International Journal of Science and Engineering Applications
Volume 8–Issue 03,93-99, 2019, ISSN:-2319–7560

An Innovative Approach of Big Data and Internet of Things Using 5G Network

Dr. R.K.Bathla
Professor
Department of Computer Science and Engineering
Madhav University, Rajasthan
India

Dr. J. N. Shrivastava
Vice-Chancellor
Manav Bharti University
Solan, Himachal Pradesh
India

Dr. Munish Goyal
Associate Professor
Department of Computer Science and Applications
Manav Bharti University
Solan, Himachal Pradesh
India

Abstract: The Big Data has achieved huge attentiveness from the educational world and the IT industry. In the digital and computing world, in order is produced and composed at velocities that quickly go beyond the boundary range. Presently, over 3 billion people world wide are connected to the Internet, and over 6 billion individuals own movable phones. By 2020, 50 billion devices are expected to be connected to the Internet. At this point, predicted data production will be 44 times greater than that in 2009. As in sequence is transferred and communal at light speed on optic fiber and wireless networks, the volume of data and the speed of market growth increase. On the other hand, the fast growth rate of such large data generates numerous challenges, such as the rapid growth of data, transfer speed, diverse data, and security. Nevertheless, Big Data is still in its immaturity stage, and the area has not been reviewed in general. Hence, this study expansively surveys and classifies the various attributes of Big Data, including its nature, definitions, rapid growth rate, volume, management, analysis, and security. Cloud computing has unlock up new opportunities for testing departments. New technology and social connectivity trends are creating a perfect storm of opportunity, enabling cloud to transform internal operations, Customer associations and industry value chains. To ensure high quality of cloud applications under development, developer must perform testing to examine the quality and accuracy whatever they design. Business consumers are drawn to the clouds simplified, self- service experience and new service capabilities. In this research paper, we speak to a testing ecological architecture with precious key benefits, to execute execution of test cases and used testing methodologies to improve excellence of cloud applications.

Keywords: Big data, Data analytics, Data management, Big data-as-a-service, Analytics-as-a-service, Internet of Things Storage cloud computing,

1. INTRODUCTION

The Internet dissemination endlessly enhances, as additional and supplementary people browse the Web, use email and social network applications to speak with each extra or access wireless multimedia services, such as mobile TV. Furthermore, numerous challenging mobile network services are now accessible, which necessitate increased data rates for specific operations, such as apparatus storage synchronization to cloud computing servers or high resolution video. The rights to use to such a worldwide in sequence and communication infrastructure along with the advances in digital sensors and storage have produced very large amounts of data, such as Internet, sensor, streaming or mobile device data. Additionally, data analysis is the basis for investigations in many fields of knowledge, such as science, engineering or management. Unlike web-based big data, location data is an essential component of mobile big data, which are harnessed to optimize and personalize mobile services. Therefore, an era where data storage and computing become utilities that are ubiquitously available is now introduced. Furthermore, algorithms have been developed to connect data sets and enable more sophisticated analysis. Ever since innovations in data architecture are on our doorstep, the 'big data' paradigm refers to very large and complex data sets (i.e., petabytes and hex bytes of data) that traditional data processing systems are inadequate to capture, store and analyze, seeking to glean intelligence from data and translate it into competitive advantage. As an consequence, big data needs additional computing power and storage provided by cloud computing platforms. In this context, cloud providers, such as IBM, Google, Amazon and Microsoft, provide network-accessible storage cost by the gigabyte-month and calculate cycle's worth by the CPU-hour.

II. BIG DATA: VS IOT

Big data" and "IoT" are scorching terms, and in Information Technology circles, it's hard to speak about one devoid of the other. Yet, regardless of their intimate connection, they are, in fact, two different technology trends. Here we breakdown how big data and Internet of Things are different.[1]

A. Two very different concepts

Big data, as its family name indicates, characterizes enormous amounts of data. But, that's not all. In adding up to volume, IBM data scientists have recognized big data to show variety, velocity and veracity. Big data is a consequence of a variety of sources – social media, selling's, venture content, sensors and mobile devices, among many others. Rapidity refers to the speed at which big data is composed. Each 60 seconds, there are 72 hours of footage uploaded to YouTube, 216,000 Instagram posts and 204 million emails sent. In regards to veracity, the data collected needs to be of good quality that is continuously updated in real-time. Analyzing big data can offer superior value to the companies and individuals who use it. The Internet of Things (IoT), on the other hand, turns day by day "things" into smart objects. Fridges, watches, thermostats, cars, shipping containers, are prepared with sensors that attach to the Internet and each other to collect and transmit data. This information can become big data when it is shared with information from other sources and meets the other measurements defined above.[2]

