WIRELESS SENSORS INTEGRATION INTO INTERNET OF THINGS AND THE SECURITY PRIMITIVES

Muhammad A. Iqbal and Dr. Magdy Bayoumi

The Center for Advanced Computer Studies, University of Louisiana at Lafayette, Lafayette, LA 70504 USA
mxi1678@cacs.louisiana.edu, mab@cacs.louisiana.edu

ABSTRACT

The common vision of smart systems today, is by and large associated with one single concept, the internet of things (IoT), where the whole physical infrastructure is linked with intelligent monitoring and communication technologies through the use of wireless sensors. In such an intelligent vibrant system, sensors are connected to send useful information and control instructions via distributed sensor networks. Wireless sensors have an easy deployment and better flexibility of devices contrary to wired setup. With the rapid technological development of sensors, wireless sensor networks (WSNs) will become the key technology for IoT and an invaluable resource for realizing the vision of Internet of things (IoT) paradigm. It is also important to consider whether the sensors of a WSN should be completely integrated into IoT or not. New security challenges arise when heterogeneous sensors are integrated into the IoT. Security needs to be considered at a global perspective, not just at a local scale. This paper gives an overview of sensor integration into IoT, some major security challenges and also a number of security primitives that can be taken to protect their data over the internet.

KEYWORDS

Internet of Things (IoT), Wireless Sensor Network (WSN), Security, Privacy, Integration, Confidentiality

1. INTRODUCTION AND RELATED WORK

Today, Internet of things (IoT) itself has become a thing – a thing worth talking about, from the university project discussions to conferences to giant tech companies' meetings. IoT is being identified as one of the top emerging future technologies. The concept is simple at its core; connecting devices over the internet: making them 'smart'. We can think of it as the internet expanding from being a network of computers to a network of both computers and things. This idea is not even new, indeed first 'thing' connected to internet was a Coke vending machine by Carnegie Mellon University students in 1982. What is new added into this concept, are the sensors - tiny sensors embedded in devices that can gather almost any kind of information about their surrounding environment (temperature, light, sound, time, movement, speed, distance, and more).

The term internet of things was devised by Kevin Ashton in 1999, co-founder and executive director of Auto-ID Center at MIT and refers to uniquely identifiable objects and their virtual

Dhinaharan Nagamalai et al. (Eds) : ICCSEA, SPPR, UBIC - 2016
pp. 59–67, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.61106

representations in an "internet-like" structure. With the advancement in technology, the cost of sensors, processors and transmitters is becoming less and their computational and processing powers becoming higher, allowing putting them into any object of our day-to-day life i.e. the food, the clothes, the medicines and so on. The technological advances also enhance this connectivity by adding one more dimension to it - connecting anything. Just to give an example, Nike has recently introduced a new line of running shoes that can track its wearer's progress and post updates online. The age of so called 'smart dust', which we have been talking about for years now, is finally upon us after the development of a fully functional computer with built-in wireless connectivity measuring just one cubic mm [2]. There is even a tree in Brussels, Belgium packed with sensors and cameras that constantly posts local environmental updates on Twitter. And that tree has 3,000 followers, how many people on Twitter can say they have 3,000 followers? At least I can't [2].

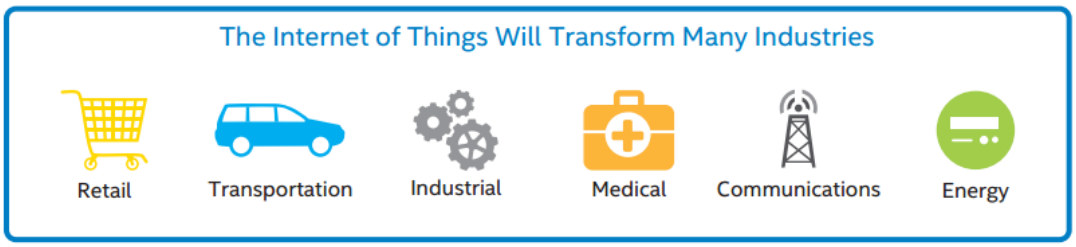

Figure 1. Internet of things Applications [14]

It is estimated that the number of connected devices is expected to grow exponentially to 50 billion by 2020 by Cisco. Intel, more optimistically, predicts 200 billion by that same year. The main driver for this growth is not human population; rather, the fact that devices we use in our daily life (e.g., refrigerators, cars, fans, lights) and operational technologies such as those found on the factory floor are becoming connected entities across the globe. This world of interconnected things - where the humans are interacting with the machines and machines are talking with other machines (M2M) — is here and it is here to stay [13].

