Cyber Security for Cloud and the Internet of Things: How Can it be Achieved?

Bob Duncan, Business School, University of Aberdeen, Aberdeen, UK
Mark Whittington, Business School, University of Aberdeen, Aberdeen, UK

Abstract. The Internet of Things is one of the new "buzz" technologies of today. We consider what it is, how it came to be, and what it is capable of doing. We consider the architecture of the technology, what the cyber security challenges are, and demonstrate how difficult these challenges are to resolve. We discuss how easily these weaknesses are exploited, and also show how compliance with security standards remains problematic. Our contribution will show how we might approach these challenges to help achieve a better level of cyber security for a sensible level of cost, particularly in the light of recent unwelcome hacking developments. We also talk about the ongoing current and future work we are undertaking to help further address these issues.

Keywords: Internet of Things; cloud; standards; audit; cyber security.

Table of Contents

List of Tables

List of Figures

1 Introduction

As the question in the title asks, how can we achieve cyber security when we use cloud and the Internet of Things (IoT)? Before attempting to answer this question, we need to add an additional ingredient into the mix, namely big data. This is because the IoT is capable of generating huge amounts of data, thus we need to factor this aspect into the equation. In this article, our main contribution will be to outline the weaknesses presented by the IoT, to attempt to define an interim solution to providing a better level of cyber security for a sensible level of cost.

However, before even addressing this question, we need to ask ourselves another question, what is the IoT anyway? We will address this question in Section 2, of this article, where we first consider the history of the IoT in order to understand a little about the complexities involved, and we look at the range of possible uses for this technology. In Section 3, we look at a typical architecture of the IoT, looking at how cloud and big data fit into the picture. In Section 4, we discuss how easily this architecture can be exploited, and how important it is to try to prevent this from happening. In Section 5, we consider whether compliance with security standards can help with these problems. In Section 6, we look at what happens when these weaknesses are exploited. In Section 7, we

consider how we might approach these challenges to help achieve a better level of cyber security for a sensible level of cost, particularly in the light of recent unwelcome hacking developments. In Section 8 we outline a possible solution and discuss ongoing and future work in this area. Finally, in Section 9, we discuss our conclusions.

2 What is the Internet of Things?

We can define the IoT as: a collection of sensors and actuators embedded in physical objects which are linked through wireless and wired networks, linked mostly to the internet by the same internet protocol (IP) that connects the internet. The name was coined almost 20 years ago by Kevin Ashton in 1999 during his work at Procter and Gamble. However, it is only in recent years that it has started to take off, mostly enabled due to the advent of cloud computing and big data. To answer why that might be, we need to consider the history of the IoT.

2.1 History of the Internet of Things

You may be surprised to learn that some of the foundations of the IoT go back considerably further than the past 20 years. In 1832, Baron Schilling invented an electromagnetic telegraph, then Gauss and Weber invented a communication language in Germany, where they successfully communicated over a distance of 1200 meters. By 1844, Samuel Morse had successfully sent the first morse code message by public telegraph. It would be over a century before further serious progress would take place, and a number of scientists gave predictions of what would be yet to come, including Tesla, Turing, McLuhan and Steinbuch. In 1949, Norman Joseph Woodland conceived the bar code, and as an engineer for IBM obtained the first patent on it in 1952. In 1955, Edward O. Thorp

conceived the first wearable computer, a cigarette pack-sized analogue device for predicting roulette wheels. In 1960, Morton Heilig obtained a patent for the first-ever head-mounted display.

