Research trends in existing technologies that are building blocks to the internet of things

Nomusa Dlodlo[1], Mofolo Mofolo[2], Lionel Masoane[3], Stanley Mncwabe[4], George Sibiya[5], Lawrence Mboweni[6]
CSIR- Meraka Institute
Pretoria, South Africa
Email: {ndlodlo[1], mmofolo[2], lmasoane[3], smncwabe[4], gsibiya[5], lmboweni[6]}@csir.co.za

***Abstract* — The internet of things (IoT) is based on interfacing the digital and physical worlds and making the information generated as a result available via the internet. The challenge that IoT faces as a new research area, is in the identification of further research areas and the way forward. Therefore this paper is the culmination of a research to identify further research areas in the IoT and the relevance of IoT to South Africa. The research first conducted a review of 28 IoT European Union (EU) Framework projects available over the internet. From the reviews, the research extracted the technologies that the EU is conducting research on as building blocks to the IoT. Using an adaptation of the Graham Vickery and Sacha Wunsch-Vincent framework which analyses developments in ICT research and development, this research interviewed experts working with the identified technologies and came up with research trends in the various technologies that are building blocks to the IoT and its relevance to South Africa.**

Keywords—internet of things, sensors, embedded systems, wireless broadband networks, cloud computing, mobile technologies, interoperability

I. INTRODUCTION

The internet of things (IoT) is a group of 'things' sitting on the internet and the related applications that enable interoperability of these 'things' [9]. The 'thing' is a physical or digital object with added intelligence. The 'things' in the IoT publish, discover, describe and invoke services. IoT in itself is a unique approach to cater for low memory, low computational capacity and low power consumption devices.

IoT research is still in its infancy. As a result its definition and scope is still evolving. So are the research directions that it will take in the future. The challenge is that IoT is about integrating a varied range of technologies. To gain a deeper understanding of these technologies, one has to consult the experts in the various technologies. The IoT researcher, however, plays the role of an integrator at a horizontal level.

This paper identifies research trends in the technologies that are building blocks to the IoT and their relevance. The technologies identified included sensors and embedded systems, interoperability, security, communications and protocols, wireless broadband networks, cloud computing integration and mobile technologies.

Section II is on the problem statement. Section III is on sensors and embedded systems. Section IV is on communications and protocols. Section V is on wireless broadband networks. Section VI is on interoperability in the IoT. Section VII is on cloud computing. Section VIII is on mobile technologies. Section IX is on security in networks and section XI is the conclusion.

II. PROBLEM STATEMENT

The IoT is about the integration and interoperability between 'things". For researchers to be able to achieve integration and interoperability of these 'things' there is a need to understand the underlying building blocks to the IoT. These building blocks are existing technologies. The research questions that this paper answers are:

a) What are the research trends in technologies that are building blocks to the IoT research?

b) What is the significance of these technologies to South Africa and the preparedness of South Africa to undertake research in these technologies?

The research first conducted a review of 28 European Union (EU) Framework projects [3], since the EU researchers are the leaders in internet of things research. From the reviews, the research extracted the technologies that the EU is conducting research on as building blocks to the IoT. Using an adaptation of the Graham Vickery and Sacha Wunsch-Vincent framework [15] which analyses developments in ICT research and development, questions were posed to experts that work in the field to come up with research trends in the various technologies that are building blocks to the IoT. The framework answers questions on what is on the ground, who are the main role players in research in the technology, what are the future research areas, what are the research drivers, i.e. the needs at socio-economic level, what are the inhibitors to research on the technology, the relevance of the technology to South Africa and its impact. The technologies identified appear in sections III to X.

III. SENSORS AND EMBEDDED SYSTEMS

A sensor is a device that detects and responds to some type of input from the physical environment [16]. The input could

be light, heat, motion, moisture, pressure or any of a number of environmental phenomena. The output is a signal that can be transmitted electronically over a network for reading or further processing. A sensor works as an embedded system, that is, it is a single purpose computer built into a larger system for the purposes of controlling and monitoring the system [4].