An interesting trend contributing to the growth of IoT is shift from the consumer-based IPv4 Internet of tablets and laptops, that is, IT to Operational Technology (OT) based IPv6 Internet of M2M interactions. This includes sensors, smart objects and clustered systems (for example, Smart Grid). IPv6 is new enabling technology, an upgrade to the Internet's original fundamental protocol – the Internet Protocol (IP), which supports all communications on the Internet. IPv6 is necessary because the Internet is running out of original IPv4 addresses. Key challenge here is to make IPv6 interoperable for the most IoT software developed for IPv4 and readily available. Many experts believe, however, that IPv6 is the best connectivity option and will allow IoT to reach its potential.

Challenges that need to be addressed include how to communicate effectively and securely between devices, how to transmit and store huge amounts of data, and how to protect the privacy. A major barrier to realizing the full promise of IoT is that around 85% of existing things were not designed to connect to the Internet and cannot share data with the cloud [4]. Addressing this issue, gateways from mobile, home, and industry playing the part to act as intermediaries between legacy things and the cloud, not only providing the required connectivity but also security and the manageability [14] as shown in figure 2.

The things to be connected to the Internet largely vary in terms of characteristics. This ranges from very small and static devices (e.g., RFIDs) to large and mobile devices (e.g., vehicles). Such

heterogeneity induces complexity and stipulates the presence of an advanced middleware that can mask this heterogeneity and promote transparency. Among other technologies, radio

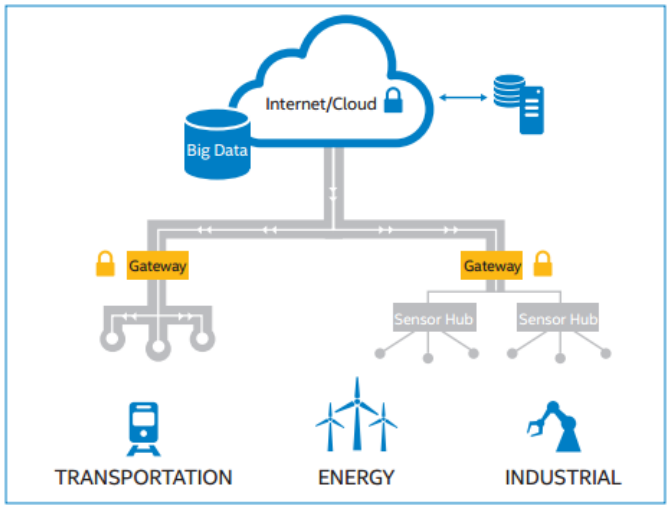

Figure 2. Addressing Endless Use Cases and Gateways [14]

frequency identification (RFID) and wireless sensor network (WSN) represent two of the most promising technologies enabling the implementation of IoT infrastructure. RFID is a low-cost, low-power technology consisting of passive or battery-assisted passive devices (tags) that are able to transmit data when powered by the electromagnetic field generated by an interrogator (reader). Since passive RFID tags do not need a source of energy to operate, their lifetime can be measured in decades, thus making the RFID technology well suited in a variety of application scenarios, including the industrial and healthcare ones [4]. The main challenges for RFID are non-uniform encoding, conflict collision and RFID privacy protection.

On the other hand, WSNs are basically self-organizing ad hoc networks of small, cost-effective devices (motes) that communicate/cooperate in a multi-hop fashion to provide monitor and control functionalities in critical applications including industrial, military, home, automotive, and healthcare scenarios. Currently, most WSN motes are battery-powered computing platforms integrating analogue/digital sensors and an IEEE 802.15.4 radio enabling up to 100m outdoor communication range (single hop). Unlike other networks, WSNs have the particular characteristic of collecting sensed data (temperature, motion, pressure, fire detection, voltage/current, etc) and forwarding it to the base station or gateway. Even though most WSN protocols were not designed for two-way communications as illustrated in IMS research, they should also be able to receive information and send it to the sensors (a command for example), and react on behalf of the commander/user, e.g., automating home appliances.

