8 BENEFITS AND RISKS OF IOT AND CIVIL SERVICE WEB APPS FOR GOVERNMENT

Dr George Gerber
Associate director, Uhambiso Consult (george@uhambiso.co.za)

ABSTRACT

The internet of Things (IoT) and application (app) economy in South Africa can provide the benefits of mobility and improved asset management for many aspects of civil service and business.

Globally, the number of devices connected to an IoT platform is expected to increase significantly, from 400 million in 2015 to 3 billion in 2020, as governments and industries begin to explore IoT solutions to solve region-specific challenges. Furthermore, the presence of 29 million smart devices in South Africa is a significant indicator of the potential growth of apps in industry.

A key benefit for government is the ability to collect big data and derive meaningful and accurate information using data analytics for use in asset management, policymaking, interventions and support measures. With these big data foundation blocks, government can solve higher-level issues, such as managing real time demand and energy costs.

The rising dependence of economic and social systems on information technology has directly increased the risks to these systems from cyberattacks. By making attacks more expensive or less profitable, the economics of the attack process can be changed and the success rate of attacks reduced.

The technology is readily available and South Africa will need to invest in the next generation IoT support staff to maximise the benefits of this technology and achieve its development goals.

1. INTRODUCTION

The South African constitution mandates municipalities with the provision of public services to meet the basic needs of its citizens. The internet of Things (IoT) and application (app) economy in South Africa can provide several unique opportunities for municipalities to automate data collection, increase efficiency, reduce costs, improve asset management and offer new services.

This paper discusses how IoT and information technologies, such as civil service web apps can be used to improve their asset management systems. It lists eight application areas for these technologies. The paper discusses the main wireless technologies that are available and their constraints. It also identifies various challenges for adopting IoT projects, specifically security. Finally, the paper draws conclusions and provides recommendation for implementing IoT projects.

1.1. The rise of IoT

The Internet of things (IoT) is the inter-networking of physical devices, vehicles, buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data (Internet of things, 2017).

Globally, the number of devices connected to an IoT platform is expected to increase significantly, from 400 million in 2015 to 3 billion in 2020, as governments and industries begin to explore IoT solutions to solve region-specific challenges.

1.2. What is a web app?

A web app is a client-server application in which the client runs inside a web browser on a desktop, tablet or smart phone (Web application, 2017). The presence of 29 million smart devices in South Africa is a significant indicator of the potential growth of apps in industry.

1.3. Using IoT and web apps to build Smart Cities

A smart city is an urban development vision to integrate information and communication technology (ICT) and Internet of things (IoT) technology in a secure fashion to manage a city's assets (Smart City, 2017).

The working principle is that IoT devices measure conditions on site and sends these measurements to servers in the cloud for monitoring purposes. These IoT devices can also perform actions, based on predefined rules or from instructions received remotely from an operator. A webapp provides a simple, yet powerful user interface to view the measurements and interact with the remote IoT devices if required.

The following is a simplified application example of IoT in disaster management: While drivers are commuting their GPS enabled mobile phones autonomously monitor traffic congestion throughout the city. The server receives this information and visualises the congestion on an online map to the traffic department. IoT enabled traffic lights to regulate autonomously the routine traffic conditions. A disaster occurs in a congested part of the city and an operator instructs all the traffic signals to reroute traffic away from the area, while allowing easy access for emergency vehicles into this area.

A key benefit of IoT and information technology for government is the ability to collect big data and derive meaningful and accurate information for use in policymaking, interventions and support measures. With these big data foundation blocks, government can solve higher-level issues, such as managing real time demand and energy costs.