A sensor node, also known as a mote in North America, is a node in a wireless sensor network that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in a network. The mote is a small, low-cost, low power computer. It monitors one or more sensors. It also connects to the outside world with a radio link. It transmits to a distance of 3 to 60 metres. Power consumption, size and cost in motes are the barrier to transmission for longer distances. Motes can run on batteries or can tap into the power grid in certain applications. The battery life of a mote depends on the amount of data processed but varies between 2 and 3 years. If motes are dedicated to a specific function, their battery life lasts longer and energy is conserved. A number of varied sensors can be connected to a single mote, which gives it a non-specific function. Examples of motes for wireless sensor networks are TelosB, Micaz, TelosA, Telosky, STM32F4-Discovery, etc. Large numbers of motes can communicate with each other and form ad-hoc networks.

A. Future research

There a number of dimensions that can be taken when conducting research sensors and embedded systems. Sensors won't work in an unsuitable environment. Therefore there is room to develop sensors/motes for the harsh environment such as dust, high temperatures and water logged places. Currently communication between any two sensors occurs via a central server and not directly. There is room therefore to enable direct communication between sensors by reprogramming them. Normally, each sensor is specialized, that is, it offers a specific function. There is an opportunity to integrate task-specific sensors towards a common functionality, in cases where several different parameters have to be measured. Alternatively addition of functionality to each sensor to be able to detect a number of various parameters would be the route. Since the energy supply of motes ideally comes from batteries, and battery life is limited and low capacity, there is an opportunity to move from battery-powered motes to energy-harvesting motes to avoid changing batteries frequently, and to conserve energy. Embedded systems protocols such as Zigbee and 802.15.4 enable integration of embedded systems with the internet and the integration of devices at the end. This means that there has to be standardization of these protocols for this integration to occur. Protocol standards are another research area. There is room for development of applications (middleware) for embedded systems. These applications enable interfacing with other embedded systems and the internet and integration with actuators, that is, it enables interoperability. Because of resource-constraints in these sensors (motes) intelligence is developed separately from the device. There is a need for development of algorithmic models for self-organising network design, routing around obstacles and tracking network management. The batteries that fire up sensors come in different forms for the various applications, i.e. made of different materials. For example in a health environment there is a restriction of chemicals/ explosives that can be used to build the batteries. Research into battery technologies is a possibility.

B. Relevance to South Africa

The main South African organisations that are involved in sensor and embedded systems research are the South African Earth Observation network (SEON), the South African National Space Agency (SANSA), and the CSIR's units such as MSM, DPSS, Central Analytic Services (CAS), ESKOM. These are in areas of health monitoring, environmental monitoring, agriculture, factory automation and earth observation. The market is available in South Africa for products of research into sensors. There is infrastructure in place for such related research. However the inhibitors are that the competence is fragmented and the basic knowledge limited to a few. Also affecting research is policy issues and regulation. Funding for research is also limited.

IV. COMMUNICATIONS AND PROTOCOLS

There are many ways to connect systems including wirelessly, via Ethernet cable or fiber cable. All these communication modes are of IEEE standards. IEEE protocol 802.1.A-B was the first wireless technology and was of a limited range. Now there is up to 802.1.G which is a higher frequency protocol. The higher the frequency of the protocol the shorter the distance it covers. 802.11.N has an even higher frequency of between 2.4 and 5 GHz and can be used to connect all devices in the home to access IPv6. The different IEEE standards are a security measure to protect connections between any two devices by restricting other protocols the device cannot recognise from accessing the device. IPv6 is the latest revision of Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the internet. IPv6 was developed by the Engineering Task Force (IETF) to deal with the long anticipated problem of IPv4 address exhaustion. IPv4 was the first publicly used version of the Internet protocol. IPv4 included an addressing system that used numerical identifiers consisting of 32 bits while IPv6 addressing is 128 bits. Thus IPv4 provides an addressing capability of 2^{32} or approximately 4.3 billion addresses. IPv6 specifies a new packet format designed to minimize packet header processing by routers. Since the headers of IPv4 packets and IPv6 packets are different the two protocols are not interoperable.