2. SENSOR NETWORKS IN A GLOBALLY CONNECTED NETWORK

Integration of Wireless Sensor Networks (WSN) into IoT is not mere speculation, a number of big technology companies supporting and developing their IoT infrastructure around WSN. Noteworthy examples are IBM's 'A Smarter Planet', a strategy considers sensors as fundamental pillars in intelligent water management systems and intelligent cities; and the CeNSE project by HP Labs, focused on the deployment of a worldwide sensor network in order to create a "central nervous system for the Earth" [11].

The question how sensor nodes should provide their services when connecting WSN to the Internet is important; either directly or through the base station. The 'thing' connected to Internet is required to be locatable and addressable via the Internet, but this particular configuration might not be suitable for certain scenarios. Some specific scenarios for instance, in SCADA systems a sensor node does not need to provide its services directly and other scenarios are where a sensor node should be completely integrated into the Internet.

There are different approaches in which WSNs are integrated into IoT depending upon the application requirements and already deployed WSNs infrastructure. Some of these approaches are described below:

- Completely independent from internet where WSN has its own protocol and sensor nodes communicate through a centralized device called base station. Any query coming from internet host is traversed through base station that collects and holds all data from sensor nodes. If base station acts as applications layer gateway, then Internet hosts and sensor nodes able to address each other and exchange information without establishing a true direct connection. WSN still independent of internet, all queries go through gateway.

- Sensor nodes implement TCP/IP stack (or a compatible set of protocols such as 6LoWPAN) so that any internet host can have direct communication with them & vice versa. Sensor nodes are no longer to use specific WSN protocols.

- There's another topology based integration approach in which level of integration depends on actual location of the nodes, nodes can be dual sensors (base stations) located on the root of the WSN or full-fledged backbone of devices that allow sensing nodes to access Internet in one-hop (access point). WSN becomes unbalanced tree with multiple roots, leaves are normal sensors nodes and other elements are internet-enabled nodes.

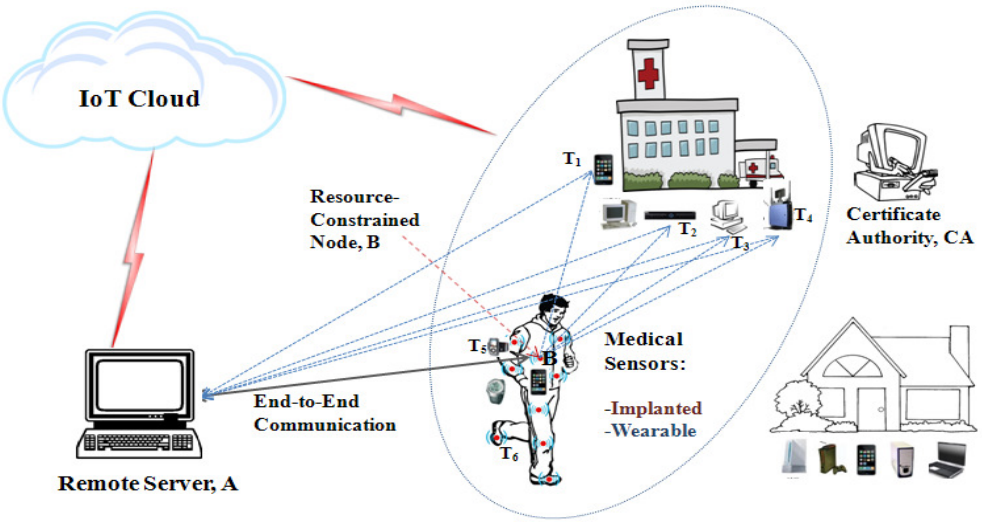

Figure 3. Typical Body Area Network Scenario in context of IoT

The evolution of the IoT has its origin in the convergence of wireless technologies, advancements of MEMS and digital electronics where as a result miniature devices with the ability to sense and compute are communicating wirelessly. However, having IP connectivity does not mean that every sensor node should be directly connected to the Internet. There are many challenges that must be carefully considered, and one of those challenges is security [11]. In the era of IoT, the

interaction or relationship between humans and machines needs to be considered more seriously as machines getting smarter and starting to handle more human tasks. A thing might be a patient with a medical implant to facilitate real-time monitoring in a healthcare application or an accelerometer for movement attached to the cow in a farm environment. In such a situation, humans are required to trust the machines and feel safe about it [10].

