The Utility of the Future

Distributed Power Generation Enabled by the Internet of Things

Author and Presenter: Dr Cathy Pickering, Solution Architect, FuseForward South Africa

Introduction

Up until now, Africa has chosen to meet its growing electrical grid requirements by focusing on large plant investments built and operated over long time-horizons. Consequently, about 91.2% of South Africa's power is currently generated by thermal power stations and only 8.8% is generated from renewable energy sources. The Intelligent Utility of the future will make power generation, distribution, and management more responsive to the needs of the communities it serves. The Intelligent Utility will be composed of a combination of intelligent, dynamic power generation and distribution systems enabled by Internet of Things (IoT) devices. The utility will be managed by a distributed cloud-based grid management system, with an increasing percentage of its power being generated from smaller, more agile renewable energy sources.

The utility of the future, the Intelligent Utility, will be made up of centralised, regional, community and home power plants. It is comprised of interconnected systems (the power generation and distribution systems enabled by IoT) and managed by a distributed cloud-based grid management system. FuseForward sees Municipalities playing an important role by helping their communities become energy self-sufficient with smaller, but modular and scalable, systems that can be deployed rapidly using pre-manufactured components. The major advantage of distributed plants is that it is easier to "ring fence" the data from the plant. Therefore, one important consideration for the Intelligent Utility is how to secure generation system and IoT information to protect this information from cyber-crime.

Research Project

Working with academic institutions in Canada, FuseForward has set up and is part of the Intelligent Systems Research Network, a team of professionals with an interest in the application of big data in various areas. Led by FuseForward, the network is working to develop intelligent IoT and big data solutions that bridge the gap between academia, industry and technology. Our goal is to create new tools that enable operational managers to harness the power of big data and smart devices in a way that is innovative and practical.

The research covers all aspects of analytics for industrial campuses and building portfolios, including streaming data management, real-time facility analytics, and automated control. The smart campus research is looking at the requirements for sustainable buildings which are cooled and heated naturally and are energy efficient. Central to this research is the use of IoT devices.

A current research project focuses on applying Artificial Intelligence (AI) and Machine Learning (ML) to energy management on a university campus in Canada, as well as the development of algorithms and AI integration for deep learning and integrating user behaviour. The research and predictive models developed so far have resulted in the decrease in the use of HVAC (Heating, Ventilation and Air Conditioning) systems and 30% power savings on the university campus. The research involves calculating dynamic set points and providing dynamic control of the HVAC systems using machine learning methods.

The smart campus research and the conceptual model being developed informs the Intelligent Utility research and the development of the Intelligent Utility. The outcome of the smart campus research will facilitate power utilities to get started with the Intelligent Utility.

The Intelligent Utility model requires that a distribution management system is overlaid on the power distribution grid. Further research is underway regarding methods to deal with the dynamic power supply, how to govern the distribution of power and optimize its usage.

What is the Intelligent Utility?

To understand the Intelligent Utility, it is important to understand that the Intelligent Utility is built on the Smart Grid. In 2014 the National Institute of Standards and Technology (NIST) in the US defined a framework and vision for the smart grid. NIST acknowledged that there are various definitions of smart grid but stated that "…*all notions of an advanced power grid for the 21st century include the addition and integration of many varieties of digital computing and communication technologies and services with the power-delivery infrastructure*". Bidirectional flows of energy and two-way communication and control capabilities will enable an array of new functionalities and applications that go well beyond "smart" meters for homes and businesses.

NIST gives nine priority areas for the application and requirements of the smart grid. These key areas are:

1. Demand response and consumer energy efficiency
2. Wide-area situational awareness
3. Distributed energy resources
4. Energy storage
5. Electric transportation
6. Network communications
7. Advanced metering infrastructure
8. Distribution grid management
9. Cybersecurity

Our vision of the Intelligent Utility encompasses these key areas and can be thought of as two interconnected systems; intelligent dynamic power generation and distribution systems, and a distributed cloud-based grid management system—both enabled by IoT. The IoT devices continually feed data into the cloud-based grid management system. This information can be analyzed in real-time to provide automated control of the system, for example predictive algorithms could be used to increase or decrease the power generated based on predicted demand. The power is generated with centralised power plants, supported be regional power plants and home power plants. Both the electricity generation infrastructure and the cloud infrastructure will contain IoT devices and will be enabled by the IoT.