The protocol stack is a set of network protocol layers that work together. The OSI Reference Model [5] that defines 7

protocol layers is called a stack. These layers are the application layer, presentation layer, session layer, transport layer, network layer, data link layer and the physical layer. The application layer defines the language and syntax that programs use to communicate with other programs, e.g. email, file transfer, client-server interactions. The presentation layer manages the way data are represented and encoded, e.g. American Standard Code for Information Interchange (ASCII) to Extended Binary Coded Decimal Interchange Code (EBCDIC), Binary Coded Decimal (BCD) to binary, etc. The session layer provides coordination of communications in an orderly manner, e.g. start-stop session. The transport layer is responsible for the validity and integrity of transmission, that is, it ensures the delivery of the entire file or message. The transport layer is like a door. Data has port numbers and headers to explain what it is, e.g., an IP address to the web browser. Each protocol has a specific port number. For example, Hypertext Transfer Protocol (HTTP) is port 80, Secure Shell (SSH) is port 22, File Transfer Protocol (FTP) is port 21. For security reasons a port number cannot be changed. The network layer establishes the route between the sender and the receiver to different local area networks (LANs) and wide area networks (WANs) based on the network address. The network layer is where IP addresses for the source and the destination are analysed for IP address authentication. If they cannot be authenticated, then access is denied. If the network layer sees its own IP and destination IP, it lets the data through to the transport layer, that is, TCP and UDP. The data link layer is responsible for node to node validity and integrity of transmission depending on station address. The link layer converts electric signals to data. The physical layer is responsible for passing bits onto and receiving them from the connecting medium. It is the electrical signals and cabling.

In the internet protocol stack [6], at the application level are Hypertext Transfer Protocol (HTTP), Remote Procedure Call (RPC), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Advanced Message Queuing protocol (AMQP), Extensible Messaging and Presence Protocol (XMPP), Message Queue Telemetry Transport (MQTT), Real Time Streaming Protocol (RTSP) and Simple Object Access Protocol (SOAP), while in the machine protocol stack at the application layer is COAP (Constrained Application Protocol). COAP is a software protocol that targets small low power sensors, switches, valves and similar components that need to be controlled or supervised remotely through standard internet networks. COAP is designed to easily translate to HTTP for simplified integration with the web. The application protocol in the machine protocol stack should be able to handle information from the internet protocol stack for interoperability in IoT systems. All computers have TCP and UDP protocols in the transport layer. Transmission Control Protocol (TCP) is for transferring reliable data such as emails which have to get to a destination point. As a result it has 3 authentication points and takes longer. User Datagram Protocol (UDP) is not very reliable as it streams video data which can results in some packets being lost. In the internet protocol stack in the transport layer are IPv4 and IPv6 while in the machine protocol stack is 6LowPAN.

A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a network [10]. Routing algorithms determine the specific choice of route. Although there are many types of routing protocols, three major classes are in widespread use on IP networks. Interior gateway routing is via link state routing protocols such as Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System protocol (ISIS). Interior gateway routing is via path vector or distance vector protocols such as Interior Gateway Routing Protocol (IGRP) and Extended Interior Gateway Routing Protocol (EIGRP). In Exterior gateway routing, the Border Gateway Protocol (BGP) is the routing protocol used on the internet for exchanging traffic between autonomous systems. An autonomous system is a network or group of networks under a common administration and with common routing policies. Routing protocols according to the OSI frameworks are layer management protocols for the network layer, regardless of their transport mechanism. ISIS runs on the data link layer. OSPF is encapsulated in IP but runs only on the IPv4 subnet while the IPv6 version runs on the link using only link-load addressing. IGRP and EIGRP are directly encapsulated in IP. EIGRP uses its own reliable transport mechanism while IGRP assumed an unreliable transport. Routing Information Protocol (RIP) runs over UDP while BGP runs over TCP. These routing protocols enable communication to occur with remote devices using various paths. ISIS is associated with larger networks while OSPF locates the shortest path that a packet can move.

Medium Access Control (MAC) [17] in a network card is a unique number which is used to communicate with other machines. Only manufacturers of the network devices can provide MAC. Companies purchase a range of MAC addresses in bulk, hence MAC addresses are unique to a device and are not duplicated. Companies also purchase only one IP address and the other IP addresses then become sub-networks of the original IP address purchased. Dynamic allocation is when computers in an organization do not have fixed IP address but are allocated IP addresses at any point in time when a transaction has to occur. Network Address Translation (NAT) translates private addresses in one network into a public address going into another network. In dual stacking, IPv6 and IPv4 addresses are running together in the same network. This results in increased overheads which in turn reduces efficiency of the network. The alternative to dual stacking is the IPv6 NAT which translates IPv6 into IPv4.

A. Future research

There is room to develop one's own connection method and get allocated an IEEE number if the method is of world class standard. ISIS and OSPF use different algorithms. There is room to come up with new algorithms to learn the shortest

path between any two routers. Research can be conducted on ways to reduce overheads so as to improve efficiency in dual stacking. UDP migration from TCP to avoid delays due to 3-way communication is another route.