1.4. Technological advances that have supported IoT and smart apps

Several advances in technology have laid the foundation for the internet of things. These include:

- Wireless communication: Allowing people and objects to move freely, while being connected to the internet. Wireless standards vary from short range-low power-high bandwidth standards, such as Bluetooth and wifi, to long range-high power-high bandwith standards, such as cellular 2G, 3G, LTE. The emerging long range-low power-low bandwith standards, such as (Sigfox) has recently also entered the market.
- Low cost realtime clock and GPS modules: These modules have added a temporal and spatial context to measured data.
- Low cost sensors.
- Improvements in microprocessor technology: These processors are allowing data to be collected, aggregated and decisions to be made at the "edge" of the IoT network (where the process is monitored). A remote device can therefore act autonomously, if required, without uploading measurements to the cloud and waiting for a response from an operator.
- Databases with spatial indices and queries: These databases provide answers to important spatial queries. For example, how far and where is the nearest service X from a given coordinate?
- Availability of online maps: Data can now easily be overlaid onto a map to provide a clear spatial visualization of the location of people and assets. This provides an essential spatial context for making informed and spatially efficient decisions.
- Improvements in web technologies: Modern web frameworks allow information to be pushed back automatically to web clients, such as web browsers, when a change to the database is detected. This allows all clients to view the latest data at any time.

2. IMPACT ON ASSET MANAGEMENT SYSTEMS

A common application of IoT is for physical asset management, monitoring and predictive maintenance. Asset monitoring systems are a powerful tool for making assets work harder, smarter and allowing them to deliver greater value. The business challenge is to keep these key assets operational for as long as possible without sacrificing reliability or safety, at an acceptable cost.

The key advantage of IoT is the ability to remotely monitor the business process and seamlessly integrate the data with a unified asset management solution so that the management has the best insights to make the right decision.

Automated data acquisition has countless advantages over traditional manual measurements:

- Sensors can be placed in environments hazardous to human operators, or in remote or inaccessible locations.
- Data acquisition are often made to greater precision, the frequency of these measurements can be adjusted quickly and easily, and they are not prone to transcription errors.
- Automated data acquisition is less labour intensive. Advanced sensors can even calibrate themselves periodically and diagnose faults, reducing sensor-servicing costs.
- The speed at which data can be collected, processed into information and fed into a decision support system can be executed near real time.
- Intelligent edge nodes using sensors and microcontrollers can bring the decision support system nearer to the edge of the process. These microcontrollers can process the data and perform routine actions, without connecting to the control centre in the cloud. This provides near real-time decision making.
- The human intervention is needed only for high level decision making. Mundane tasks and rule-based actions can be automated with a decision support system.
- Non-compliance can be eliminated by automated monitoring, reporting and scheduling of maintenance.

3. MUNICIPAL APPLICATION EXAMPLES OF IOT

IoT can be applied to several areas where municipalities provide basic services. The following section provides a brief list of applications (Dlodlo, Olwal, & Mvelase, 2012). The application areas are:

- Water supply
- Sewage collection and disposal
- Refuse removal
- Electricity
- Traffic and parking
- Disaster recovery
- Public health services
- Public safety

3.1. Water supply

Water quality can be monitored at critical locations in a town's water supply reservoir. The measurements can be sent wirelessly to the treatment works and provide pro-active warning of pollution incidents in the reservoir. The treatment works can mitigate the impact of the pollution before it reaches consumers.

Water meters can send measurements wirelessly to water service providers to help detect leaks early and to improve consumption estimates. Consumers can also view a detailed time record of their consumption which will assist them in reducing their consumption.

Pumpstation and treatment plant control equipment can monitor key performance variables and relay this information to a SCADA system. The operator can stop/start various parts of the plant through a web interface. These devices can also inform the SCADA server or operator of their condition in order to schedule repair and maintenance activities in an efficient manner.

3.2. Sewage collection and disposal

The status of the pumps in a pumpstation can be monitored remotely and they can started and stopped remotely as well (Figure 1 and Figure 2).

Level sensors can be installed at key locations in the network and wirelessly send an alarm when it is about to overflow, so that preventative action can be taken. The sensor data can be overlaid on a map to identify surcharging areas in the system (Figure 3).

The public can tag burst pipes or overflowing manholes using an app on their mobile phones. This method of crowdsourcing can assist maintenance teams in finding problems.

3.3. Refuse removal

Refuse bins can monitor their capacity and wirelessly inform sanitation workers where it is located and that is full and ready for collection.