Current power generation is focused on large plant investments with long time-horizons, as mentioned previously. In South Africa, the current centralised power distribution by Eskom will provide the core of the system, the Intelligent Utility will augment this with smaller, modular systems that can be deployed rapidly with pre-manufactured components. The energy generation will be distributed between regional, community and house/building systems with differing power generation rates, such as 500KW to 10MW for regional generation, 50-300KW for community generation and 5-30KW for home generation. This distributed model will do away with the current need to 'step down' the power for communities and home requirements, the distributed model will provide the correct power rating where it is required. The Intelligent Utility will provide dynamic load balancing across these generating facilities and enable full network optimization encompassing the distribution grid and consumption management.

The Intelligent Utility is enabled by IoT, fibre connectivity and cloud-based digital control services that control, manage and analyse the information coming from the entire system. The system is also able to provide internet and application services to consumers, businesses and industry.

Smart meters are not the only IoT devices that are utilised in the Intelligent Utility. Devices such as surveillance cameras, remotely monitored real-time sensors, supervisory control centres and smart devices are also utilised. These devices are strategically placed in the power generation and distribution systems, the communications network, and at the point of consumption. These devices feed data into the cloud-based digital control system, which also has IoT devices for monitoring and securing the state of the cloud infrastructure.

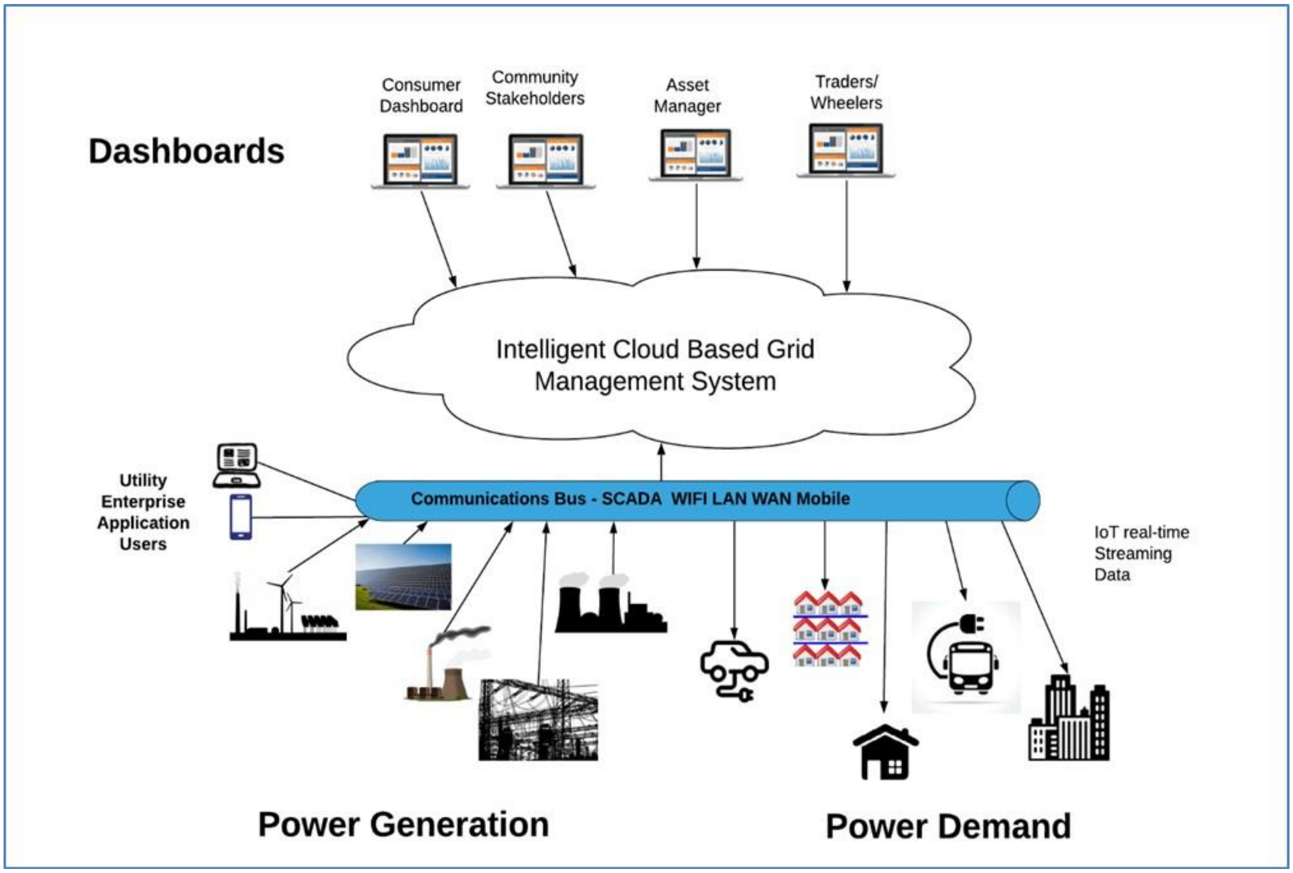
Dashboards
Consumer Dashboard
Community Stakeholders
Asset Manager
Traders/ Wheelers
Intelligent Cloud Based Grid Management System
Utility Enterprise Application Users
Communications Bus - SCADA WIFI LAN WAN Mobile
IoT real-time Streaming Data
Power Generation
Power Demand