B. Relevance to South Africa

Due to an increase in the number of devices that are being connected to the internet, high-speed internet is a requirement. More mobile technology integration is a necessity into the internet. Wireless hotspots should be a prerequisite in every corner to reduce dependency on cell phone service providers. An increase in UDP communication is also a necessity.

V. WIRELESS BROADBAND NETWORKS

Wireless broadband networking is a technology that provides high-speed wireless internet access or computer networking access over a wide area. 4G Long Term Evolution (4G-LTE), 4G-WiMAX, Universal Terrestrial Radio Access Network (U-TRAN), DigiMesh, General Packet Radio Service (GPRS), Bluetooth, are examples. Wireless broadband falls into local area and wide area categories. Wireless local area networks (WLANs) namely 802.11 Wi-Fi networks transmit at very high speeds but coverage area (hotspots) spans only a few metres. In contrast, the 3G/4G LTE wireless wide area networks (WWANs) from cellular carriers are slower but provide data services nationwide like they do with voice.

White space refers to parts of the radio spectrum that are not utilized all the time or in all geographic locations. Several regulators around the world are moving towards using unlicenced access to these frequencies, subject to the provision that licenced transmissions are not adversely affected. By allowing access to these white space frequencies, more effective and efficient use of radio spectrum is envisaged. Controlling access to white space spectrum involves use of cognitive radio techniques in which white space devices would sense their radio frequency environment and be able to automatically identify radio channels they could use without causing degradation to primary transmissions.

In wireless networks the problem of allocating transmission rights to subsets of networks users at each time and under different channel qualities is known as the scheduling problem. Transmissions tend to interfere with each other and also undergo impairments such as fading, attenuation, etc. Therefore scheduling mitigates that. Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in the communications. It can be performed even when messages are encrypted and cannot be decrypted.

A. Future research

Free space technologies where no spectrum is needed, e.g., to use sunlight to transmit data during the day (white light networking), and light from the moon during the night are one area of research. So is finding spectrum vacant spaces/ holes in TV white spaces. So is the scheduling problem a potential research area. In the area of cognitive radios, research can be on scanning the environment and adapting parameters such as power, radios, antennae, CPU speed, memory allocations, embedded components and mobility. For energy-efficient networks, research on integrating renewable energy into these technologies is the route.

B. Relevance to South Africa

South Africa is currently under-served in broadband connectivity. E-government is an area that requires broadband access. Broadband is an accelerator of economic and social development according to the World Economic Forum. Broadband enables infrastructure for building the knowledge economy. The “last mile” of copper wires into homes and businesses is controlled by Telkom, limiting access by competitors to this infrastructure. South Africa’s broadband policy is informed by the need to fast track the deployment of high-speed broadband infrastructure such as fibre-optic backbones and wireless and international connectivity. The role players are in the South African environment are state owned SenTech and Broadband Infraco.

VI. INTEROPERABILITY

Due to the large numbers of devices that connect to the internet of things, interoperability [7] becomes an important issue. Technical interoperability means that a signal can get from object A to object B. In other words, technical interoperability requires that objects be able to speak and be heard. Semantic interoperability means that object B can understand object A’s message. Semantic operability requires that they speak the same language. Systemic interoperability refers to the ability of distinct IoTs to communicate with each other. It is another form of technical interoperability that deals with the arrangement of IoTs on a meta level. IETF is leading efforts to design international standards suitable for constrained environments including the internet of things, leading to a new protocol suite enabling interoperability between the regular internet and this emerging constrained environment. The working groups include 6LowPAN in the internet area, ROLL (Routing over Low Power and Lossy Networks) in the routing area and Constrained Restful environments (CoRE) in the application area. The other role players in interoperability are Internet Research Task Force (IRTF), IPSO Alliance, CISCO, Atmel and SICS. The common internet protocols are IP, TCP, DHPC, DNS, HTTP, TLS, HTML and XML. Dynamic Host Configuration Protocol (DHPC) is a network protocol used to configure devices that are connected to a network so they communicate on that network using IP. Transport Layer Security (TLS) is a protocol that ensures privacy between communication applications and their users on the network. Transmission Control Protocol (TCP) is one of the core protocols of the IP suite and provides reliable, ordered, error-checked delivery of

a stream of octets between programs running on computers connected to a local area network (LAN), intranet or public internet. It resides at the transport layer. Domain Name System (DNS) is a hierarchical distributed naming system for computers, services or any resource connected to the internet or a private network. It associated information with domain names assigned to each of the participatory entities. HyperText Markup Language (HTML) is the main markup language for creating web pages and other information that can be deployed in a web browser. Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. Extensible Markup Language (XML) is a markup language that defines asset of rules for encoding documents in a format that is both human-readable and machine readable.