3. IOT SECURITY AND PRIVACY

IoT applications projections predict a safer, smarter and efficient world while some observers show concerns that it would be a darker world of surveillance, privacy and security violations, and consumer lock–in. The scale and context of the IoT make it a compelling target for those who would do harm to companies, organizations, nations, and more importantly people. With continued adoption of IP networks, IoT applications have already become a target for attacks that will continue to grow in both magnitude and sophistication. The interconnected nature of IoT devices means that every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally. The weakest link defines the overall level of security of the whole infrastructure. This challenge is amplified by other considerations like the mass-scale deployment of homogenous IoT devices, the ability of some devices to automatically connect to other devices, and the likelihood of fielding these devices in unsecure environments.
IoT presents new challenges to network and security architects. Smarter security systems that include managed threat detection, anomaly detection, and predictive analysis need to evolve [13]. There are various challenges to design security solutions in the IoT because of network characteristics e.g., device heterogeneity, resource constraints, unreliable communication links and the distributed nature. In traditional TCP/IP networks, security is built to protect the confidentiality, integrity and availability of network data. It makes the system reliable and protects the system from malicious attacks which can lead to malfunctioning systems and information disclosure. The IoT requires multi-facet security solutions where the communication is secured with confidentiality, integrity, and authentication services; the network is protected against intrusions and disruptions; and the sensor node as in WSN, additional security protection requirements and user privacy are imposed depending on the application scenario.

With IPv6 there are enough IP addresses to connect billions of ‘things’ to form our new IoT world but whether these things would be secured enough to ensure individual privacy rights and secure the systems from malicious attacks? The cryptographic algorithms are required to be highly efficient, low power, low energy realizations especially for battery operated or passively powered devices. In many practical applications, the gateway needs to send periodic control messages, notifications, and sensitive confidential data to all the wearable devices where a common secret key is required to encrypt the broadcast messages. Symmetric key cryptography such as AES provides fast and lightweight encryption/decryption on such smart devices and their integrated hardware supports it as well. However, when this number of connected devices becomes high, exchanging symmetric keys becomes infeasible and the need to have an efficient scalable key establishment protocol becomes critical. Another approach is to distribute keys by asymmetric key cryptography but it requires high computational costs; the main concern for resource-constrained devices [16]. Therefore, conventional security primitives cannot be applied due to the heterogeneous nature of sensors (either implanted, on-body or wearable), low resources and the system architecture of IoT based healthcare systems [3].

4. IOT SECURITY PRIMITIVES

Devices will only be smart if they include technology to provide security and privacy. Poorly secured IoT devices could serve as entry points for cyber-attack by allowing malicious

individuals to re-program a device or cause it to malfunction. Moreover, unique to cryptographic implementations is that they also need protection against physical tampering either active or passive. This means that countermeasures need to be included during the design process. Security in the IoT must ensure secrecy and integrity of communication, as well as the authenticity of messages being exchanged.

From the end-user's perspective, it is not possible to easily modify these smart devices; security primitives must be pre-embedded into the system. The integration of sensors in the Internet must ensure the interoperability, transparency and flexibility. However, sensor nodes inherently have constrained resources; small batteries are typically the main energy sources for these sensor nodes with the requirement to operate for longer durations [17]. Hence, energy efficiency becomes an important factor besides security and privacy issues.

Different approaches are being employed for secure E2E communication in WSNs and IoT, they can be classified into major research directions as follows

- Centralized Approaches
- Protocol-based Extensions and Optimizations
- Alternative Delegation Architectures
- Solutions that Require Special Purpose Hardware Modules

It is also important to understand the attack techniques in order to rationalize security mechanisms in communication protocols. Some important attacks with respect to IoT are

- Eavesdropping: process of overhearing an ongoing communication, that is as well preliminary for launching next attacks. In wireless communication, everyone has in general access to the medium so takes less effort to launch as compared to wired communication. Confidentiality is a typical counter-measurement against eavesdropping but if keying material is not exchanged in secure manner, eavesdropper could compromise the confidentiality. Secure key exchange algorithms such as Diffe-Hellman (DH) are used.

- Impersonation: a malicious party pretends to be a legitimate entity for instance by replaying a generic message, in order to bypass the aforementioned security goals.