Figure 1: Intelligent Utility

Electric Vehicles

A market intelligence report written earlier this year by GreenCape says that public transport in South Africa gives the best business case for electrification, more so than private transport. The South African bus market makes buses that are designed in South Africa for the local market. However, the local bus market is currently flat, the report cites that manufacturing intelligent, electric buses to provide additional services would be a way of achieving a refresh of the industry.

With the current centralised grid system, a municipality with a large electric bus fleet would have the problem of loading the grid when trying to ensure all the buses were fully charged at the start of the day shift. The Intelligent Utility and decentralised power generation provides the solution to this problem. The revitalisation of the local bus market is just one example of the types of innovation and business opportunities that can be created by the Intelligent Utility.

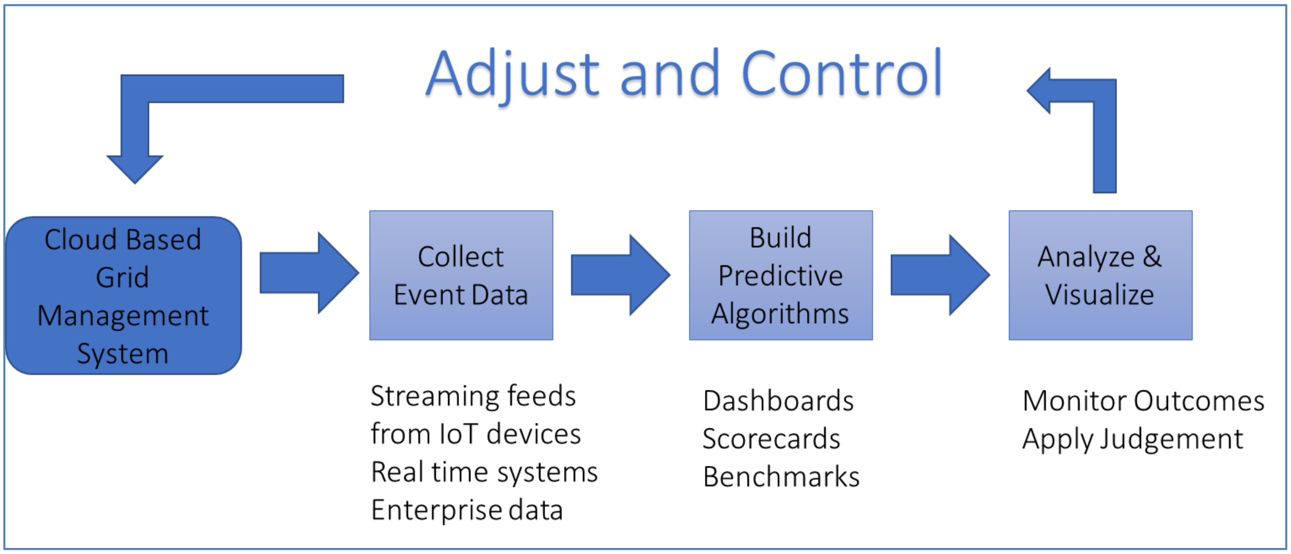

Figure 2: Cloud Based Grid Management System

Key Considerations for implementation

Security

One of the key areas in the NIST framework is cybersecurity. Securing the information and the information systems of IoT devices connecting to the grid is a major challenge.