A. Future research

There is room for research in a new protocol suite enabling interoperability between the regular internet and this emerging constrained environment which is to be composed of a very wide range of smart objects with different communication technologies such as wireless sensor networks and wired control systems.

In the area of protocols there is room for investigating possible issues hindering wide adoption of the new protocols in crowded networks. The development of a transport protocol suitable for IoT and mappable to TCP so that a regular TCP connection can transparently flow into the constrained network and access the available services, by passing through a low-cost general purpose IoT gateway mapping TCP to a lightweight transport protocol is the route to go.

B. Relevance to South Africa

In the networking of data, there is an opportunity to network government data which has existed as autonomous and owned by various government departments separately. Integrated systems in any domain assist keep track of data so as to improve knowledge about the state of the world. Greater operability would mean that people can pick and choose their preferred technologies, leading to a greater competition in the market place. The trend nowadays is towards automation that is based on IoT principles for the various domains. Through capability enablement South Africa needs to empower the people involved with the right skills to be able to make the technology that is interoperable. This includes enabling data usage, application integration and application context. The main goal should be to describe the overall capability enabled at a particular Interoperability Readiness Level. It is relevant to South Africa and that is proven by the announcement that was made on the 14 June 2013 that the IEEE 1904.1TH Standard FOR SERVICE INTEROPERABILITY (SIEPON) was approved by the IEEE Standard Association (IEEE-SA) at the Standard Board meeting. It provides open, international, system-level specifications enabling multi-vendor, "plug-and-play" interoperability in EPON systems. The department of Communications, DST and DTI are driving initiatives of this kind.

The inhibitors to interoperability are at human and organizational level. Individual firms develop distinct and limited IoTs with internal technical and semantic interoperability. As IoTs spread international/governmental legal issues arise. Security issues are also escalated as a result of interoperability. For example, an attack targeting weaknesses in the system can shut the whole system down, install data collecting malware or control systems. On the issue of privacy, more interactions lead to more points of attack. More extensive communications lead to more data being collected, increasing more damage when the system is hacked.

One of the research drivers is the semantic operability, that is, the ability of devices to understand what the data they communicate means. This is about standardizing the protocol and data formats. RFID was standardized under ISO/IEC standard ISO 180000. The physical layer of most wireless systems is standardized under IEEE 802.15.4-2006 which lays out specifications for low power wireless personal area networks. There is usually a capability mismatch between traditional internet hosts and small devices due to the widely differing communication and processing bandwidths in different devices. This calls for interoperability at semantic level. The different internetworking protocol choices such as legacy IP versus IPv6 and simplified web protocols such as COAP/UDP instead of HTTP/TCP are key determinants of the level of interoperability in IoT systems. Where IPv4 and IPv6 exist in isolation from each other is the single stack, and where both exist in the same network it's the dual stack.

VII. CLOUD COMPUTING

The cloud is a term for networked computers that distribute processing power, applications and large systems among machines [1]. It refers to a 'remote data centre', that is, computing is no longer on local computers but on centralized facilities operated by third party compute and storage facilities. Any IT outsourcing – network infrastructure, security, monitoring, remote hosting – is a form of cloud computing. Among the drivers that are encouraging more institutions to contemplate cloud services are budget pressures, calls for increased reliability of and access to IT systems, and the need for institutions to provide timely access to the latest IT functionality. Cloud computing services can be classified into three primary categories of software-as-a-service (SaaS), infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS). In SaaS an independent software vendor offers usage of applications as a subscription service delivered over a network. The advantage is that an application can be deployed without requiring expansion of the enterprise data

centre infrastructure with additional servers, storage and networking resources, channels and applications. In IaaS, an organization can provide access to a large network of virtual servers that facilitate the development and testing of distributed applications. The goal of PaaS is to facilitate the deployment of applications without the cost and complexity of buying and managing underlying hardware and software layers.

