EIMJ
المجلة الإلكترونية الشاملة متعددة التخصصات
www.eimj.org
المجلة الإلكترونية الشاملة متعددة التخصصات
العدد السابع عشر شهر (10) 2019

Cloud Computing and IoT in the era of Strategic transformation of Saudi Arabia through Vision 2030

Dr. Saleh AL Saleh, *Saudi Electric Company, Saudi Arabia* and Eng. Abdullah Odeh, *Almotahida Group, Saudi Arabia*

Email : saleh.alsaleh@gmail.com

Abstract

Cloud Computing and Internet of Things (IoT) can contribute immensely towards Saudi Vision 2030's Effective Governance initiative and also to the "Power " vision 2030. These contributions have been demonstrated in this Paper through an exploration of the technical visions underlying the Internet of Things and Cloud Computing, their market potentials, driving factors, the benefits they offer to Saudi Arabia and to the Saudi Electric Company (SEC), as well as their interface or integration applications and challenges.

Cloud Computing and IoT provide values for real time reaction and business intelligence for many applications in industry, commerce and customer areas for the Kingdom and specifically for SEC. IoT and Cloud computing and their connected devices and sensors and platforms for household appliances,

Dr. Saleh AL Saleh is with Saudi Electric Company, Riyadh, Saudi Arabia (e-mail: SSBinsaleh@se.com.sa)
Eng. Abdullah Odeh is with Almotahida Group, Riyadh, Saudi Arabia (e-mail: abdullhs.odeh@gmail.com).

projects planning and monitoring, inventory control, smart grid, electric meters are some of the potential value-added business opportunities for SEC to explore over the next few years.

Towards this end, SEC needs to develop appropriate roadmap and action plans for meeting IoT and Cloud Computing Technologies driven Power Vision 2030.

Index Terms--Clouding computing, Fog computing, Internet of Things (IoT) , Smart environment, Wireless sensor networks.

I. INTRODUCTION

Saudi Vision 2030 is a visionary strategic initiative to reduce Saudi Arabia's dependence on oil, diversify its economy and develop service sectors such as health, education, infrastructure, recreation and tourism. The goals include reinforcing economic and investment activities, increasing non-oil based industry, manufacturing and trade between countries and increasing government spending on military manufacturing of equipment and ammunitions within the Kingdom. The Vision has more than 20 initiatives and one of them is "Effectively Governed initiative". The main objective of this initiative is to raise Saudi's ranking on the E-Government Survey Index from its current position of 36 to 10.

This paper is written to explore and present the role of current Information Technologic evolution in the implementation of Vision 2030 strategy focusing specifically on the importance Cloud & IoT in effective governance and also on concerns of security in the era of Cyber warfare. This paper will present in-depth discussion of Internet of Things and their effect on business and individuals, with specific focus on Vision 2030 Strategy implementation. It provides information on key emerging technologies, and opportunity for their alignment with growth strategy and policy implementation.

A. *IOT: Internet of Thing*

The Internet of Things (IoT) as shown on Fig. 1 and Fig. 2 is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. The Internet of Things also refers to the rapidly growing network of connected objects that are able to collect and exchange data using embedded sensors. IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS), micro services and the internet. The convergence has helped tear down the silo walls between operational technologies (OT) and information technology (IT), allowing unstructured machine-generated data to be analyzed for insights that will drive improvements.

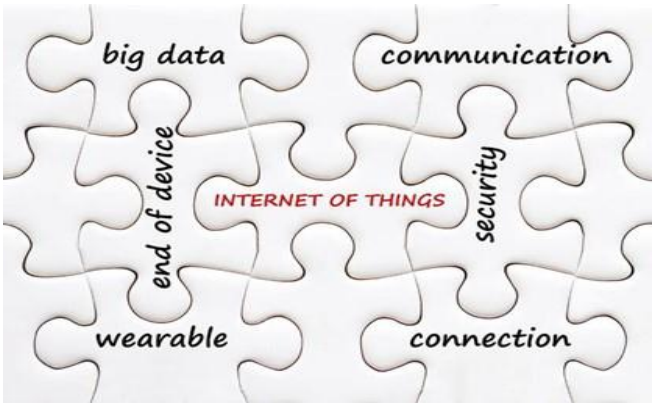

Fig 1. Internet of Things system

B. *Cloud Computing*

Cloud computing is defined as the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Also cloud computing can be defined in a general term as the delivery of hosted services over the internet.

Cloud computing enables companies to consume a compute resource, such as a virtual machine (VM), storage or an application, as a utility -- just like electricity -- rather than having to build and maintain computing infrastructures in house.

Cloud computing is different –in that it separates your data from your IT infrastructure, so your data is replicated 'in the Cloud', which could be anywhere in a multitude of 'virtual' servers. However, these qualities give rise to a new set of security and privacy issues that will influence risk management practices. It has also triggered a re-evaluation of the complex legal issues in areas such as compliance and auditing.