Globally, the power sector is the most frequently targeted sector by cyber criminals. Cybersecurity attacks threaten the power grid, enterprises, and consumer devices on a nearly constant basis, putting valuable digital assets, private information, and corporate secrets at risk, while also carrying the potential for physical harm. As IoT technologies become more popular, new threats are appearing and the need for stronger IoT security increases. Growing adoption of IoT devices and the systems that support them is increasing the number of vectors and surfaces for cybersecurity attacks against utilities and other enterprises.

In South Africa, a case in point is the recent (July 2019) Johannesburg City Power ransomware attack which took down most of their applications and network, affecting customers' ability to buy prepaid electricity. These attacks are prevalent worldwide—in March a major US utility experienced a serious "denial-of-service condition", and in 2015 an attack in Ukraine left a quarter-of-a-million residents without power for two days.

Although these attacks are not necessarily via IoT devices, research shows an increase in the amount of cyber-attacks targeting IoT devices as the number of IoT devices grows. In 2016, in what is known as the biggest distributed denial of service attack to date, hackers took control of thousands of IoT devices and brought down a European web host. Since then (2018) a global IT security firm reports that the number of IoT threats have doubled. Thankfully, many of these threats use predictable, known techniques to compromise devices, either targeting weak credentials, unpatched vulnerabilities or both. As a result, many threats are preventable by applying good cyber security practices.

The table below gives the potential threats that can affect IoT devices:

Attack Type	**Sub Type**	**Part of Intelligent Utility to be secured against attack**
Nefarious activity/abuse	• DOS • Malware • Manipulation of hardware and software of a device • Targeted attacks • Abuse of personal data • Brute force	• Control systems e.g. SCADA • Software in cloud management system • IoT devices • Mobile devices • Personal data within systems • Communication networks • People
Eavesdropping, interception, hijacking	• Man in the middle/session hijacking • Communication protocol hijacking • Network reconnaissance	• Communications network • IoT devices • Information
Physical attack	• Vandalism/theft • Sabotage	• Power plants • Data centers • IoT devices • Mobile devices • Control systems e.g. SCADA • People
Accidental Damage	• Misconfiguration • Erroneous use or admin of devices • Third-party damage	• Power plants • IoT devices • Control systems • Communications networks • Information • Cloud computing services • Data analytics • Software and licenses • Servers and systems • People
Failures/Malfunctions	• Failure or malfunction of a sensor / actuator • Failure or malfunction of a control system • Exploitation of a software vulnerability • Failure or disruption of service providers	• Power plants • IoT devices • Control systems • Software • Cloud service providers • Information

Outages	• Communications network • Power supply • Support services	• IoT devices • Servers and systems • Control systems • Communications network
Legal	• Violation of rules and regulations / breach of legislation / abuse of personal data ○ POPI (GDPR in Europe) • Failure to meet contractual requirements	• IoT devices • Cloud computing services • Information • Control systems • Software and licenses
Disasters	• Natural • Environmental	• Power plants • IoT end devices • People • Control system • Communications network • Data centres

The Intelligent Utility needs to have the relevant security systems in place, both for physical and IT/information related security. This security should not only deal with known security threats and vulnerabilities, but also to be able to deal with new threats as the cyber criminals develop them. As can be seen from the table above, the security systems required to protect the Intelligent Utility from cyberattacks need to be multi-layered and protect all parts of the Intelligent Utility, not just the IoT devices.

Reliability

From the reliability point of view, failures in a centralized distribution model can lead to blackouts affecting areas as large as a country. The recent blackout in Argentina in June 2019 left the whole of mainland Argentina and parts of Uruguay and Paraguay without power, an estimated 48 million people were affected. In August 2019 a large blackout affected parts of England and Wales, affecting nearly a million people, causing travel disruptions and trapping people in trains for several hours. A distributed generation model, with its built-in redundancy, is inherently more reliable as the total failure of one power plant can be compensated by other plants in the network.

Large power plants require large distribution lines and power step-downs so that the correct power is distributed to the relevant electricity users. As a result, the power is not necessarily generated where it is needed, which means a failure in one part of the distribution network can potentially affect a widespread area, as in the examples above.

Reliability in the Intelligent Utility is provided both by the dynamic power generating systems and the cloud-based grid management system. With the Intelligent Utility model, smaller, independent systems at regional, community and house or building level can continue to operate when there is a power failure elsewhere on the network, providing the required reliability.