In 1967, Hubert Upton invented an analogue wearable computer with eyeglass-mounted display to aid in lip reading. In 1973, Mario Cardullo obtained the first patent for a passive, read-write radio-frequency identification (RFID) tag. The invention of Arpanet in 1969 really started to get things moving, and the basis of TCP/IP was developed 5 years later, in 1974. In 1984, the Domain Name System was introduced, and five years later, in 1989, Tim Berners-Lee proposed the World Wide Web. In 1990, John Romkey created the first internet 'device', a toaster which could be turned on and off via the internet. In 1991, Tim Berners-Lee created the first web page. In 1993, Quentin Stafford-Fraser and Paul Jardetzky created the Trojan Room Coffee Pot within the Computer Laboratory of the University of Cambridge to monitor coffee levels of the lab coffee pot. The system captured images of the coffee pot level, and saved them using a server, which other lab users could access, which was later adapted for the internet once browsers could display images.

In 1994, while still at school, Steve Mann created WearCam, a wearable camera system based on a computer in a backpack. 1995, the internet goes commercial, as Amazon and eBay are founded, followed in 1998 by Google. In Kevin Ashton's 1999 work at Procter and Gamble, he proposed the use of RFID technology, Ashton (2009), which lead to development of the Electronic Product Code or EPC, a global RFID-based item identification system intended to replace the universal product code (UPC) bar code. Thus there was now an understanding of what the IoT could become, but the technology to deliver on the dream was still insufficiently developed to make it a reality. Over the next seven years, a disparate variety of IoT-capable "things" were developed and released, but the rapidly expanding proliferation of smartphones, tablets and

other connected devices was what really started to gain some momentum for the IoT.

In 2007, Gantz et al., Gantz et al. (2007) forecast that all the electronic data collected throughout the globe would double every 18 months. In 2008, the EU founded an international conference on the IoT, and Cisco suggested that the IoT had now been born, as there were now more connected devices to the internet than people. This also coincided with concerns over the address limitations of internet protocol version 4 (IPv4), which was projected to run out of numbers some time around the end of the century, one of the reasons that Kevin Ashton had been so keen on the RFID approach. However, internet protocol version 6 (IPv6) had been developed to address this issue, which meant there would no longer be any practical limitation to the number of "things" that could be connected to the internet, and this explains why the use of IP became the preferred route for IoT connection. At this time, cloud computing had also evolved, and this helped too with the expansion of the big data concept. Thus, we can see that through all of these developments in technology, the IoT became much more enabled and really started to take off!

2.2 What Kind of Things can the Internet of Things Do?

Having reached the point where the technology has enabled the idea, what can we do with it? The answer to that is pretty well anything we like. We will merely be constrained by our imagination, Bojanova et al. (2013); Sharma et al. (2016), although we will talk later about some practical restrictions that may have to be considered.

Here are a few examples of some of the most popular uses for the IoT:

- Domestic and Home Automation
- eHealth
- Industrial Control

- Logistics
- Retail
- Security and Emergencies
- Smart Agriculture
- Smart Animal Farming
- Smart Cities
- Smart Environment
- Smart Water
- Smart Metering

Without suggesting in any way that this represents a comprehensive list, by looking at each of these areas in turn, we can get an idea of the range of implementations for which IoT is well suited.

Domestic and Home Automation: Art preservation, achieved by monitoring conditions inside the home where artworks are stored; Energy and water use, where consumption monitoring is used to optimise costs and suggest use of resources; Intrusion detection systems, where detection of window and door openings and violations thereof are used to prevent intruders; and, the use of remote control appliances which switch appliances on and off remotely to avoid accidents and save energy.

eHealth: Fall detection can be used to help provide assistance for elderly or disabled people to allow them to live independently at home; Medical fridges can be used to control conditions inside freezers storing vaccines, medicines and organic elements; Patient surveillance can be used to monitor the condition of patients inside hospitals and in old people's homes; Athlete care can be provided by monitoring vital signs in high performance centres and out in the field; and, Ultraviolet radiation measurement of UV sun rays can be carried out in order to warn people not to be exposed during certain hours.