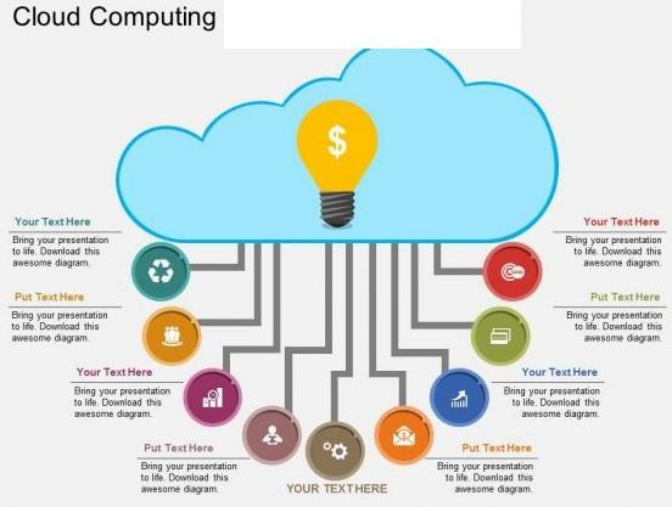

Fig 2. Internet of Things system 2

II. SYNERGY BETWEEN IOT AND CLOUD

The Internet of Things (IoT) is a novel paradigm relying on the interaction of smart objects (things) with each other and with physical and/or virtual resources through the Internet. Despite the recent advances that have made IoT a reality, there are several challenges to be addressed towards exploiting its full potential and promoting its tangible benefits to society, environment, economy, and individual citizens. Recently, Cloud Computing has been advocated as a promising approach to tackle some of the existing challenges in IoT while leveraging its adoption and bringing new opportunities. With the combination of IoT and Cloud Computing, the cloud becomes an intermediate layer between smart objects and applications that make use of data and resources provided by these objects.

In so doing, IoT can benefit from the almost unlimited resources of Cloud Computing to implement management and composition of services related to smart objects and their provided data. On the other hand, the cloud can benefit from IoT by broadening its operational scope to deal with real-world objects. In spite of this synergy, literature still lacks a detailed and comprehensive presentation on what has been investigated on the integration of IoT and Cloud Computing and what are the open issues to be addressed in future research and development. The goal of this work is to fill this gap by systematically collecting and analyzing studies available in the literature aiming to: (i) obtain a comprehensive understanding on the integration of IoT and Cloud Computing paradigms; (ii) provide an overview of the current state of research on this topic; and (iii) identify important gaps in the existing approaches as well as promising research directions. To achieve this goal, a systematic mapping study was performed covering papers recently published in journals, conferences, and workshops, available at five relevant electronic databases.

III. Major Challenges in the Adaptation

The universe of connected things providing key physical data and further processing of that data in the cloud to deliver business insights— presents a huge opportunity for many players in all businesses and industries. Many companies are organizing themselves to focus on IoT and the connectivity of their future products and services. For the IoT industry to thrive there are three categories of challenges to overcome and this is true for any new trend in technology not only IoT: A. technology, B. business and C. society.

As exciting as the Internet of Things world may be—from the promise of autonomous cars to the egalitarian idea of a robotic butler in every home—there are still some serious technical challenges that organizations dabbling in the IoT must be aware of. The protocols of interconnectedness are still evolving, and the industry is miles away from a standard. Some devices require a fast and efficient protocol where reliability isn't important. Others prize reliability over speed. The flux state of IoT protocols has created new challenges for ensuring the security of the devices that rely on them. A reporter George Lawton discusses the security issues devices may encounter and how an IoT gateway can be used to plug up some of those holes.

Another challenge organizations are dealing with is how to handle the massive amounts of data an army of interconnected devices generates. A software developer Swathija Raman discusses how IoT devices are changing the way analytics is done and what types of insights can be mined from the gathered data. To close, we look at the challenges of testing IoT applications. When software gets deployed on components that can fly and accelerate, testing for safety and trustworthiness takes on new meaning. If you're embarking on the path of IoT development, these are some of the key topics you'll want to be informed about.

A. *Technological Challenges*

Although all technologies needed to make IoT systems function smoothly as a standalone solution or part of existing systems, that's not an easy mission., They give rise to are many technological challenges, including Sensors/devices and Security, Connectivity, Compatibility, Longevity, Standards and Intelligent Analysis & Actions, as shown on Fig. 3.

Fig 3. Technology challenges

B. Sensors/Devices and Security

Although all technologies needed to make IoT systems function smoothly as a standalone solution or part of existing systems, that's not an easy mission., They give rise to are many technological challenges, including Sensors/devices and Security, Connectivity, Compatibility, Longevity, Standards and Intelligent Analysis & Actions.