IoT devices continually feed data into the cloud-based grid management system. This information is fed into data stores for analysis and can also be put into a machine learning platform. These systems can identify problems before they happen by recognizing failure patterns. This data can increase awareness of grid performance and can also be used for predictive analytics, further increasing system reliability and reducing expenses related to maintenance and outage hours.

Scalability

As identified in the NIST framework, demand response and consumer energy efficiency are key requirements for the intelligent grid. The intelligent grid must be able to scale to meet consumer requirements, deal with burst load requirements, balance domestic and industrial peak requirements. As before, artificial intelligence and advanced analytics in the cloud-based grid-management system can be used to predict expected demands and scale the provision of electricity accordingly. The information from this analysis also assists decisions regarding cost-savings and increased productivity. In competitive markets, optimizing the purchase and sale of power based on instantaneous pricing information offers both tangible and commercial benefits.

As an example, smart meter data can be used for locational load forecasting. As a result, smart meter data becomes the ‘enabler’ of the automated distribution grid. This data can be used to reconcile the activity of controllable devices against the utility’s ability to provide the required capacity and adjust the capacity being supplied automatically.

The Intelligent Utility model encompasses smaller, modular systems serving regional, community and residential or building requirements. This model leads to the physical scalability of the Intelligent Utility. Small home or community systems can quickly be installed as demand increases.

The ability of the distribution grids in the Intelligent Utility to allow two-way distribution of power means that a small home solar system can provide power back to the grid if excess is generated. This leads to further scalability and provides an incentive for homeowners to invest in power-generation assets.

The cloud-based grid management system is also scalable, as it runs on cloud technology which enables IT infrastructure to scale to meet demands. For example, additional IT infrastructure can be provisioned to perform monthly billing runs and then de-provisioned after the billing cycle is complete, thus optimizing the cost of the IT infrastructure.

Role of the Municipalities

The local municipality has a very important role to play in the Intelligent Utility. They can assist their communities to become self-sufficient with the power generated by the regional, community and home-based systems. They will have the role of managing the power generation and distribution systems enabled by IoT and the distributed cloud-based grid management system. They will be in charge of ensuring that the correct levels of security are in place, both physical and cyber, and of ensuring applicable regulations are adhered to.

A discussion paper commissioned by the South African-German Energy Partnership in 2017 reviewed the various business models that municipalities can adopt to benefit from the opportunities provided by domestic renewable energy, while also minimizing the associated risks. These business models can be applied to the role of the municipality in the Intelligent Utility. The roles played by municipalities can be broken down into three classifications; building generation capacity, procuring energy and facilitation.

If the municipality has the role of building generation capacity, they will build and own the regional and community generation systems. By building them on municipal land and municipal buildings, they can make revenue from selling the power generated. If they have the role of procuring energy, then third parties (including IPPs and community groups) will build and own the generation systems.

In the third role, as facilitator, the municipality will procure electricity from the owners of the regional, community and home systems and on-sell to customers. Municipalities will also operate an electricity storage facility on municipal land to store power when there is excess supply and sell it when there is a shortage of power or a time of high demand. Additionally, they may provide services such as installing the community and home systems, providing maintenance services and so on.

A business model that is appropriate for a large municipality will not necessarily suit a small one. The various municipal business models provided by the Intelligent Utility give scope for each municipality to decide which role best suits them. The municipality could choose to implement a combination of the roles, building generation capacity in some areas and playing a facilitation role in other areas. The South African-German Energy Partnership discussion paper outlines concepts that municipalities should consider when deciding what role to take on. The intelligence provided by the system will be an enabler to the municipalities for whichever role they choose.

Challenges

Worldwide the utility/energy sector is risk adverse. New technologies and systems need to be proven before utilities will adopt them. The Intelligent Utility comprises innovative technology which is enabled by IoT. These new and innovative technologies are present in both parts of the system, the intelligent dynamic power generation and distribution systems and the distributed cloud-based grid management system. Integration with legacy systems is another challenge.

Some of the challenges are technical, such as validating and testing the new technology. Some of the challenges are related to people, and whether they are willing and able to use the new systems and accept the changes. Currently many South Africans have smart meters, but in most cases the data that these smart meters provides is not being utilised to its fullest. Typically, the data is only being used for billing purposes and much of the data provided by these devices is simply being discarded. It involves a mindset change to take the available data and use it for predictive analytics and AI purposes. There are also regulatory and financial issues to be taken into consideration.

