netstat -ano | findstr :8080 and then removed by the command taskkill /F /PID 4800 [46].

Once the DGLux5 server of the DSA is launched in localhost, a project is created to demonstrate the services provided by the underlying architecture. Two gauges are selected from the dashboard panel to represent the temperature data.

Two primary nodes used by the DSA-Broker are sys node, which include the installed system

services, and downstream node which include the connections to the services [47]. The children of the downstream node are the currently executing services [47]. The weather DSLink was installed which provided the real time weather data including the temperature. To start the incoming data stream, the link is right-clicked and the Start Link option is selected. A weather tracker is created for New York, NY and State College, PA. Real-time data from sensors is then obtained by DSA in the downstream node. The temperature feature has been demonstrated in the gauge to demonstrate the incoming flow of weather data which is managed by the Distributed Services Architecture.

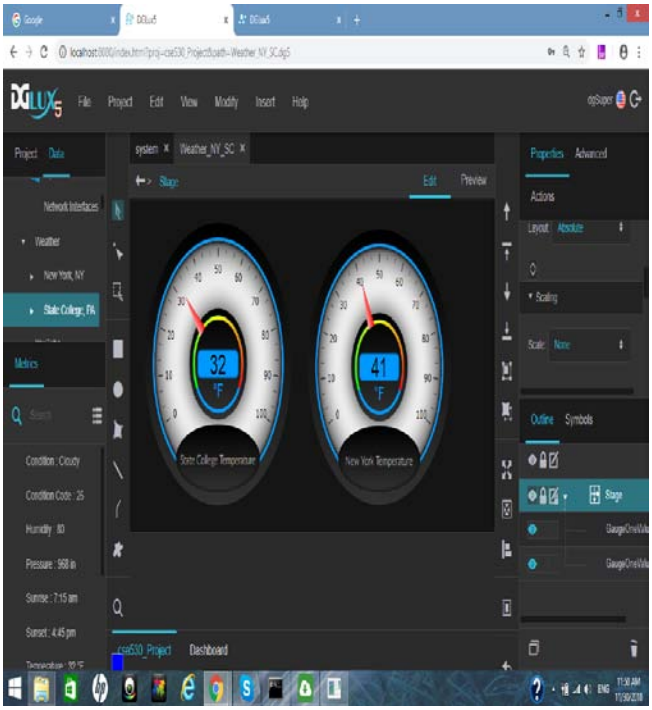

Figure 1: Real-time data of temperature of State College and New York as displayed by Distributed Services Architecture (DSA)

17. FUTURE WORK

More detailed review of the publications and study of new papers is necessary for the above identified research areas. The workshops and symposiums of IoT under the noted ISCA and Microarch conferences [22], [27], [29], [31] have to be investigated for deliberation on the above research areas and to find new areas of interest in IoT architecture. More experimentation on the tools should be done to understand the scalability effects on the architecture with a large number of IoT devices. The challenges to security, energy, scalability, integration and interconnection of the components of the IoT architecture needs to be addressed along with development of a new Instruction Set Architecture.

18. CONCLUSION

The increasing number of smart devices point out the unavoidable requirement of improving the efficiency of the IoT architecture. The CSE 530 class project report gives an idea of the salient issues in IoT architecture whose application is increasing in every passing day like analytics of social media data across IoT devices and studying real time weather in remote places to name a few. It is expected that more optimizations in the access management, security, power consumption and new ISA will improve the efficiency of IoT based systems in future.

19. REFERENCES OF PAPERS AND RESOURCES

1. J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions" by, Future Generation Computer Systems, Volume 29, Issue 7, September 2013, pages 1645-1660,

DOI: https://doi.org/10.1016/j.future.2013.01.010

2. L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey", Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 54, Issue 15, October 2010, pages. 2787-2805,

DOI: 10.1016/j.comnet.2010.05.010

3. That 'Internet of Things' Thing by Kevin Ashton, https://www.rfidjournal.com/articles/view?4986

4. P. Sethi and S. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", Journal of Electrical and Computer Engineering, Volume 2017, Article ID 9324035, 2017, 25 pages DOI:https://doi.org/10.1155/2017/9324035