A. Future research

For the South African environment there is room for research into the public government cloud architecture. Currently the different government departments are the sole custodians of their data. This results in duplication of data. An integrated cloud platform would make the data available across all departments. Green cloud computing infrastructure that is environmentally-friendly offers another potential research direction. Hardware platforms and architectures with high energy-efficiency and low initial investment costs, security and productivity and reduces costs of signing in for services.

Digital cloud forensics is meant to gather evidence to support criminal cases in data that is associated with the cloud. Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data including the cloud platforms. This involves computer forensics, network forensics, forensic data analysis, cloud forensics and mobile device forensics.

Bring Your Own Device (BYOD) is an approach to enable access to enterprise resources from any device that is connected to the cloud without compromising the security of data. There is room to research on how this can be achieved, considering the IoT approach and the myriad of devices involved.

A business model describes the value proposition, market segment, and cost structure, position in the network of competitors, the competitive advantage and the infrastructure of a business entity. In the IoT approach to the cloud various business models result and these can be researched into.

Automated self-service provisioning is the ability to deploy an IT or telecommunications service by using pre-defined procedures that are carried out electronically without human intervention. Automating provisioning allows customers to set up and make changes to services themselves by using a web browser or other client interface to provide a more efficient and rapid response to business requests. Automated provisioning is a type of policy-based management, i.e. an administrative approach used to simplify the management of a given endeavor by establishing policies to deal with the situation.

Automating virtual machine migration is about allowing data centres to rebalance workloads across physical machines while applications on existing virtual machines continue to run. Simply moving an overloaded VM to a random underloaded physical machine can inadvertently overload the network. Research on decreasing network traffic during this migration is therefore an essential.

There is room for research in the area of legal implications of cloud computing and possible policy interventions. The number of trademark filings covering cloud computing brands, goods and services is increasing, increasing the risk of litigation. Data on the cloud can be stored in any country. The physical location raises the question of legal governance over the data. Organisations are legally prohibited from transferring personal information to countries that do not provide the same level of protection with respect to personal information.

Security is one of the most-often cited objections to cloud computing. A cloud-specific security issue is that of running arbitrary virtual machine images. This is only one aspect of making sure the right data is available to the user at the right time. The issues of authentication, authorization, privacy, integrity, data reliability and availability are to priority. When one participates in the cloud, they depend on third party to make decisions about data and platforms. When the internet goes down access to one's data is cut off. The security of a system is only as strong as the weakest user's set-up.

B. Relevance to South Africa

With the introduction of South Africa's National Health Insurance, collaboration in patient information and diagnosis is an essential, as a result of accessibility from anywhere. So is the government cloud platform for interoperability between government departments. The rural South Africa has limited IT infrastructure, hence hosting services externally not only lowers costs, but it also provides the scarce infrastructure. The key enabling institutions to a South African cloud platform are SITA which provides the cloud platform. The challenge though is manual capture of existing paper documents into the new cloud

VIII. MOBILE TECHNOLOGIES

Mobile technology is the technology used for cellular communications [12]. The future of computer technology rests in mobile computing with wireless networks. Mobile computing by way of tablet computers are becoming popular. Tablets are available on 3G and 4G networks. Many types of mobile operating systems are available on smartphones including Android, Blackberry OS, Web OS, iOS, Symbian, Windows Mobile Professional (touchscreen) and Windows Mobile standard (non-touch screen). Google Chrome is releasing an OS for mobiles where everything runs on the cloud. The phone is just a connection to the internet without

any processing power. The next generation of smart phones is going to be context-aware, taking advantage of the growing availability of embedded physical sensors and data exchange abilities. One of the main features applying to this is that the phone will start keeping track of your personal data.

The trend in mobile technologies today is in the seamless migration of different technologies, that is, any mobile application should be able to run on a number of different mobile platforms without any modifications to it. The application should have the same interface irrespective of the device it is running on.

The main players in the mobile market in South Africa are Vodacom, MTN, Cell C, 8ta, Virgin mobile. The main role players in mobile research in South Africa are the University of Capetown's Apple Lab and the Blackberry Lab at the University of Pretoria. The external role players are Samsung, Blackberry, Google and Apple.