B. Diverse time sequencing

Big data is paying attention on the long-game. Big data bring together enormous amounts of data, but it doesn't influence the information to make real-time decisions. Instead, there is more often than not a lag between when the data is collected and when the data is analyzed. For IoT, time is of the essence. It collects and uses data in real-time to optimize operations; become aware of security breaches, correct malfunction and more. IoT data analytics must include administration real-time streaming data, and making real-time analytics and real-time decisions "at the edge" of the network, says Bill Schmarzo, CTO for Dell EMC Services' Big Data Practice. Streaming data management must have the ability to ingest, combined (mean, median, mode) and compress real-time data from sensor devices at the edge. Edge analytics would robotically analyze real-time sensor data and render real-time decisions (actions) that optimize operational performance (blade angle or yaw) or would flag unusual performance or behaviors for instantaneous investigation (security breaches, fraud detection)

C. Diverging Investigative goals

Big data scrutinize regularly human-generated data in the recreation of discovery prototype in human behaviors and movement. To ensure confidence in any human-related patterns, an hard to believe amount of data from multiple sources over longer periods of time is required. This give details the longer lead time required for big data. It is for this reason that big data is used for long-term projects like projecting maintenance, capacity planning, customer 360 and revenue protection. On the contradictory spectrum, IoT aggregates and compresses machine-produce data from a mixture of sensors that include RFIDs, fitness trackers, virtual reality devices, smart air purifiers and every other smart device. The ambition in collecting this data through effective IoT device management is to track and monitor assets and be able to correct problems in real-time. For example, the sensors in a smart garbage container will indicate when it is near capacity. This knowledge is then used to schedule a garbage collector to empty the bin. Big data and IoT are different, but they are intricately linked. Used in racing bike, IoT delivers the information from which big data analytics can sketch the information to create the obligatory insights – helping businesses not only react to problems as they occur, but forecast them and fix them ahead of time.

III. IoT HISTORY

Internet of things from the 1832 can see the different landmark of Electronics and telecommunication. I would like to recall the history of telecommunication and internet from the article History of IoT, that was written on Post capes (2016), catalogs following milestones 1832: An electromagnetic telegraph was created by Baron Schilling from Russia 1844: Samuel Morse sends first Morse code public message 1926: Nikola Tesla to Colliers magazine: "When wireless*1 is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket."

1964: Marshall McLuhan "....by means of electric media, we set up a dynamic by which all previous technologies -- including cities -- will be translated into information systems"
1969: ARPANET developed
1974: TCP/IP started
1989: Tim Berners-Lee proposes World Wide Web
1990: Toaster was created by John Romkey 1
1991: First web page 1995: First e-commerce service started (Amazon, Echo Bay or eBay). 1998: Google integrated.
1998: Mark Weiser: "Ubiquitous computing is approximately the opposite of virtual reality," Weiser wrote "Where virtual reality puts people inside a computer-generated world, ubiquitous computing forces the computer to live out here in the world with people."
1999: The internet of things not precisely exact but the concept was introduced. The Auto-ID Centre Kevin Ashton described Internet of things "I could be wrong, but I am moderately sure the phrase "Internet of

Things" started life as the title of a presentation I made at Proctor & Gamble (P&G) in 1999.Linking the new idea of RFID in P&G's supply chain to the then-red-hot topic of the Internet was more than just a good way to get executive attention. It summed up an important approaching which is still often misunderstood."

Fig:1 An IOT Analytics system with Matlab

2000 to 2004: The term Internet of things or connected word that was remained in Guardian and other Scientific American magazines. There were some discussions about in near future devices that will automatically connect and works independently with very less instructions. When RFID developed on massive scale then the concept of IoT is becoming more and clearer.

2005: Then in 2005 after previous terms become visible in protector and other systematic publications the term starts to gain more popularity so the ITU (International Telecommunication Union) and the first report is published: "A new measurement has been added to the world of in sequence and communiqué technologies (ICTs): from anytime, anyplace connectivity for anyone, we will now have connectivity for anything. Connections will multiply and generate an completely new dynamic network of networks – an Internet of Things"

2006-2008: European Union recognized the Internet of things term in a consultation that was held IPSO alliance (members are: Ericsson, Google, Cisco, SAP, Sun, Fujitsu and Bosch, Intel) opened for study to promote the IP network of smart object and to empower IoT. (IPSO alliance.)[4]

2011: IPv6 was launched After 2011 the big companies like Cisco, Ericsson, IBM produces large educational and promotion intuitive on IoT or other related terms. We can divide internet of things into many stages I have drawn a figure that illustrated the timeline and growth of internet of things.