- MITM Attack: Man-in-the-middle attack takes place when a malicious entity is on the network path of two genuine entities. Capable of delaying, modifying or dropping messages. Interesting within the context of PKC, malicious entity doesn't attempt to break the keys of involved parties but rather to become the falsely trusted MITM.

- DoS Attack: targets the availability of a system that offers services, is achieved by exhaustingly consuming resources at the victim so that the offered services become unavailable to legitimate entities. A common way to launch this attack is to trigger expensive operations at the victim that consume resources such as computational power, memory bandwidth or energy. This attack is critical for constrained devices where existing resources are already scarce.

Conventional security primitives cannot be applied due to the heterogeneous nature of sensors, low resources and the system architecture of IoT based systems. Any unauthorized use of data or privacy concerns may restrict people to utilize IoT-based applications. To mitigate these security and privacy threats, strong network security infrastructures are required. Peer authentication and

End-to-End data protection are crucial requirements to prevent eavesdropping on sensitive data or malicious triggering of harmful actuating tasks [15].

Some other security primitives worth consideration are:

- Securing device identity and mechanisms to authenticate it. IoT devices may not have the required compute power, memory or storage to support the current authentication protocols. Therefore, authentication and authorization will require appropriate re-engineering to accommodate our new IoT connected world.

- Protection of the initial configuration and provisioning of devices from tampering, theft and other forms of compromise throughout its usable life, which in many cases can be years.

- Application of geographic location and privacy levels to data

- Strong identities

- Strengthening of other network-centric methods such as the Domain Name System (DNS) with DNSSEC and the DHCP to prevent attacks

- Adoption of other protocols that are more tolerant to delay or transient connectivity (such as Delay Tolerant Networks)

- Lastly, the communication and the data transport channels should be secured to allow devices to send and collect data to and from the agents and the data collection systems. While not all IoT endpoints may have bi-directional communications, leveraging SMS (automatically or via a network administrator) allows secure communication with the device when an action needs to be taken [12].

Data Privacy is another important challenge; privacy fears stemming from the potential misuse of IoT data have captured public attention. There are various questions to be answered: Who owns the data? How a user can be sure that this data is safe and will not be used without his consent? How personal data can be disclosed and used by authorized parties?

Privacy issues are particularly relevant in healthcare, and there are many interesting healthcare applications that fall within the realm of IoT. We can cite among others the tracking of medical equipment in a hospital, the monitoring of vital statistics for patients at home or in an assisted living facility. The system application might be looking for a continuous monitoring of the person's health parameters, while the sensor's ability to record data might limit the sophistication of the security solution used to protect the data it records. In situations for instance, emergency data should be readily available to the medical care unit or responders even without the user's interaction. There would always be a trade-off between functionality and privacy. The one important question still remains: how much privacy are we happy to give up for the potential benefits this new technology can do for humans?

5. IS INTERNET OF THINGS REAL?

Internet of Things is coming. It's not a matter of if or whether, but when and how. And also where do the humans will be placed into this exponentially expanding growth of IoT? Innovations in technology mostly emerge from the needs of human society. Today's top emerging technology:

IoT, focused on proficiently monitoring and controlling different activities will have the impact on human society including everyday life of common people. Ultimately, people will become a part of the IoT through devices for instance in the case of medical implants, without even knowing that they have become part of today's technology.

Here, I will like to quote Mark Weiser's statement in his well-known Scientific American paper, back in 1991. *"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it"*.

6. CONCLUSIONS

This paper aims to give an introductory overview to the reader how wireless sensor are integrated into the Internet of Things, what are the security challenges and the security primitives that might be taken to protect the sensors' data. Current approaches are focused on pre-deployed pre-shared keys on both ends whereas certificate-based authentication is generally considered infeasible for constrained resource sensors. Any unauthorized use of data or privacy concerns may restrict people to utilize IoT-based applications. Peer authentication and data protection are crucial requirements to prevent eavesdropping on sensitive data or malicious triggering of harmful actuating tasks. There are other challenges to be solved if the sensor nodes are integrated into the internet infrastructure and the complete integration of sensor networks and the internet still remains as an open issue. Secret key distribution for heterogeneous sensors in Internet of Things becomes challenging due to the inconsistencies in their cryptographic primitives and computational resources in varying applications. Highly constrained sensors cannot provide enough resources required for the heavy computational operations. The paper studies the interactions between sensor networks and the internet from the point of view of security identifying both the security challenges and the primitives as well.