A. Future research

Current research is in the area of development of a mobile platform to which services can be added. In addition to this there is room for the development of mobile applications that offer a range of functionalities and are device-independent. There is room for developing web applications that run on mobile devices using software such as JQuery Mobile, ASP.Net, etc. In South Africa access to government services via mobile technologies currently is based on one way communication via SMS, MMS, etc. from the government departments to the citizens. Therefore there is room for research into two-way communications through mobile technologies. With mobility comes network congestion that requires a redesign of network connectivity. Japan has assigned IPv6 addresses in its networks to counter congestion and for reasons of scalability. Research opportunities are available in balance load scheduling algorithms on mobile platforms. With mobility also come issues of security, privacy, mobile governance and interoperability.

B. Relevance to South Africa

South Africa has its own set of problems that need solutions and some of these problems can be solved through mobile technologies. Health and mobile education in remote rural areas can be enhanced through mobile technologies. Mobile health information can be dispensed to remote areas using mobile technologies. Mobile diagnostic kits enable malaria detection on camera. In cases of blended learning where the internet provides education, mobile technologies could be handy. There are enough researchers in the mobile community to take mobile research forward. However, the degraded network power in remote regions can be an inhibitor to mobile adoption.

The need to establish quick communication, that is, roaming without a cable is one of the drivers of adoption of mobile technologies. Landline penetration is very low in South Africa due to inaccessibility of some areas and hazardous terrain. Therefore this drives the mobile market up since cell sites can be placed far and wide to cover a larger terrain. Unfortunately mobile costs are very high, with South Africa being the 6th highest in the world. Bringing the cost down would further up the impetus of adoption of mobile technologies. Cell phone service providers usually set up their own individual infrastructure. However a shared resource use by cell phone service providers would result in scalability of infrastructure. However congestion due to large traffic volumes results in calls being dropped at peak times, meaning there is a level of unreliability. There are many socio-economic problems in South Africa. Cellphone coverage is high in South Africa and offers the opportunity to bring services to the marginalized. When processing power is placed in the cloud and not on the handset, a web server processes the handset faster. In South Africa cellular access is via service providers predominantly and yet in more developed countries WiFi hotspots are available in every corner and funded by the government. There is also what is called location-based WiFi where according to the GPS the WiFi can be turned on and off. Nowadays cell phones are advanced in features for mobile support. The laptop is smaller and therefore moving towards mobility. These low-cost devices are also reason for the rise in cell phone banking.

IX. SECURITY

Well-designed security services can contribute to the reliability and robustness of a network's communications infrastructure and the protection of data sent over the network [11]. Any network communication medium has a protocol. The medium of communication is either wired or wireless. The protocol in a particular communication medium does not change, i.e., you do not have to install any particular software on it for the protocol to work.

Security threats on the networks can be both internal and external and each type of threat calls for different handling [8]. External security threats are as a result of unauthorized access. One of these is about connecting to the wireless node which is the entry point to a network and gaining access to network resources. The other one is installing a program either intentionally or unintentionally on the network, thus allowing unauthorized access to the network by outsiders. Vulnerabilities in the network such as buffer overrun pose a threat. An application is expected to reject junk, but in the case in which this is allowed, the code accepts unauthorized data such as a link to an external unauthentic connection for instance, or executes unauthorized code which threatens the system.

Any network-controlling entity has some maximum capacity in terms of memory and connections at a time, e.g., with a PABX one has to wait for an available line. Denial of service is about making a network inaccessible by making it busy through establishing too many connections and congesting it. The network administrator can easily resolve the issue if the threat is internal by identifying the IP address of the device that is congesting the network. On the other hand, if

the attack is from an external source, the attacker may move from one IP address to the next to evade identification.

Device manufacturers provide APIs to developers so that their software can interface to the manufacturer's device. However the Android API comes from Google and not the manufacturer of the device on which the Android runs since Android is open source. Traditionally device manufacturers also come up with the operating system. Middleware enables heterogeneous devices to communicate. IP is normally built into devices. An open API at the top end of the system makes it easier to integrate devices rather than talk to each device separately. The middleware can link different vendor platforms. This results in security of data integrity when data is moved between devices.

Authentication is the process of identifying a user that can access a network resource. In a security system, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the user is who they claim they are, but says nothing about the access rights of the individual. Authentication asks the question, "Who or what are you?" Authorisation asks, 'what are you allowed to do?". Accounting wants to know, 'what did you do?". The existence of authentication, authorization and accounting is about enabling mobility and dynamic security as opposed to a network that must be statically configured to control access.