The time duration is indicated from 2004 to 2018.So the IoT is coming with huge possibilities and challenges for the business and all aspects of the life. The popularity is marked between 0 to 120 where value of 60 means half as popular. Today the google trends IoT popularity worldwide is around 80% so it is very popular and its becoming more popular as the concept is coming to reality. The top five countries that is are more interested are South Korea, St. Helena, Japan, Singapore, Taiwan, Finland is at 21st place as of today about IoT term reputation search on Google.

IV. HOW 5G DIFFERS FROM 3G AND 4G

5G is not merely a supplementary room of 3G and 4G. Instead, it is a transformative ecological unit that includes a heterogeneous network that integrates 4G, Wi-Fi, millimeter wave, and other wireless access technologies. It merge cloud transportation, a virtualized network core, intelligent edge services, and a scattered computing model that derives insight from the data generated by billions of devices. According to Asha Keddy, Vice President in the Platform Engineering Group and General Manager of Next Generation and Standards at Intel, "5G is much more than a G. It is much more transformative. With 5G, we will be moving from a user centric world to one of massive machine type communications where the set of connections will move from enabling millions to billions of devices—an era that will connect these devices intelligently and usher in the commoditization of information and intelligence."5 The promising group capitalizes on a mixture of interfaces across licensed, licensed shared, and unlicensed spectrum in low-, mid-, and high-frequency bands. By design, it will not only increase capacity, it also will enable even the smallest devices to perform high-level working out and connect quickly to processing power that is diffused throughout the system.6 It is imperative to note that 5G is an end-to-end system that shifts communications to a computing platform. 5G symbolize a development from a point-to-point system to one that senses data from billions of devices and works to move those communication packets seamlessly to the right device, using the suitable processing platform. Four factors differentiate 5G from its predecessors: connected devices, fast and intelligent networks, back-end services, and extremely low latency. These qualities enable a fully connected and interactive world with a variety of applications. This includes enhanced mobile broadband, machine-to-machine communications, artificial intelligence, and highly developed digital services

A. 50 billion devices and 212 billion sensors

By 2020, the 5G network is expected to support 50 billion connected devices and 212 billion connected sensors as well as enable access to 44 zettabytes (ZB) of data.7 This will range from smart phones and tablets to smart watches, cars, machinery, appliances, and remote monitoring devices.8 All of these will generate a massive amount of "useful data" that can be analyzed. Indeed, researchers estimate that this connected ecosystem will make it possible to utilize a much larger percent of digital data (35 percent) than before (5 percent).

B. Fast, intelligent networks

High broadband speeds and intelligent networks will characterize the 5G network. Currently, it takes about eight minutes to download a feature movie using 4G; people will be able to do this in less than five seconds with 5G.10 The speed of the network will enable applications such as social gaming, interactive television, high definition and 3-D video, virtual reality, robotics, driverless cars, and advanced manufacturing, among others.

C. Back-end services

The up-and-coming network will enlist back-end data centers, cloud services, and remote file servers into a computational behemoth. There will be “computing at the edge,” which means that computations can be performed near the source or in the cloud, depending on the immediate need. These 5G innovations will allow applications to quickly process content and provide an experience that is very responsive. This will make computing more economical, more efficient, and we’ll see savings on storage costs. At the same time, as devices make their way into the hands of users, data center network infrastructure and cloud services are evolving to meet the needs of new business. Systems will be optimized so that software can perform difficult tasks and network functions unfettered from physical hardware. That increases network agility, and allows for rapid and customized configurations.

D. Low latency

Latency refers to the time among when people request that a computing command be executed and the actual implementation of that task. In today’s mobile world, execution takes place in around 50 to 80 milliseconds. That is a sufficient amount of time for voice, email, and web surfing, which is the bulk of current usage.