3.4. Electricity

Smart homes will provide a Home Area Network for various IoT appliances (hot water geyser, television, oven etc). These appliances will monitor their energy consumption and relay this information via the Home Area Network to the owner. These devices will be able to adjust their operation in order improve the overall efficiency of the home or comply with load shedding requirements communicated from the electrical grid.

3.5. Traffic and parking

Camera technology is successfully being used in cities to identify speedsters and red-light violators. The photographs of the offenders can be sent remotely to the traffic department. Image processing technology can automate the process of identifying the vehicle number plates and sending fines to the registered email address.

E-tolling is already being used to toll road users, without creating traffic congestion. A small radio transmitter in the vehicle sends the vehicle registration details remotely to a receiver at the toll. The road user is automatically billed via email.

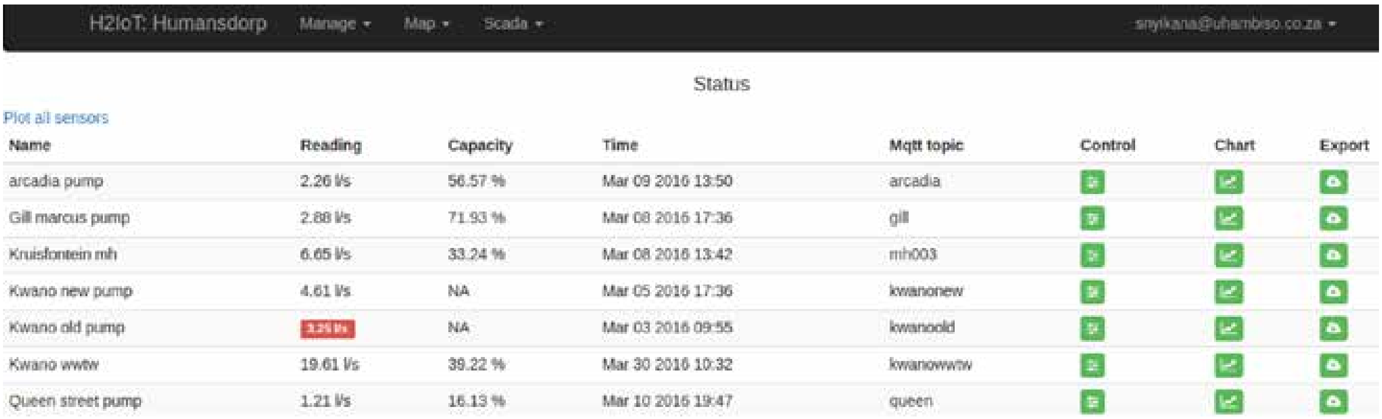
Crowdsourcing of mobile phone GPS data is also being used to map traffic congestion to guide emergency services and road users along the best routes.

Motion sensors and GPS speed/acceleration data in a driver's mobile phone can indicate to insurance companies whether a driver drives aggressively or dispatch emergency services in the event of an accident. This information is sent using the cellular network.

A parking sensor can detect whether its space is occupied and send its status to a remote server. The parking rate can be adjusted depending on the demand and congestion can be reduced by guiding vehicles to areas where parking is available.

Smart street lights can switch themselves on or off depending whether there is sufficient sunlight. They can also vary their brightness depending on whether they detect traffic nearby.

Bridges and low-level river crossings can have sensors monitoring water levels and inform oncoming traffic whether it is safe to cross or redirect them to an alternative crossing. Similarly, sensors in tunnels or railway tracks can identify accidents or smoke/fire conditions and redirect oncoming traffic.