How to Get Started and Next Steps

FuseForward understands these very really challenges and follows a proven implementation methodology for its solutions and demonstration projects. Our methodology takes into consideration the ability of people and organizations to adopt and effectively use new technology and incorporates an agile incremental release cycle with validation and refactoring of solutions as required. Therefore, our Intelligent Utility implementation follows a phased, a four-step model.

Step 1 – Pilot Demonstration Deployment.

The initial phase of implementation of an Intelligent Utility is the deployment of a pilot demonstration system. The pilot system focuses on the deployment, configuration and initial “template” implementation of the Intelligent Utility for a small community with a small number of IoT devices. In the African context this ‘small community’ could be a collection of homes within a municipality, a university campus, a small neighbourhood or a gated community.

A key part of the pilot deployment is the development of an operational business plan. This plan includes a revenue-based funding model to ensure that the solution does not become a cost-burden to the municipality or other involved players.

Step 2 – Micro Grid Deployment.

Step two expands the deployment of the pilot, using the lessons learned from the pilot phase,. This phase focuses on expanding the use of the solution to all areas of a small town/rural area with a larger number of IoT devices. This phase also further develops the operational business plan to ensure that the solution generates a return on investment, meets its social objectives and does not become a cost burden to the municipality. Operations are designed to test the ability of the system to scale under operating conditions and tests the assumptions of the business plan.

Step 3 – Regional Grid Deployment.

The third step further expands the solution to deployment of the regional grid. This phase focuses on the ongoing operations of the Intelligent Utility, the continuous improvement and deployment of new innovations and the continued revenue generation of the Intelligent Utility. By this step the municipality involved will have decided the role it will play in the Intelligent Utility and will have finalised the business model, including development of key commercial contracts. Also, by this stage there will be enough time and data to prove the stability and reliability of the network.

Step 4 – Integration with Centralized Generation and Distribution System

This is the final phase which integrates the distributed power generation system with the centralised power generation and power system, ultimately completing the Intelligent Utility system. This step builds incorporates experiences from the first three steps, making appropriate changes to complete the Intelligent Utility system.

Conclusion

This paper has described the Intelligent Utility of the future. The Intelligent Utility is made up of intelligent dynamic power generation and distribution systems, enabled by IoT and managed by a distributed cloud-based grid management system, with an increasing percentage of the power being generated from renewable energy sources.

It has covered three key considerations for implementation—security, scalability and availability. Cybersecurity and the risks involving IoT are a key challenge in the Intelligent Utility. The intelligence in the Intelligent Utility comes from analyzing the data being fed from the IoT devices and performing predictive analytics and Artificial Intelligence predictions on that data and using this information to dynamically adjust and control the Intelligent Utility.

The paper discussed the role of the municipality in the Intelligent Utility. FuseForward believes that the Intelligent Utility offers many benefits to the municipalities in Africa.

Participate in a pilot

We have opportunities available for an interested municipality or university (or other interested party) to work with us on a pilot demonstration deployment. Not only will this pilot prove the solution, it will demonstrate that the utility of the future is available today in Africa, enabled by IoT and current cloud infrastructure.

If you are interested in helping your organization be a part of this leading-edge initiative, please connect with us on the provided contact details.

Appendices

Selected Sources

NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0

Good practices for Security of Internet of Things - European Union Agency for Network and Information Security (ENISA)

New Roles for South African Municipalities in Renewable Energy - A Review of Business Models Discussion Paper, South African-German Energy Partnership, March 2017

Optimizing Energy with Machine Learning Grey-Box Models, Gilani et al, 2019

Electric Vehicles 2019 Market Intelligence Report -https://www.greencape.co.za/assets/Uploads/ELECTRIC-VEHICLES-MARKET-INTELLIGENCE-REPORT-WEB4.pdf

Massive DDoS attack harnesses 145,000 hacked IoT devices - https://www.healthcareitnews.com/news/massive-ddos-attack-harnesses-145000-hacked-iot-devices

Acknowledgement

This paper was prepared with the assistance of Mark Damm, CEO, FuseForward Group and Carla Tooley, Marketing Communications Manager, FuseForward Group.

Contact FuseForward

Website:	www.fuseforward.com
Email:	cathy.pickering@fuseforward.com
South Africa:	+27 11 575 7609