C. Security a Concern

IoT has already turned into a serious security concern that has drawn the attention of prominent tech firms and government agencies across the world. The hacking of baby monitors, smart fridges, thermostats, drug infusion pumps, cameras and even the radio in your car are signifying a security nightmare that affect the future prospects of IoT advancement For instance, so many new nodes are being added to networks and the internet that will provide malicious actors with innumerable attack vectors and possibilities to carry out their hacking s, especially since a considerable number of them have security holes.

The more important shift in security concerns will come from the fact that IoT will become more ingrained in our lives. Concerns will no longer be limited to the protection of sensitive information and assets. Our very lives and health can become the target of IoT hack attacks.

1) Challenges and Implementation:

They are many sensors/devices for IoT application depending on what kind of objectives we want to achieve. Utility like SEC need to define roadmap of the future application in the IoT application. Smart meters, energy Service Company, asset management, smart home and smart appliances are some of potential area of IoT application for a utility such as SEC. The challenge for SEC is to define the roadmap, and strategy goal connecting the need, requirement and scope of the future application of IoT, cloud computing and fog computing. Therefore, the first stage is to understand the need and requirement of utility visionary in terms of IoT, cloud computing and fog computing. This is then followed by, setting up the roadmap and strategy goal to attain the target. Once the roadmap is defined, the sensors and devices can be selected by their function. All the resource needed should support the roadmap including the manpower, financial, hardwires and soft wares.

D. Security a Concern Connectivity in the New Era

To get data into cloud, the sensors/devices can be connected to the cloud through a variety of methods including: cellular, satellite, WIFI, Bluetooth, low-power wide-area networks (LPWAN), or connecting directly to the internet via Ethernet.

Choosing which connectivity option is best comes down to the specific IoT application, but they all accomplish the same task: getting data to the cloud. However, each option has tradeoffs between power consumption, range and bandwidth (here's a simple explanation)

. Connecting so many devices will be one of the biggest challenges of the future of IoT, and it will defy the very structure of current communication models and the underlying technology. At present we rely on the centralized, server/client paradigm to authenticate, authorize and connect different nodes in a network.

The future of IoT will therefore very much have to depend on decentralizing IoT networks. This can partly be realized by moving some of the tasks to the edge, such as using fog computing models where smart devices such as IoT hubs take charge of mission-critical operations and cloud servers take on data gathering and analytical responsibilities.

1) Challenge and Implementation:

Telecommunication characteristics relate to power consumption, range and bandwidth. Different wireless, wire or hybrid telecommunication system has different ability of communication performance. Generally speaking, High performance means high cost in terms of capital investment. IoT application varies from many fields. For example, smart meters need communication ability less than mobile phone which needs high speed and stations and therefore bandwidth. So, While LPWAN could be a better solution one first needs to build up the base and this requires a high initial investment cost. On the contrast, 3GPP cellular system can provide quick and reliable products but the service fee is high due to i its high licensed fee and the frequency e. Challenge for SEC is to clarify the telecommunication needs in the future IOT application at connecting the projects in every utility sector.

E. Data Processing, Compatibility and Longevity

Once the data gets to the cloud, software performs some kind of processing on it. This could be very simple, such as checking that the temperature reading is within an acceptable range. Or it could also be very complex, such as using computer vision on video to identify objects (such as intruders in your house).

IoT is growing in many different directions, with many different technologies competing to become the standard. This will cause difficulties and require the deployment of extra hardware and software when connecting devices.

Other compatibility issues stem from non-unified cloud services, lack of standardized M2M protocols and diversities in firmware and operating systems among IoT devices.

Some of these technologies will eventually become obsolete in the next few years, effectively rendering the devices implementing them useless. The good thing is that in contrast to generic computing devices which have a lifespan of a few years, IoT appliances (such as smart fridges or TVs) tend to remain in service for much longer, and should be able to function even if their manufacturer goes out of service.

1) Challenge and Implementation:

Data processing varies in both structure database and non-structure database. Nowadays, the applications in utility are mostly in structure database. But, in the mobile phone and other social media, IoT and machine to machine communication are almost in non-structure database system. New technology need to be introduced into utility. Big data analysis and business intelligence technology could be involving a very complex algorithm. Talent engineers regarding big data, cloud computing and fog computing should be a big challenge in the area.

For smart meters projects, SAP system has been installed in SEC already. So the interface of database should consider the integration of existing structured database and MDMS, such that MDUS (Meter data utilization system) can be introduced to interface the new system and existing database system. If the IoT, cloud computing and fog computing are introduced, then non-structured database should be or integrated with combined structured database to provide the business intelligence. Required related big data processing scientist and engineers should be recruited, trained and deployed in advance.

F. Standards and User Interface

Technology standards which include network protocols, communication protocols, and data-aggregation standards, are the sum of all activities of handling, processing and storing the data collected from the sensors [3]. This aggregation increases the value of data by increasing, the scale, scope, and frequency of data available for analysis.