Name	Reading	Capacity	Time	Mqtt topic	Control	Chart	Export
arcadia pump	2.26 l/s	56.57 %	Mar 09 2016 13:50	arcadia			
Gill marcus pump	2.88 l/s	71.93 %	Mar 08 2016 17:36	gill			
Kruisfontein mh	6.65 l/s	33.24 %	Mar 08 2016 13:42	mh003			
Kwano new pump	4.61 l/s	NA	Mar 05 2016 17:36	kwanonew			
Kwano old pump	[illegible]	NA	Mar 03 2016 09:55	kwanoold			
Kwano wwtw	19.61 l/s	39.22 %	Mar 30 2016 10:32	kwanowwtw			
Queen street pump	1.21 l/s	16.13 %	Mar 10 2016 19:47	queen			

FIGURE 1: Example pumpstation status page

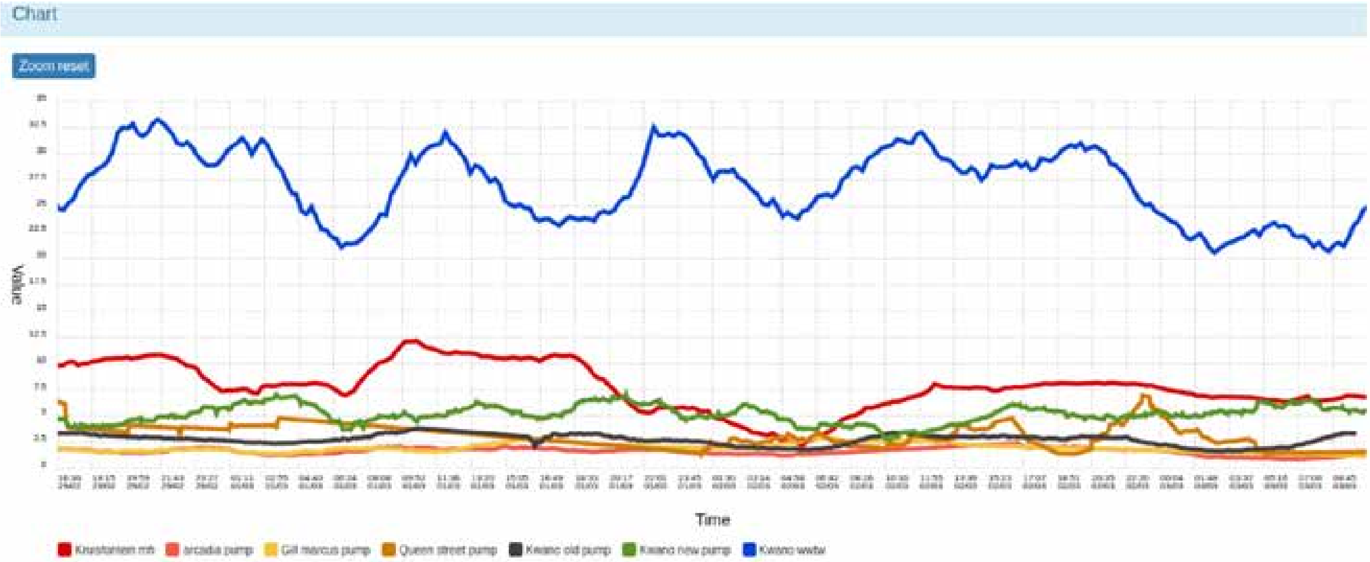


FIGURE 2: Example pumpstation output history page

3.6. Disaster recovery

Disasters can include storms, flooding, fires, earthquakes and transport accidents. Sensors can be placed to monitor the structural stability of key public infrastructure, such as bridges, dam walls and other flood prevention infrastructure. Buildings can have smoke and fire detection sensors and autonomously warn the fire brigade and route people inside the building along the safest route.

These early warning systems can provide timely alerts to the public in the affected area using various communication mediums.

Traffic lights can be remotely controlled to improve mass evacuation out of disaster areas. Mobile phone GPS measurements can provide information on the volume of people moving through certain areas, and assist rescue teams in locating missing persons.

3.7. Public health services

Wearable devices can monitor key vital signs, such as heart rate, blood pressure. The movement of elderly people can be tracked and changes in their behaviour identified.

These sensors can transmit their measurement via Bluetooth to a mobile phone or remote gateway, where emergency services can be notified of an emergency.

Furthermore, the location of medical waste bags can be monitored to ensure correct disposal. Finally, medical cabinets can dispense the correct medication to the elderly and wirelessly inform service providers when it needs to be refilled.