Industrial Control: Indoor air quality can monitor toxic gas and oxygen levels inside chemical plants to ensure safety of workers and goods; Indoor location can detect asset location by using active means, such as ZigBee, or by the use of passive tags using either RFID or near field communications (NFC); Machine to Machine (M2M) applications allow for machine auto-diagnosis and asset control; Ozone presence monitoring systems in food factories can monitor ozone levels during the meat drying process; Temperature monitoring can be used to control temperature inside industrial and medical fridges which store sensitive merchandise; and Vehicle auto-diagnosis using information collection from Controller Area Network (CanBus) applications to send real time alarms in the event of emergencies or provide advice to drivers.

Logistics: Fleet tracking can be implemented through control of routes followed for delicate goods like medical drugs, jewels or dangerous merchandise; Item location allows search of individual items in large volume areas such as warehouses or harbours; Quality of shipment conditions can be ensured by monitoring of vibrations, strokes, container openings or cold chain maintenance for insurance purposes; and Storage incompatibility detection can be achieved through warning of emissions from containers storing inflammable goods close to others containing explosive material.

Retail: Intelligent shopping applications can deliver advice at the point of sale according to customer habits, preferences, presence of allergic components for them, or expiry dates; NFC payment systems can carry out payment processing based on location or activity duration for public transport, gyms, theme parks, and so on; Smart product management allows control of rotation of products in shelves and warehouses to automate restocking processes; and Supply chain control systems monitor storage conditions along the supply chain and provide product tracking for traceability purposes.

Security and Emergencies: Explosive and hazardous gases detection can ensure safety of gas levels and leakages in industrial environments, or in the surroundings of chemical factories, and inside mines; Liquid presence detection in data centres, warehouses and sensitive building grounds, can help to prevent break downs and reduce corrosion; Perimeter access control systems can be used to control access to restricted areas and for the detection of people in non-authorized areas; and Radiation levels using distributed measurement of radiation levels in nuclear power stations and their surroundings can be used to generate leakage alerts.

Smart Agriculture: Compost control by measuring levels of humidity and temperature levels in alfalfa, hay, straw, and so on, can be used to prevent fungal and other microbial contaminants; Golf courses can use selective irrigation in dry zones to reduce the water resources required in the greens; Green houses can use control of micro-climate conditions to maximize the production of fruits and vegetables and ensure quality; Meteorological station network can use study of weather conditions in fields to forecast ice formation, rain, drought, snow or wind changes; and in wine quality systems, monitoring of soil moisture and trunk diameter in vineyards can be used to control the amount of sugar in grapes and grapevine health.

Smart Animal Farming: Animal tracking can be used to monitor location and identification of animals grazing in open pastures or to identify location in large stables; Hydroponics systems can control the exact conditions of plants grown in water to get the highest efficiency crop yields; Offspring care systems can be used to control the growing conditions of the offspring in animal farms to ensure their survival and health; and, Toxic gas level systems can be used to study ventilation system effectiveness and air quality in farms, including detection of harmful gases from excrement.

Smart Cities: Electromagnetic field level monitoring can use measurement of the energy radiated by cell stations and WiFi routers to assess electromagnetic risk for citizens; Smart lighting can provide intelligent and weather adaptive lighting for street lights, for greater safety and energy control; Smart parking can monitor parking space availability throughout the city; Smart roads allow the provision of intelligent roadways with warning messages and diversions activated according to climate conditions and unexpected events such as accidents or traffic jams; Smartphone detection systems detect any device which works with WiFi or Bluetooth interfaces, which can be used for enhancing tourism, or for public safety announcements in the event of a disaster; Structural health systems can monitor vibrations and material condition of buildings, bridges and historical monuments; Traffic congestion systems can monitor vehicles and pedestrian levels to optimize driving and walking routes; Urban noise maps can be developed to monitor sound in bar areas and other zones in real time; and, Waste management systems can use detection of rubbish levels in containers to optimize the rubbish collection routes.