Challenges facing the adoptions of standards within IoT: -

• Standard for handling unstructured data: Structured data are stored in relational databases and queried through SQL for example. However, unstructured data are stored in different types of NoSQL databases without a standard querying approach and that can pose challenges for their integration or interface.

• Technical skills to leverage newer aggregation tools: Companies that are keen on leveraging big-data tools often face a shortage of talent to plan, execute, and maintain systems.

Next, the information is made useful to the end-user in different ways. This could be via an alert to the user (via email, text, notification, etc.). For example, a text alert when the temperature is too high in the company's cold storage.

In other words, it's not always a one-way street. Depending on the IoT application, the user may also be able to perform an action and affect the system. For example, the user might remotely adjust the temperature in the cold storage via an app on their phone. On the other hand, some actions may be performed automatically. For instance, rather than waiting for you to adjust the temperature, the system could do it automatically via predefined rules. And rather than calling you to alert you of an intruder, the IoT system could also automatically notify relevant authorities.

1) Challenge and implementation:

Challenges facing the adoptions of standards within IoT: Standard for handling unstructured data: Structured data are stored in relational databases and queried through SQL for example. Unstructured data are stored in different types of NoSQL databases without a standard querying approach.

Technical skills to leverage newer aggregation tools: Companies that are keen on leveraging big-data tools often face a shortage of talent to plan, execute, and maintain systems.

User interface for smart customers will be blooming soon: Customer may want to intercommunicate with utility by bidirectional way but not in a unidirectional way, or by nonnative communication like before. Implementing a good bidirectional communication must be based on the good telecommunication in the fields of hardware, software and firmware. Challenge for SEC is how to build up a functional platform to effectively communicate with its customers in manner that meets the needs of both customers and the utility at large.

G. Intelligent Analysis & Actions

The last stage in IoT implementation is extracting insights from data for analysis, where analysis is driven by cognitive technologies and the accompanying models that facilitate the use of cognitive technologies.
This entails first, intelligent analysis regarding artificial intelligent, analytic software & real time data processing

H. Driving Factors

• More readily available large data set: Artificial intelligence models can be improved with large data sets that are more readily available than ever before, thanks to the lower storage
• Growth in crowdsourcing and open- source analytics software: Cloud-based crowdsourcing services are leading to new algorithms and improvements in existing ones at an unprecedented rate.
• Real-time data processing and analysis: Analytics tools such as complex event processing (CEP) enable processing and analysis of data on a real-time or a near real-time basis, driving timely decision making and action

1) Adaptation Challenges for intelligent analytics:

• Inaccurate analysis due to flaws in the data and/or model: A lack of data or presence of outliers may lead to false positives or false negatives, thus exposing various algorithmic limitations
• Legacy systems' ability to analyze unstructured data: Legacy systems are well suited to handle structured data; unfortunately, most IoT/business interactions generate unstructured data

• Legacy systems' ability to manage real- time data: Traditional analytics software generally works on batch-oriented processing, wherein all the data are loaded in a batch and then analyzed

Next, are intelligent actions which can be expressed as M2M and M2H interfaces for example due to all the advancement in UI and UX technologies.

I. DRIVING FACTORS FOR ADOPTION

1) Regulatory Standards:

Regulatory standards for data markets are missing especially for data brokers that sell data collected from various sources. Even though data appear to be the currency of the IoT, there is a lack of transparency about who gets access to data and how those data are used to develop products or services and sold to advertisers and third parties. There is therefore a need for clear guidelines on the retention, use, and security of the data including metadata (the data that describe other data).

2) Technical Support for the Service:

Many cloud-based services are known for their ease of use, but there will come a time when you will need some technical support. When you use cloud-based services, you'll be entrusting a lot of your business data to the service's servers, so it's only right for you to have a service representative to consult in case things go wrong. Therefore, before you go with any cloud-based service, make sure that you will be able to receive adequate technical support from the provider.

3) Ownership and Access of your Data:

The application, the hardware and the operating system will be owned by the cloud provider. However, the data is what your intellectual property is based on and it has to be clearly acknowledged in the contract that you can take that data away whenever you want to. Your Cloud subscription gives you access to the functionality of the application or function that you use. That raises the question, if that access is removed, whether you can still have access to your the data so that you can take it away with you. The answer is to ensure that the contract allows for access to the back-end data, either directly or via the provider offering an export capability,

even after the contract has terminated or ended, as shown on Fig. 4.