REFERENCES

[1] Nacer Khalil, Mohamed Riduan Abid, Driss Benhaddou, Michael Gerndt, (2014) "Wireless Sensors Networks for Internet of Things", IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP) Symposium on Public IoT

[2] Jameson Berkow (2011) "Is the Internet leaving humanity behind?" Financial Post

[3] Muhammad A. Iqbal, Dr. Magdy Bayoumi (2016) "Secure End-to-End Key Establishment Protocol for Resource-Constrained Healthcare Sensors in the Context of IoT" The 2016 IEEE International Conference on High Performance Computing and Simulation (HPCS 2016) Innsbruck, Austria

[4] "Internet of Things: An overview by Internet Society" https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf

[5] Kashyap Kompella, "A Guide to the Internet of Things"

[6] Azmi Jafarey, "The Internet of Things & IP Address Needs" Network Computing

[7] Phillip Howard, (January 2015) "The Internet of Things Reference Model" Bloor

[8] Therese Sullivan, (November 2014) "The Cutting-Edge of IoT, how does the IoT really change the future of commercial building operations?" Automated buildings

[9] Jim Duffy, (January 2016) "AT&T allies with Cisco, IBM, Intel for city IoT" Network World

[10] Bruce Ndibanje, Hoon-Jae Lee, and Sang-Gon Lee, "Security Analysis and Improvements of Authentication and Access Control in the Internet of Things"

[11] Cristina Alcaraz, Pablo Najera, Javier Lopez, Rodrigo Roman, "Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?" University of Malaga, Spain

[12] Securing the Internet of Things: A Proposed Framework by Cisco

[13] White Paper Internet of Things Intel Corporation (2014). "Developing Solutions for the Internet of Things"

[14] Intel corporations, USA. Intel® Gateway Solutions for the Internet of Things

[15] D. E Vans, (2011)"The Internet of Things: How the Next Evolution of the Internet is Changing Everything", Cisco Internet Business Solutions Group (IBSG).

[16] H. Shafagh and A. Hithnawi, "Poster Abstract: Security Comes First, A Public-key Cryptography Framework for the Internet of Things", 2014 IEEE International Conference on Distributed Computing in Sensor Systems, (2014), pp. 135-136.

[17] Muhammad A. Iqbal, Dr. Magdy Bayoumi, (2016) "A Novel Authentication and Key Agreement Protocol for Internet of Things Based Resource-constrained Body Area Sensors" The IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud) 2016 Vienna, Austria

AUTHORS

Muhammad A. Iqbal is a graduate student in Computer Science at the University of Louisiana at Lafayette, LA 70504 USA. His research and thesis center around security and privacy for Internet of Things, Wireless Sensor Networks especially in the area of Body Area Networks and healthcare applications in the context of Internet of Things (IoT).

Dr. Magdy A. Bayoumi is the Z.L. Loflin Eminent Scholar Endowed Chair Professor in Computer Science. Dr. Bayoumi has been a faculty member in CACS since 1985. He is the recipient of the 2009 IEEE Circuits and Systems Meritorious Service Award. Dr. Bayoumi is the recipient of the IEEE Circuits and Systems Society 2003 Education Award, and he is an IEEE Fellow. He was on the governor's commission for developing a comprehensive energy policy for the State of Louisiana. He represented the CAS Society on the IEEE National Committee on Engineering R&D policy, IEEE National Committee on Communication and Information Policy, and IEEE National Committee on Energy Policy. He is also active in the "Renewable & Green Energy" and "Globalization: Technology, Economic and Culture" fields. He was a freelance columnist for Lafayette's newspaper.

Dr. Bayoumi has graduated more than 45 Ph.D. and about 175 Master's students. He has published over 300 papers in related journals and conferences. He edited, co-edited and co-authored 5 books in his research interests. He was and has been Guest Editor (or Co-Guest Editor) of eight special issues in VLSI Signal Processing, Learning on Silicon, Multimedia Architecture, Digital and Computational Video, Perception on a Chip, and Systems on a Chip. He has given numerous invited lectures and talks nationally and internationally, and has consulted in industry.

Dr. Bayoumi is the Vice President for Conferences of the IEEE Circuits and Systems (CAS) Society, served in many editorial, administrative, and leadership capacities, including Vice president for technical Activities. He is a technology columnist and writer of the Lafayette newspapers as well.