The main international players in network security are CISCO, MacAfee, Norton and JUNIPER

A. Future research

There is an opportunity to research on how to write antivirus software and firewalls that run on the same level. Anti-virus software runs on the operating systems such that when a virus is developed for the hardware (assembly) level it will act against the operating system. There is room to develop secure protocols. Protocols are defined by request for comment (RFC) that is a standard of IETF. Researchers normally put together a proposal on how to get a particular result and publish it as an RFC. Potential problems in protocols result from the implementation of RFC that may have been misinterpreted when code is written. There is research into understanding network security threats and their combinations by creating false-controlled scenarios. So is there an opportunity to develop security middleware

B. Relevance to South Africa

In South Africa the key enabling institutions to network security are Electronic Communications Security (ECOMSEC), DPSS at the CSIR, FARITECH and NANOTECH for communications between embassies. The drivers to enabling network security are preserving data integrity, guarding against data loss, privacy of data and security of data. The need for an integrated network management system is also a key driver. The inhibitors are in the ownership of the data, institutional policies and government policies.

X. CONCLUSION

This research identified the research trends in technologies that are building blocks to the IoT and the relevance of these technologies to South Africa. These technologies vary from sensors and embedded systems, to interoperability, security, communications and protocols, wireless broadband networks, cloud computing, mobile technologies and socio-economic, legal, regulatory and governance issues. The information generated will assist guide the identification of the South African IoT landscape. It is also a measure of the research landscape in the basic IoT technologies from an international perspective. The technologies identified are what is already on the ground. The advantage is that the research now looks at South Africa specifically. To understand these technologies people with expertise had to be drawn from the different areas. Therefore IoT is a complex multidisciplinary area that needs multidisciplinary teams.

REFERENCES

[1] Dlodlo, N., A review of cloud computing, CSIR Report No. CSIR/MI/ISPT/IR/2011/00005/A, 2011

[2] Dlodlo, N., Legal, privacy, security, access and regulatory issues in cloud computing, ICIME 2011, Ted Rogers School of Management, Ryerson University, Toronto, Canada, 27-28 April 2011

[3] Dlodlo, N., Foko, T., Mhlanga, M., Mvelase, P., Mofolo, M., Montsi, L., Internet of Things EU Framework projects, CSIR Report No. CSIR/MI/ISPT/IR/2013/0020/A, 2013

[4] Embedded systems, en.wikipedia.org/wiki/Embedded_system

[5] Day, J.D., Zimmermann, H., OSI Reference Model, Proceedings of IEEE, Volume 71, No. 12, 1983

[6] Jang, J., Jung, J., Choi, K., Jeon, G., Ching, Y., Joung, J., An internet protocol stack for high speed transmission in a non-OS environment, proceedings of 2011 ACM Symposium on Research in Applied Computation, RACS'11, 2011

[7] Kominers, P., Interoperability Case Study – Internet of Things, Berkman Centre fior Internet and Society at Harvard University, Research Publication No. 2012-10, 2012

[8] Heinrich, F.R., Kaufman, D.J., A centralised approach to computer network security, AFIPS'76 Proceedings of the June 7-10, 1976 National Computer Conference and Exposition, pp. 85-90, 1976

[9] Horrow, S., Sardana, A., Identity management framepwrk for cloud-based internet of things, SECURIT'12 Proceedings of the First International Conference on Security of Internet of Things, pg 200-203, 2012

[10] Hummel, S., Routing protocol Selection Guide – IGRP, EIGRP, OSPF, ISIS, BGP, CISCO Support Community, https://supportforums.cosco.com/docs/DOC-30205

[11] Messerges, T.S., Cukie, J., Kevenaar, T.A.M., Puhl, L., Struik, R., Callaway, E., A security design for a general-purpose self-organising multihop ad hoc wireless network, Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, Virginia, USA, 2003

[12] Mobile technology, en.wikipedia.org/wiki/Mobile_Technology

[13] PROBE-IT, http://www.probe-it.eu

[14] Socioeconomics, https://en.wikipedia.org/wiki/socoeconomics

[15] Vickery, G., Wunsch-Vincent, S., R&D and Innovation in the iCT Sector: Towards Globalisation and Collaboration, The Global Information Technology Report 2008-2009, World Economic forum

[16] What is a sensor?, whatis.techtarget.com

[17] Zhao, Y., Miao, C., Ma, M., Zhang, J., Leung, C., A survey and projection on medium access control protocols for wireless sensor networks, Computing Surveys, Volume 45, Issue 1.