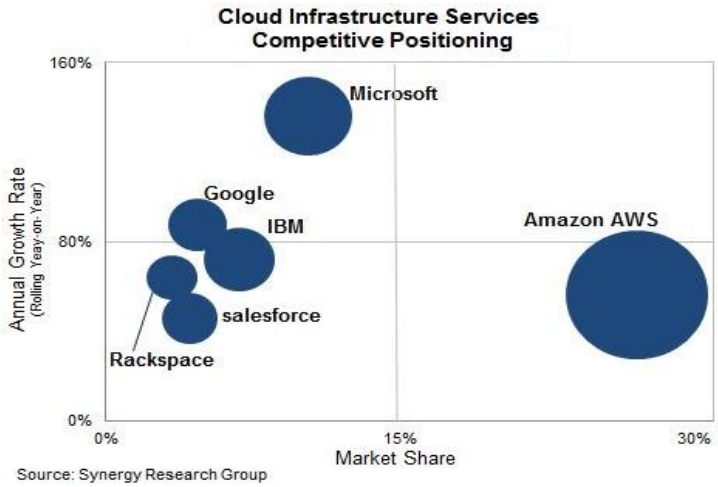

Fig 4. Cloud infrastructure services competitive positioning

4) Cloud Infrastructure:

Some countries such as Spain have prescriptive requirements for security set out in their legislation, that requires the cloud computing service provider to confirm that its security arrangements meet those laws.

5) Compliance:

Organizations which will use Cloud services should perform a gap analysis between the specific requirements identified in relevant regulations and the set of controls provided by the Cloud service provider. Using Cloud computing services for data and applications subject to compliance regulations should require high degree of transparency on the part of service providers.

6) Cost Analysis:

The business case for Cloud application migration is never complete without taking the target Cloud platform into consideration. The migration and overhead costs vary widely based on the target Cloud platform and thus will skew the estimated cost savings.

Cost analysis helps decide whether to go ahead with moving an application to the cloud or not from a return on investment perspective. Cost should include capital expenditure, operational expenditure, and the overhead costs involved with migration.

7) Data Migration:

This is the most important task for cloud computing vendors because this will not only deal with the future efficiency of the application but also the security of the data. The vendor should have a detailed plan including the time frame for data migration.

8) Security & Privacy:

Security is very important when moving r data to the cloud; the cloud provider should therefore work with fully secure cloud environment.

9) Service Quality:

Service quality is often one of the most significant factors that businesses cite as a reason for not moving their business applications to the cloud. Often businesses feel as though the SLAs provided by the cloud providers today are not adequate to assure the requirements for running their business applications on the cloud, especially those related to availability, performance and scalability.

10) Access to Data:

The major problem many organizations face regarding access to data in cloud-based servers do come or emanate from lack of most effective or appropriate customer service support systems. Ensuring that all of the applications are able to seamlessly integrate with one another is also a common challenge.

11) Availability and Reliability:

Availability and reliability are a service provider issues. For instance, there is no doubt that delivering on a stringent SLA requires a commitment to best practices, a thoroughly reliable and dependable architecture.

12) Lack of Skills, Knowledge and Expertise:

Many IT organizations, and cloud may not have the necessary tools or resources to implement, monitor and manage cloud solutions. Consequently, educating staff on new processes and tool sets, or hiring staff with required skills, may be necessary so as to ensure that the organizations' operations and applications move to the cloud effectively and successfully over time.

13) Performance and Bandwidth Cost:

Businesses can save money on system acquisitions, management and maintenance, but the problem this may entail or demand spending more on the bandwidth especial, for the data-intensive applications. Delivering and receiving intensive and complex data over the network requires sufficient bandwidth to stave off latency and application time outs.

14) Integration with Existing Infrastructure:

This is a difficult yet essential piece of maximizing the value of cloud services. This can be achieved by developing a cohesive strategy; an effort that is paramount and that will be aided greatly by a good governance strategy, first at the corporate level and then within the IT business units.

IV. SMART BUSINESS OPTION

While many IoT applications may attract modest revenue, some can attract more. For little burden on the existing communication infrastructure, operators have the potential to open up a significant source of new revenue using IoT technologies, as shown on Fig. 5.

Consumer IoT includes the connected devices such as smart cars, phones, watches, laptops, connected appliances, and entertainment systems.

Commercial IoT includes things like inventory controls, device trackers, and connected medical devices.

Industrial IoT covers such things as connected electric meters, waste water systems, flow gauges, pipeline monitors, manufacturing robots, and other types of connected industrial devices and systems.

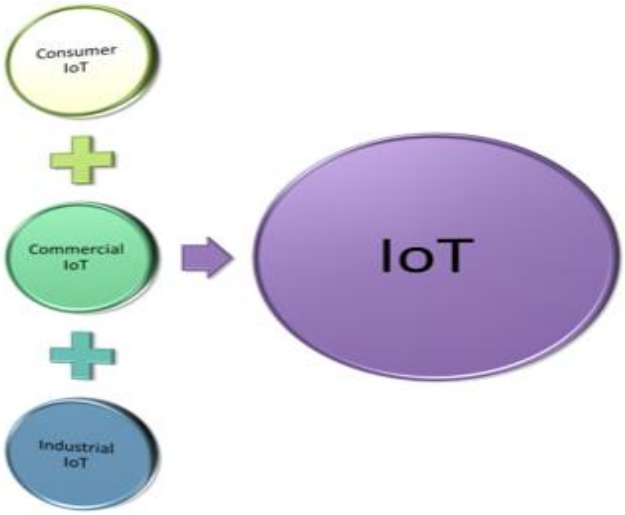

Fig 5. Revenue using IoT technologies.