Fig:2. 5G Network

V. BIG DATA SPECIFICATIONS

A. Information Increase Rapidly

The rate of 10x every five years [6]. From 1986 to 2007, the international aptitude for hi-tech data storage, computation, handing out, and communication were tracked through 60 analogues and digital technologies in 2007, the capacity for storage in general-purpose computers was 2.9 × 1020 bytes (optimally compressed) and that for communication was 2.0 × 1021 bytes. These computers could also provide accommodation 6.4 × 1018 instructions per second. However, the computing volume of general-purpose computers increases annually at a rate of 58%. In computational sciences, Big Data is a weighty issue that requires serious attention. Thus far, the indispensable landscapes of Big Data have not been unified. Furthermore, Big Data cannot be procedure using existing technologies and methods. Therefore the generation of incalculable data by the fields of science, business, and society is a global problem. With respect to data analytics, for example, procedures and average tools have not been planned to explore and analyze large datasets. As a result, associations come across early challenges in creating, managing, and manipulating large datasets. Systems of data duplication have also displayed some security weaknesses with respect to the creation of multiple copies, data governance, and policy. These policies define the data that are accumulate analyzed, and accessed. They also determine the weight of these data. To process shapeless data sources in Big Data projects, concerns regarding the scalability, low latency, and performance of data road and rail networks and their data centers must be addressed. In the IT industry as a whole, the rapid rise of Big Data has engendered new issues and challenges with respect to data management and analysis. Five common issues are volume, variety, velocity, value, and complexity according to in this study, there are additional issues related to data, such as the fast growth of volume, variety, value, management, and security. Each issue represents a serious problem of technical research that requires discussion. Hence, this research proposes a data life cycle that uses the technologies and terminologies of Big Data. Future research directions in this field are determined based on opportunities and several open issues in Big Data domination. This groups the critical issues in Big Data into three categories based on the commonality of the challenge.

B. Volume of Big Data

The volume of Big Data is characteristically large. However, it does not require a convinced amount of petabytes. The increase in the volume of various data records is naturally managed by purchasing additional online storage; however, the virtual value of each data point decreases in proportion to aspects such as age, type, quantity, and richness. Thus, such expenses are unreasonable (Doug, 212). The following two subsections detail the volume of Big Data in relation to the rapid growth of data and the development rate of hard disk drives (HDDs). It also examines Big Data in the present atmosphere of endeavor and technologies.[8]

C. Swift Growth of Data

The data type that increases most speedily is shapeless data. This data type is distinguish by "human information" such as high-definition videos, movies, photos, scientific simulations, financial transactions, phone records, genomic datasets, seismic images, geospatial maps, e-mail, tweets, Face book data, call-center conversations, mobile phone calls, website clicks, documents, sensor data, telemetry, medical records and images, climatology and weather records, log files, and text. According to Computer World, formless information may account for more than 70% to 80%of all data in organizations. These data, which mostly originate from social media, constitute 80% of the data worldwide and account for 95% of Big Data. Currently, 87% of IT managers process unstructured data, and this percentage is expected to drop by 47% in the near future. Most shapeless data are not modeled, are random, and are difficult to analyze. For many organizations, appropriate strategies must be developed to manage such data. Table 1 describes the rapid production of data in various organizations further. According to Industrial Development Corporation (IDC) and EMC Corporation, the amount of data generated in 2020 will be 47 times greater [40 zetta bytes (ZB)] than in 2009. This rate of increase is expected to persist at 55% to 65% annually. To store the increased amount of data, HDDs must have large storage capacities. Therefore, the following section investigates the development rate of HDDs C. Development Rate of Hard Disk Drives (HDDs).
The demand for digital storage is highly elastic. It cannot be completely met and is controlled only by budgets and management capability and capacity. Goda et al. (2002) and discuss the history of storage devices, starting with magnetic tapes and disks and optical, solid-state, and electromechanical devices. Prior to the digital revolution, information was predominantly stored in analogue videotapes according to the available bits. As of 2007, however, most data are stored in HDDs (52%), followed by optical storage (28%) and digital tapes (roughly 11%). Paper-based storage has dwindled 0.33% in 1986 to 0.007% in 2007, although its capacity has steadily increased (from 8.7 optimally compressed PB to 19.4 optimally compressed PB). Although the topic of IoT security is gaining increasing traction in the networking community, we believe that some important research challenges related to the field still remain substantially unexplored. We summarize and discuss the challenges below, hoping that the following roadmap will eventually stimulate discussion and further research and development in the IoT research community at large.