5. P.P. Ray, "A survey on Internet of Things architectures", Journal of King Saud University - Computer and Information Sciences, Volume 30, Issue 3, July 2018, pages 291-319,

DOI: https://doi.org/10.1016/j.jksuci.2016.10.003

6. https://www.alibabacloud.com/blog/the-building-blocks-of-an-iot-architecture_593731

7. Intel IoT Platform Reference Architecture https://www.intel.in/content/www/in/en/internet-of-things/white-papers/iot-platform-reference-architecture-paper.html

8. IIC: Industrial IoT Reference Architecture

https://iiot-world.com/connected-industry/iic-industrial-iot-reference-architecture/

9. R. Alur, E. Berger, A. W. Drobnis, L. Fix, K. Fu, G. Hager, D. Lopresti, K. Nahrstedt, E. Mynatt, S. Patel, J. Rexford, J. Stankovic and B. Zorn, "Systems Computing Challenges in the Internet of Things", White paper at Computing Community Consortium (CCC), April 2016, arXiv:1604.02980

10. I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises", Business Horizons Journal, Volume 58, Issue 4, July-August 2015, pages 431-440,

DOI: https://doi.org/10.1016/j.bushor.2015.03.008

11. IoT architecture Factsheet
https://www.scribd.com/document/356485436/2InternetofThingsFactsheetArchitecture-pdf

12. A. Gill, V. Behbood, R. Ramadan-Jradi and G. Beydoun, "IoT Architectural Concerns: A Systematic Review", Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing (ICC '17), Article No. 117, Cambridge, United Kingdom, March 2017,

DOI: 10.1145/3018896.3025166

13. M. Díaz, C. Martín and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing", Journal of Network and Computer Applications, Volume 67, Issue C, May 2016, pages 99-117,

DOI:10.1016/j.jnca.2016.01.010

14. O. Uviase and D. Kotonya, "IoT Architectural Framework: Connection and Integration Framework for IoT Systems", D. Pianini and G. Salvaneschi (Eds.): First workshop on Architectures, Languages and Paradigms for IoT EPTCS 264, 2018, pages 1–17, DOI:10.4204/EPTCS.264.1

15. Internet of Things for insights from Connected Devices

https://www.ibm.com/cloud/garage/architectures/iotArchitecture/0_1

16. H. Lin and N. Bergmann, "IoT Privacy and Security Challenges for Smart Home Environments", Information Journal, Special Issue on Preserving Privacy and Security in IoT, Volume 7, Issue 3, Article No. 44,

DOI: https://doi.org/10.3390/info7030044

17. C. Bekara, "Security Issues and Challenges for the IoT-based Smart Grid", Procedia Computer Science, Volume 34, 2014, pages 532-537, DOI: 10.1016/j.procs.2014.07.064

18. IoT Security Reference Architecture

https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf

19. B. Martinez, M. Montón, I. Vilajosana, and J. Daniel Prades, "The Power of Models: Modeling Power Consumption for IoT Devices", IEEE Sensors Journal, 15(10), pages 5777-5789, October 2015, DOI: 10.1109/JSEN.2015.2445094

20. D. Kim, J. Choi and J. Hong, "Evaluating energy efficiency of Internet of Things software architecture based on reusable software components", International Journal of Distributed Sensor Networks, 2017, https://doi.org/10.1177/1550147716682738

21. J. Pan, R. Jain, S. Paul, T. Vu, A. Saifullah and M. Sha, "An Internet of Things Framework for Smart Energy in Buildings: Designs, Prototype, and Experiments", IEEE Internet of Things Journal, 2015, DOI: 10.1109/JIOT.2015.2413397

22. The 54th Issue (Volume 15, Number 2) Special Issue on Advances in IoT Architecture and Systems (AioTAS'17) (5/2018) in ACM SIGBED Review (ISSN: 1551-3688) (Special Interest Group on Embedded System)

http://sigbed.seas.upenn.edu/vol15_num2.html

23. Cloud Customer Architecture for IoT https://www.omg.org/cloud/deliverables/cloud-customer-architecture-for-iot.htm

24. https://www.datascience.com/blog/predictive-analytics-in-industrial-iot

25. Architecture for IoT applications https://medium.com/@maheshwar.ligade/architecture-for-iot-applications-d50ece031d38