V. INTERNET OF THINGS 'PICKING UP' IN THE SAUDI ARABIA

New research conducted by the International Data Corporation (IDC) indicates that the popularity of Internet of Things applications are growing across Saudi organizations, driven by the increasing number of IoT offerings from telecoms companies and system integrators.

KSA IoT and M2M Communication market is estimated to grow from $4.88 billion in 2014 to $16.01 billion by 2019, at a Compound Annual Growth Rate (CAGR) of 26.8% from 2014 – 2019. The KSA IoT and M2M communication market is primarily driven by requirement of M2M control system in transportation and automotive sector.

Internet of Things (IoT) is described as network of networks and it is a central part of Future Interne. In simple terms, IoT is like layer of digital information that covers the physical world.

M2M Services adopted by Business in Saudi Arabia cover a range of activities within the kingdom (automotive, healthcare, construction, and utilities) and require flexibility and scalability that can be delivered through cloud. Apart from this, there are agreements that IoT also provides single platform with potential to reach the global markets.

Security and monitoring, smart grid, and smart traffic are some of the emerging IoT applications expected to become more widespread across the kingdom over the next few years.

Organizations across a number of verticals in Saudi Arabia are intensifying their efforts to implement the latest ICT solutions in a bid to improve operational efficiencies and enhance the customer/citizen services they provide. At the same time, the share of Internet of Things applications within the ICT ecosystem is growing. While most of the applications are essentially ICT, IoT solutions are increasingly being applied, particularly in Smart City projects. Similarly, Internet of Things development in Saudi Arabia, is the fixed and mobile infrastructure across the country, enabling telecoms companies to offer IoT services.

Saudi Arabia is still in the early stages of economic diversification and private sector development. In the future, more opportunities will arise to deploy smart solutions as part of ongoing infrastructure projects. In fact, IDC recommends that telecom Companies in the country should pioneer smart project initiatives and drive the development of new solutions.

Saudi telecom should not be overly cautious in their approach. They should be proactive in capturing opportunities by driving market development and building end-to-end solutions, rather than restricting themselves solely to providing connectivity.

VI. CASE STUDY

Many companies use IoT and cloud computing in their facilities, equipments, fleets and most of their business, in this part we will discuss two case study

A. *Sensors and Intelligent Analysis*

Sensors and intelligent analysis are playing a curial role for IoT, the first are collecting the data and the second is transforming these data to valuable information.

1) SEC:

SEC will be our case study. To reduce energy, and costs. SEC is moving to new buildings in Riyadh as shown in figure 6 this building consist four towers and each one has many offices and meeting rooms. Sec has established building management systems (BMS) and IoT system as shown in Fig 7. BMS is collecting different data from the environment of the building and send it to the servers and convert these data to valuable information to act. By using the IoT sensors and BMS the SEC can control the light, so when the offices and meeting rooms are empty the lights will be off. By this way the cost of energy will be save about 50%. SEC will not only decrease the cost, but it can use the data are coming from these sensors to understand the behavior of employees and to marge these data with BMS, also these two technologies will be used to control the ACs in the future.

Fig 6. SEC new building

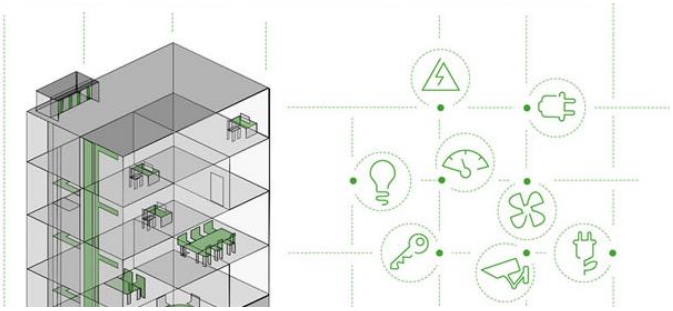

Fig 7. BMS with IoT

2) AT&T:

AT&T company will be our case study. To reduce energy costs and greenhouse gas emissions (GHG), AT&T has incorporated the IoT, connectivity with legacy building information to identify when facility equipment is operating inefficiently. The AT&T

IoT Professional Services group, experts in the design, testing, and implementation of IoT projects, has worked with the AT&T Energy team to use IoT sensors to gather data on previously unmonitored equipment and merge it with data from existing BMS. To go into this case study AT&T set out to create a single platform to track facility equipment data. AT&T IoT Professional Services worked closely with the AT&T Energy team and other technology collaborators to develop reporting platforms comprised of two primary internal data sources: BMS and IoT Sensors.