FIGURE 3: Example mapview with pumpstation outputs

3.8. Public safety

Handheld devices by traffic and police officers enable them to scan a driver license or identity document on site and query a remote server whether the motorist is unlicensed or wanted by the police.

Facial recognition technology may in future also be used to identify criminals walking into malls or other areas using smart surveillance cameras.

Research is being done to locate the origin of gunshot sounds. These sensors will be able inform the police of the time, number and location of gunshots.

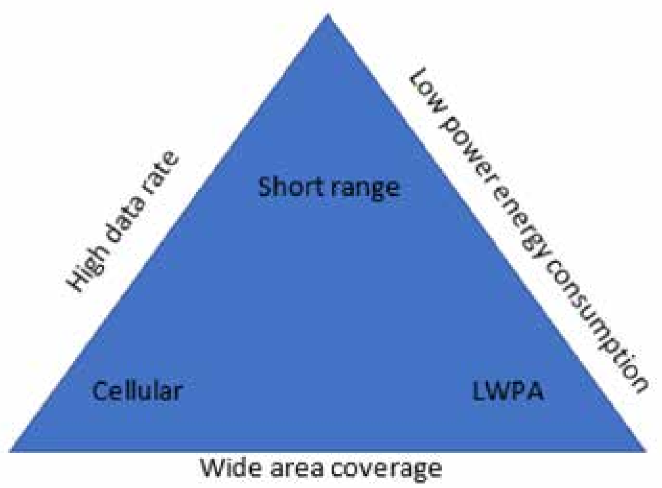


FIGURE 4: IoT communication constraints

4. IOT CONNECTIVITY TECHNOLOGIES

There are various methods by which an IoT device can connect to the internet and communicate with cloud servers. These range from wired connections (ethernet) to wireless connections (wifi, 3G etc). This section will discuss the constraints for a wireless implementation, as this option has the most applications for municipalities.

Figure 1 presents the main technologies and constraints for a wireless implementation. The main constraints are:

- Device power requirements
- Bandwidth
- Area of coverage

The three main technologies available to address these constraints are:

- LAN short range
- Cellular long range
- Low power wide area networks (LWPA)

The ideal wireless technology would have:

- low power requirements: It would use a single battery for years, as opposed to regularly being recharged like a mobile phone or wired to a power source.
- High bandwidth capability: It would be able to stream substantial amounts of data very fast.
- Wide area coverage: It would be able to communicate through trees and buildings for long distances (10's of kilometres).

Table 1 summarises the advantages and disadvantage of each of these technologies. It shows that, unfortunately, none of the technologies can satisfy all three main constraints. This means that the selected technology needs to be appropriate for the project conditions. For example, if small data volumes are needed for real-time analysis and reporting, such as fault codes generated by on vehicle intelligent systems, data streams over mobile networks are used. If, however larger data volumes are needed for detailed off-vehicle analysis, the acquired data is often cached on the vehicle and then off-loaded in batches via WiFi at designated access points such as stations or depots.

5. CHALLENGES FOR ADOPTING IOT

There are several challenges that municipalities could face when adopting IoT solutions. These are:

- Strategic leadership: A lack of strategic leadership from government about how to utilise IoT
- Skills: Municipalities may not have enough workers with the required technical skills to effectively use the IoT generated data.
- Funding: Municipalities may not have the funding to modernize their IT infrastructure and implement IoT projects.
- Policies: Procurement policies could make it difficult to easily adopt these technologies
- Security and privacy: Cyberattacks will become more frequent and the protection of confidential data and municipal assets require the implementation of a robust security layer on top of the IoT infrastructure.

5.1. IoT security concerns

The rising dependence of economic and social systems on information technology has directly increased the risks to these systems from cyberattacks.

By making attacks more expensive or less profitable, the economics of the attack process can be changed and the success rate of attacks reduced.

Crowdsourcing and sharing information about attacks more broadly is one of the critical initial steps that can be taken to improve security.