VI. RESEARCH CHALLENGES IN IOT

A. Toward Secure-by-design IoT Systems

The most important takeaway from the previous discussion is that, as yet, IoT security has been so far approached in an ad-hoc fashion, where countermeasures are not planned for beforehand but instead temporary measures (i.e., "patches") are put in place when an attack is discovered. Considering that the IoT will work at a scale in the order of billions of devices, these patches are not adequate to address the need of homogeneous, standard, widely-adopted security procedures. Our vision is the following. We believe that the complexity and the scale of the IoT require the enactment of a novel, holistic approach to IoT security, where security is approached in a proactive fashion and threats are addressed in a scalable and reliable manner. The IoT technology landscape of today is too complex and disruptive for security to be more than a set of loosely-integrated solutions. On the contrary, security must be deeply embedded in every stage of the production cycle, from product design to development and deployment. Too often, security tends to be an afterthought in development, and while there are exceptions, in many cases economic drivers or lack of awareness of the risks cause businesses to push IoT devices to market with little regard for their security. For these reasons, the concept of security-by-design should be a main driving force in future IoT security research. The secure-by-design approach to IoT security offers several advantages with respect to previous paradigms. First, it provides a framework that abstracts from the specific security threat and tackles classes of problems, rather than a series of specific threats. Second, it stimulates IoT system designers to be proactive in considering security, and to come up with a security design plan that formalizes and addresses threats before their device/technology is released on the market. Third, it is flexible and scalable, since the control and learning modules can be designed and implemented both at the device and the system level to address different security threats, as we will discuss later. Although the secure-by-design approach provides advantages, it also comes with novel and exciting technical challenges. We recognize two main research challenges toward the implementation of our IoT security framework, which are summarized below.

B. Learning to Detect and Mitigate IoT Security Threats.

In every control and learning problem, the inputs and the state of the system must be properly modeled and formalized. This aspect is significantly challenging in the context of the IoT, as devices may generate significantly heterogeneous data (i.e., multimedia, text, sensory). After modeling states and inputs, it is necessary to design mechanisms able to detect and mitigate threats based on the current state and input. This implies that the characterization of "good" and "bad" states has to be factored into the mechanism design.

C. Design of Polymorphic Hardware and Software Modules to Enact Mitigation

When a threat has been detected, it is necessary to enact countermeasures so as to swiftly mitigate the effect of the ongoing attack. This critical aspect requires the design of hardware and software modules able to "polymorphically" adapt to different requirements and thus swiftly put in action the necessary counterattack strategies.

D. Existing Work on Machine Learning and Software defined Networking for IoT Security

Although ML can be considered a mature field, few works have applied ML techniques to solve issues related to IoT security. Recently, Zhang et al. have proposed a framework [18] to detect and mitigate cross-layer wireless attacks based on the application of Bayesian learning [184]. Specifically, the framework establishes a probabilistic relation between an hypothesis (i.e., the attack is likely taking place) and the supporting evidence (i.e., there are signs of attack activities). This allows to update the hypothesis dynamically when new evidence is available. Therefore, the more evidence is gathered, the more accurate is the resulting hypothesis. The authors demonstrate through experiments and simulations that even small-scale malicious activities can still be detected with high confidence, as long as enough evidence is accumulated.[6]

E. Explore the Use of Reinforcement Learning

An area that is yet to be explored is the opportunity of leveraging unsupervised learning to implement secure-bydesign IoT systems. Specifically, reinforcement learning (RL), which is ML inspired by behaviourist psychology, deals with how agents ought to take actions in an environment so as to maximize a cumulative reward. The problem, due to its generality, is studied in many other disciplines, such as game theory, control theory, operations research, information theory, simulation-based optimization, multi-agent systems, swarm intelligence, statistics and genetic algorithms, among others . The advantage of RL for the IoT context is that there is no need for training or datasets, as the nodes can learn by themselves what is the right strategy to achieve the maximum reward according to the current state.

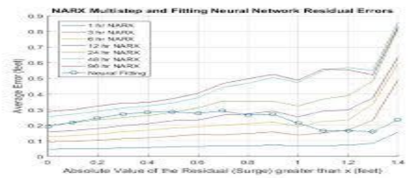

Fig:2 An IOT Analytics system with Matlab

F. Blockchain for Decentralized IoT Security

Although being originally designed to store and validate cryptocurrency transactions, the blockchain has recently attracted much in the IoT networking research community to address scalability and security problems.The blockchain technology relies on decentralized, and thus scalable, consensus mechanisms that check, verify and store transactions in the blockchain while guaranteeing protection against data tampering attacks.