The IoT-Enabled Building Energy Management system not only collects information from the IoT sensors and BMS, but also integrates other data that aids in analyzing building efficiency such as the building portfolio details, utility data and weather details. The data from all these sources is transported over the AT&T network into a virtual cloud. It then is analyzed and presented to managers and technicians via a dashboard equipped with easy-to-read reports. The IoT-Enabled Building Energy Management system also provides AT&T with tools to create customized data visualization, analytics and fault detection. The AT&T network allows the system to share this information with the facility management team much faster and more securely than before.

AT&T reduced energy consumption and associated GHG emissions by using the IoT-Enabled Building Energy Management system to actively monitor equipment performance across a large portion of the portfolio. In 2017,

AT&T managers evaluated 2,900 Facility Improvement Measures (FIMs) at over 350 facilities, with heating and cooling efficiency representing much of the work.

In sum, the system enabled $925,000 in annualized electricity savings and a 9 million kWh energy reduction in 2017. The effort is ramping up in 2018, and we expect to see significant incremental energy savings over time. This electricity savings equals almost 5,150 metric tons of CO2.

B. *Cyber Security and IoT*

IoT collect the data and send it to server or cloud, these data are valuable for hackers especially if these data are coming from sensitive places.

1) SEC:

SEC has a Cyber Security Strategic Initiative to enhance information security posture at the Sector to ensure confidentiality, integrity and availability of information and to protect the data and digital environment from the access of the hackers and enemies with malicious intentions. It also to ensure resilience of business dependent on IT and OT and to minimize downtown, make the users satisfy and minimum possibility of breach of SLA. The comprehensive Cybersecurity strategy adopted to ensure ration investments in various initiates for cybersecurity. Elevate SEC security posture by 20-40% to be in line with leading utilities. Avoid potential cyber-attacks cost will be roughly about 2% of CAPEX and 1% of OPEX per year and.

The investment in cyber security would avoid the cost resulted from cyber security attacks and the consequential cost on the oil and gas industry and other businesses in the Kingdom.

The annualized cost of cybercrimes impacting utilities and energy sector organizations in 2014 is estimated to range from SAR 50 to SAR 225 million with 10% annual projected increase of cyber-attacks cost. The consequential impact of power loss on the Kingdom and the oil and gas sector could be 20-100 times higher.

SEC is embarking on IT transformation program in which new technologies are acquired and new IT services are introduced. As a result, the cyber exposure of SEC in increasing taking into consideration the following internal and external factors, for internal factor (i) Increased adoption of new technologies and services with new delivery channels to beneficiaries and integration between IT and OT, (ii)Smart metering mandate, (iii) Expanding populations of devices. External factors (i) The power sector continues to be one of the most targeted globally, (ii) Saudi national interests, including Saudi Aramco, have already been subject to targeted cyber-attack from other nation states.

As shown in Fig 8, the development of the cyber security strategy took into consideration several strategic inputs as follows:

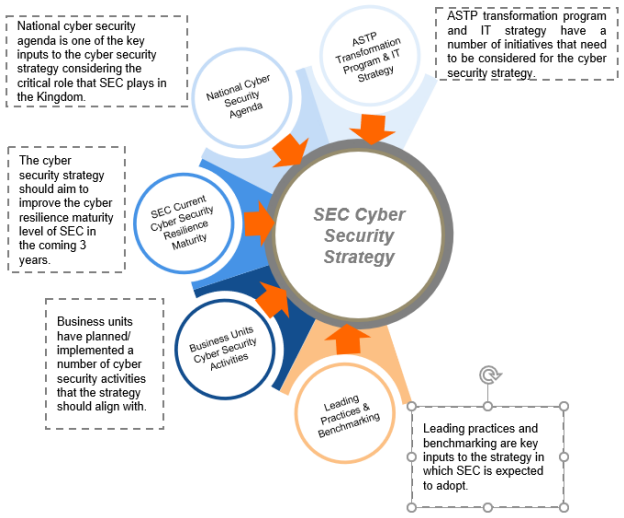

Fig 8. Strategic inputs

The SEC cyber security resilience maturity level, based on the Information Security Forum (ISF) benchmark results, indicates that SEC is below the average of utilities (10-15 utility organizations) in most areas.

The cyber security strategy should take into consideration improving the SEC cyber security resilience maturity level by 20-40% to be in line with leading utility organizations by 2017 as shown in Fig. 9.