Cybercriminals have managed to compromise many insecure IoT devices and use them for their own purposes in Distributed Denial of Service DDOS attacks. These attacks are aimed at shutting down an essential service, such as Twitter or Paypal, by using the devices to bombard the service with fake queries. The service shuts down when it is unable to keep up with the enormous number of queries.

There are several reasons why IoT devices have had security problems in the past. These include:

- Desktop computers have had many decades to mature in terms of security and therefore have built in security features, such as firewalls and anti-virus scanning. On the other hand, IoT devices are very new and have initially been aimed at the consumer market. This market regularly makes its purchasing decisions based on cost and number of features and rarely on security. Time to market pressures have caused manufacturers to focus more on features than on security.
- Many of the IoT devices do not have the processing power to use high levels of encryption, due to their low power and low-cost design.
- The more devices a user owns the more firmware updates are required to patch security vulnerabilities. This problem is compounded when the devices are in hazardous or remote areas.

5.2. Minimum security requirements

The following is a non-exhaustive list of security issues that need to be addressed when implementing an IoT project:

- Encryption: All communication between the device and the cloud need to be encrypted. The latest TLS cryptographic protocol should be used
- Authentication: Devices should only be accessible by providing correct authentication credentials. Furthermore, each device should have a

TABLE 1: Suitability of various wireless standards

Type	LAN-Short range	Cellular Long range w power	Low power WAN
Examples	ZigBee 3.0, Bluetooth 4.0, WiFi	2G/3G/4G/H, Lte, Cat-M1/NB 1	Sigfox, Genu, Lightless, Lora, NB-IoT
Standards	Well established	Well established	Emerging
Good for	Mobile, In home, Short range	Long range, High data rate, Coverage	Long range, long battery
Not good for	Battery life, Long range	Battery life, Low OPEX	High data rate

unique username and random password preloaded in order to prevent cybercriminals from compromising a device using factory default passwords, such as admin/admin etc.

- No back doors: Devices should not have back doors for debugging purposes. Cybercriminals will eventually discover these backdoors and compromise the device and its data.
- Updates: All IoT devices should support over-the-air updates. Furthermore, software signing must be used to ensure that the firmware updates are legitimate.
- Privacy: Data on the device should be encrypted along with salts. This will provide a second line of defence, should the device be compromised.

6. CONCLUSIONS

The following conclusions can be drawn from this paper:

1. Future smart cities plan to leverage information and communication technology, as well as the Internet of Things to manage a city's assets in a more effective and secure fashion.
2. A key benefit for cities and municipalities is the ability to collect big data and derive meaningful and accurate information for use in policymaking, interventions and support measures. With these big data foundation blocks, government can solve higher-level issues, such as managing real time demand and energy costs.
3. Municipalities can enhance a wide range of civil services by applying these technologies to their asset management and decision support systems. (Section 2 for examples).
4. Various wireless connectivity technologies exist to connect IoT devices to the cloud. Each of these connectivity technologies have their advantages and disadvantages with respect to power, range and bandwidth (Section 3).
5. IoT projects present their own unique challenges to municipalities, which needs to be addressed to be successful (Section 4)

7. RECOMMENDATIONS

The following recommendations are given:

1. A cost-benefit analysis should be performed before implementing an IoT project.
2. The connectivity technology must be appropriate for the application. Consideration should be given to power, bandwidth and power requirements for the nodes on the edge of the network.
3. The power requirements of the sensors, as well as the environment in which they will operate needs to be considered as well, in order for the system to be reliable and cost effective.
4. Special attention should be given to the securing the system against cyberattacks. Section 4.2 gave a brief list of minimum requirements.
5. In house training and skills development will be required from municipalities to effectively manage the substantial amounts of data generated from a network of IoT devices.

REFERENCES

Dlodlo, N., Olwal, T., & Mvelase, P. (2012). The internet of things in bridging the gap in municipal service delivery in South Africa. *IST Africa*. Dar es Salaam.

Internet of things. (2017, June 9). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Internet_of_things

Smart City. (2017, June 9). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Smart_city

Web application. (2017, June 9). Retrieved from https://en.wikipedia.org/wiki/Web_application