26. O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT", IEEE Internet of Things Journal, Volume 5, Issue 2, May 2018, pages 1184-1995,
DOI: 10.1109/JIOT.2018.2812239

27. http://comparch-conf.gatech.edu/iot15/

28. https://techbeacon.com/67-open-source-tools-resources-iot

29. http://iscaconf.org/isca2018/turing_lecture.html

30. https://en.wikipedia.org/wiki/Internet_of_things

31. https://sites.google.com/view/aiotas2018/

32. M. Weiser, R. Gold, and J. S. Brown, "The origins of ubiquitous computing research at PARC in the late 1980s", IBM Systems Journal, Volume 38, Issue 4, December 1999, pages 693-696. DOI: http://dx.doi.org/10.1147/sj.384.0693

33. C. Zavazava, "ITU work on Internet of things", Presentation at Workshop on Scientific Applications for the Internet of Things, at International Centre for Theoretical Physics (ICTP), March 2015. http://wireless.ictp.it/school_2015/presentations/secondweek/ITU-WORK-ON-IOT.pdf

34. https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture

35. K. Zhao and L. Ge, ", A Survey on the Internet of Things Security", 2013 Ninth International Conference on Computational Intelligence and Security, December 2013, pages 663-667
DOI: 10.1109/CIS.2013.145

36. R. Weber, " Internet of things: Privacy issues revisited", Computer Law and Security Review, Journal, Volume 31, Issue 5, October 2015, pages 618-627,
DOI: https://doi.org/10.1016/j.clsr.2015.07.002

37. M. Conti, A. Dehghantanha, K. Franke and S. Watson, " Internet of Things security and forensics: Challenges and Opportunities", Future Generation Computer Systems Journal, Volume 78, Part 2, January 2018, pages 544-546, DOI: https://doi.org/10.1016/j.future.2017.07.060

38. Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao , "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications", IEEE Internet of Things Journal, Volume 4, Issue 5, October 2017, pages 1125-1142, DOI: 10.1109/JIOT.2017.2683200

39. https://www.microsoft.com/en-us/sdl

40. K. Wang, Y. Wang, Y. Sun, S. Guo and J. Wu, "Green Industrial Internet of Things Architecture: An Energy-Efficient Perspective", IEEE Communications Magazine, Volume 54, Issue 12, December 2016, pages 48-54,
DOI: 10.1109/MCOM.2016.1600399CM

41. A. Perles, E. Pérez-Marín, R. Mercado, J. Damian Segrelles, I. Blanquer, M. Zarzo and F. Garcia-Diego, " An energy-efficient internet of things (IoT) architecture for preventive conservation of cultural heritage", Future Generation Computer Systems Journal, Volume 81, April 2018, pages 544-546,
DOI: https://doi.org/10.1016/j.future.2017.06.030

42. N. Kaur and S. Sood, " An Energy-Efficient Architecture for the Internet of Things (IoT)", IEEE Systems Journal, Volume 11, Issue 2, October 2015, pages 796-805,
DOI: 10.1109/JSYST.2015.2469676

43. P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. Leung and Y. Guan, "Wireless energy harvesting for the Internet of Thing", IEEE Communications Magazine, Volume 53, Issue 6, June 2015, pages 102-108, DOI: 10.1109/MCOM.2015.7120024

44. L. Atzori, A. Iera, G. Morabito and M. Nitti, "The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization", Volume 56, Issue 16, November 2012, pages 3594-3608, DOI: https://doi.org/10.1016/j.comnet.2012.07.010

45. http://iot-dsa.org/get-started/download-dsa

46. https://stackoverflow.com/questions/39632667/how-to-kill-the-process-currently-using-a-port-on-localhost-in-windows

47. https://www.youtube.com/watch?v=x3JMquRp6BA

48. http://iot-dsa.org/get-started/how-dsa-works