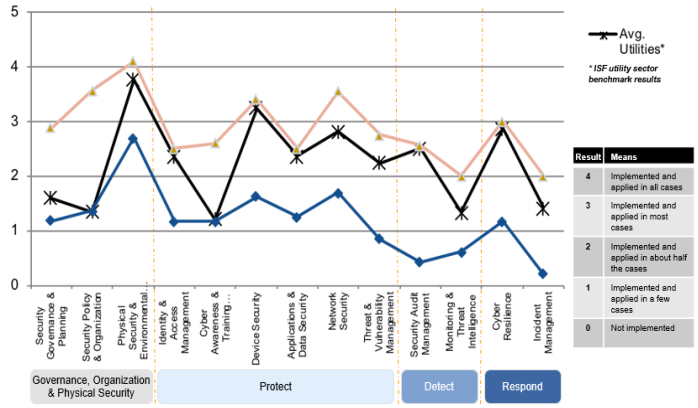

Fig 9. Overall SEC cyber security resilience maturity compared with utility sector average

VII. CONCLUSION

This paper introduces IoT and cloud computing and presents some of the key challenging issues and opportunities resulting from the overwhelming innovative technology revolution towards the Kingdom's vision 2030. IoT has been growing at very high speed nowadays and provide the value for real time reaction and business intelligence for many applications in industry, commercial and customer area for the country and also specifically for SEC. IoT has the characteristics of variety, volume, veracity and velocity. The application involves in hardware, software and firmware that highly connect to the telecommunication, database integration and data analytic capacity. The Challenge for SEC is to select suitable sensors/devices with suitable connectivity that can talk well to data processing software in forms of cloud computing or fog computing and provide customers with good platform to implement big data application.

An IoT ecosystem consists of sensors/devices, connectivity, data processing and a user interface. Sensors/devices mainly focus on the function of data reading, writing or collection, and application and vary from simplicity to complexity that influences the choice of what kinds of sensors/devices could be applicable.

Connectivity is highly connecting to telecommunication application regardless of whichever wire, wireless or hybrid system is used, but wireless is prevalent due to its scalability and availability. Cost and capital investments vary with quality of services. Data processing is connecting to traditional structure database and IoT-based unstructured database, and therefore cloud computing mostly focuses on a huge centralized database processing for creating business intelligence. On the other hand, fog computing plays a key role mainly in distributed computing for instant reaction application. User interface determines the requirements where the unidirectional or bidirectional telecommunication should be provided/offered/implemented.

Issues and challenge for SEC in IoT and cloud computing could emerge in many ways. For IoT, the challenge could show up in technology including security, connectivity, compatibility & longevity, standards, and intelligence analysis & actions respectively. The establishment of appropriate standards, big data processing capacity, and connectivity infrastructures are fundamental for implementation of successful IoT application. For cloud computing, technical support, cloud infrastructures, data accessibility, availability, reliability and migration, legal compliance, uptime & downtime, and cost analysis are also of paramount importance for is successful implementation.

In conclusion, hardware assessment and deployment, and software installment, operation and maintenance in electric sector to meet the power vision 2030 depend on well planned roadmap in terms of IoT, connectivity, database integration and big data analytic processing capacity. Skills, knowledge and expertise, performance and cost, database integration are some of the main challenges for SEC. Thus, SEC needs develop the appropriate roadmap and action plans that includes amongst other things recruit recruitment of talent engineers, prepare financial and commitments support, and relevant infrastructures for building platform of big data and artificial intelligence to create business value and meet the vison of power 2030.

VIII. REFERENCES

[1] Hao Chen, Network Technology Research Centre, China Unicom Research Institute, Beijing 100032, China.

[2] Saudi Electricity Website.

[3] AT&T Website.

[4] DavidBarton, https://channels.theinnovationente rprise.com/articles/158-7-uses-for-analytics-insmart-cities

[5] Case study on multiscale climate data In: Proceedings of the 3rd IEEE International Conference on Cloud Computing Technology and Science, Divani Caravel, Athens, Greece.

[6] Lu S, Li MR, A framework for cloud-based large-scale data analytics and visualization.

[7] Prof. Nick Cercone, Big data analysis for Smart Cities.

IX. BIOGRAPHIES

Saleh AL Saleh was born in 1963, he has a PHD of Science from Tulane University, USA in 1999. He worked in many places such as: Saudi Electric Company, Naif Arab University for Security Science (NAUSS), Imam University. He has many certificates such as: CCNA, Java, ICDL, Oracle, VB. NET, PMP, ITIL Foundation , ITIL Service Manager. He has published many paper with following titles: DSS Crisis Management, Cadet Discipline ▪ Service object architecture(SOA) ▪ Expert System, ERP, Role of Augmented Reality in smart grid, Cloud Computing and Internet of thing (IOT).

Abdullah Odeh He is an electrical engineer who specialized in IoT and control systems. He achieved two prizes in IoT fields. The first-place award in King Abdelaziz City for Science and Technology in Mobtakron for renewable energy fields with IoT solution for solar systems. The best idea award in Thaka centre in King Saud University in Hackathon Arabia with smart fitbit.