VII. CONCLUSION

The IoT is revolutionizing the world around us by empowering every device, object and person to be connected to the Internet. With such massive presence of interconnected things deployed all around us, and in some cases inside us, the IoT offers exciting yet significant security research challenges that need to be addressed in the upcoming years. In this paper, we have provided our novel perspective on the issue of IoT security, which is based on a unique mixture of the notions of security-by-design, polymorphism, and software-defined networking. We have categorized and summarized the relevant state-of-the-art research, and proposed a roadmap of future research issues. We hope that this work will inspire fellow researchers to investigate topics pertaining to IoT security and keep on the race for a more secure technological world.

REFERENCES

[1]. Vakintis, I., Panagiotakis, S., Mastorakis, G., Mavromoustakis, C.X.: Evaluation of a Web Crowd-sensing IoT ecosystem providing big data analysis. In: Pop, F., Kołodziej, J., di Martino, B. (eds.) Resource Management for Big Data Platforms and Applications. Studies in Big Data Springer International Publishing, 2017.

[2]. Park, K., Nguyen, M.C., Won, H.: Web-based collaborative big data analytics on big data as a service platform. In: Proceedings of the 2015 17th International Conference on Advanced

Communication Technology (ICACT), Seoul, pp. 564–567 (2015)

[3]. J. M. Borwein and A. S. Lewis, Convex analysis and nonlinear optimization: Theory and examples, CMS books in Mathematics, Canadian Mathematical Society, 2000.

[4]. J. Basilico and T. Hofmann, Unifying collaborative and content-based _ltering, Proc. Intl. Conf. Machine Learning (New York, NY), ACM Press, 2004

[5]. Lijuan Cai and T. Hofmann, Hierarchical document categorization with support vector machines, Proceedings of the Thirteenth ACM conference on Information and knowledge management (New York, NY, USA), ACM Press, 2004

[6]. J. D. La_erty, A. McCallum, and F. Pereira, Conditional random _elds: Probabilistic modeling for segmenting and labeling sequence data, Proceedings of International Conference on Machine Learning (San Francisco, CA), vol. 18, Morgan Kaufmann, 2001

[7]. N. Ratli_, J. Bagnell, and M. Zinkevich, Maximum margin planning, International Conference on Machine Learning, July 2006.

[8]. IOS Press. (2011). Guidelines on security and privacy in public cloud computing. *Journal of E-Governance, 34* 149-151. DOI: 10.3233/GOV-2011-0271

[9]. Park, K., Nguyen, M.C., Won, H.: Web-based collaborative big data analytics on big data as a service platform. In: Proceedings of the 2015 17th International Conference on Advanced Communication Technology (ICACT), Seoul, pp. 564–567 (2015)

[10]. Agneeswaran VS, Tonpay P, Tiwary J (2013) Paradigms for realizing machine learning algorithms. Big Data 1(4):207–214

[11]. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I.: Cloud computing and emerg ing IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Gener. Comput. Syst. 25, 599–616 (2009)

[12]. T. He, J. Stankovic, C. Lu and T. Abdelzaher, A Spatiotemporal Communication Protocol for Wireless Sensor Networks, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 16, No. 10, Oct. 2005, pp. 995-1006.

[13]. M. Huang, J. Li, X. Song, and H. Guo, Modeling Impulsive Injections of Insulin: Towards Artificial Pancreas. *SIAM Journal of Applied Mathematics 72*, 5, 2012, pp. 1524–1548.

[14]. M. Kay, E. Choe, J. Shepherd, B. Greenstein, N. Watson, S. Consolvo, and J. Kientz, Lullaby: a Capture & Access System for Understanding the Sleep Environment. *UbiComp*, 2012.

[15]. A Liu, and D. Salvucci, Modeling and Prediction of Human Driver Behavior, *Intl. Conference on HCI* , 2001.

[16]. J. Lu, T. Sookoor, V. Srinivasan, G. Gao, B. Holben J. Stankovic, E. Field, and K. Whitehouse, The Smart Thermostat: Using Occupancy Sensors to Save Energy in Homes, *ACM SenSys*, 2010.

[17]. M. Maroti, B. Kusy, G. Simon, and A. Ledeczi, The Flooding Time Synchronization Protocol, *ACM SenSys*, November 2004.

[18]. S. Mohammed, P. Fraisse, D. Guiraud, P. Poignet, and H. Makssoud, Towards a Co-contraction Muscle Control strategy for Paraplegics. *CDC-ECC*, 2005.

[19]. S. Munir, J. Stankovic, C. Liang, and S. Lin, New Cyber Physical System Challenges for Human-in-the-Loop Control, *8th International Workshop on Feedback Computing*, June 2013.