Smart Environment: Air pollution control systems can be used to measure the amount of CO2 emissions from factories, or the pollution emitted by cars, or toxic gases generated in farms; Early detection of earthquake systems can provide distributed control around places which are prone to tremors; Forest fire detection systems can be used to monitor combustion gases and allow preemptive fire responses to be enabled; Landslide and avalanche prevention systems can be used to monitor soil moisture, vibrations and earth density to detect dangerous patterns in land conditions; and Snow level monitoring systems can be used to check snow level measurement to provide real time assessments of the quality of ski runs and allow advanced warnings of possible avalanche conditions developing.

Smart Water: Chemical leakage detection systems in rivers can be used to detect leakages and waste from factories entering rivers; Pollution level systems in the sea can be used to control real time leakages and wastes entering the sea; Potable water monitoring systems can be used to monitor the quality of tap water in cities; River flood systems can be used to monitor water level variations in rivers, dams and reservoirs; Swimming pool remote measurement allows for remote control of the swimming pool conditions; and Water leakage systems can be used to detect liquid presence outside tanks and pressure variations along pipes.

Smart Metering: Photovoltaic systems can be used for monitoring and optimization of performance in solar energy plants; Silos stock calculation systems can measure the emptiness level and weight of the goods in the silo; Smart grid systems can be used for energy consumption monitoring and management; Tank level systems can be used to monitor levels of water, oil and gas in storage tanks and cisterns; and Water flow systems can measure water pressure in water transportation systems.

As you can see, this represents a wide variety in types of systems, areas of application and potential use cases to which the IoT can be put, and there are a few more here: future ideas, Bughin et al. (2010), smart city (there are currently 500 smart cities in the Innovation Cities Global list InnovationCities.com (2017)), Gubbi et al. (2013), Suciu et al. (2013), Aziz et al. (2016), analytics, Larson and Chang (2016), analysis of IoT data for business intelligence purposes, Chang et al. (2014).

3 Internet of Things Architecture

To come back to earlier questions, how does cloud and big data fit into this picture? We can use the word “picture” to illustrate this point very neatly. Those

of you who are old enough to remember the introduction of the VGA standard in 1987 will remember how amazed you were that your screen resolution was now 640x480 pixels, a vast improvement on the earlier 320x240 pixels. Today, we are all accustomed to having full HD which gives us 1920x1080, although Samsung have developed a massive 8K screen, with a resolution of 7680x4320. Thus, in 30 years, screen size has gone from 307,200 pixels to 2,073,600 pixels, and in the case of 8K to 33,177,600 pixels. This ever increasing resolution is not limited to computer screens. The same thing is happening to all our technology, and none more so than with camera images. If we consider the best digital cameras from 15 years ago would have had an image resolution of around 2 megapixels, this is the same resolution as our Full HD desktop screen. Modern digital cameras can easily far exceed the 33 megapixels of the 8K screen. Indeed, the car manufacturer Bentley have a 53 gigapixel image on their website Bentley (2016). It is well worth a look to see just what a high level of resolution this image offers.

Thirty years ago, you would not have any digital images to store, since you could not yet buy a commercial digital camera, and the JPEG and MPEG standards had yet to be developed. In the intervening years, as digital still and cine cameras gained traction, the need for storage also started to grow, as resolution also grew year on year. During this time, software systems also grew in complexity, leading to more pressure on storage, resulting in the need to buy ever larger hard drives. In 2010, when Gantz et al., Gantz et al. (2010) revisited their earlier work, they discovered that the reality of data expansion turned out to be more than double the expansion rate they had predicted, and this is unlikely to slow down any time soon.

Why does this matter for the IoT? It matters because any use of the IoT which relies on capturing and storing data, especially video data, will require an ever larger facility for storage, especially as resolution of the images gets

better. This means that conventional computing systems are no longer suited for connecting to IoT systems for storage and processing of data, and this is where big data and the cloud have been the great enabler to allow the IoT to flourish.

For those who are unsure of what cloud computing is, we will use the NIST definition of Cloud Computing, Mell and Grance (2011): "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.*"

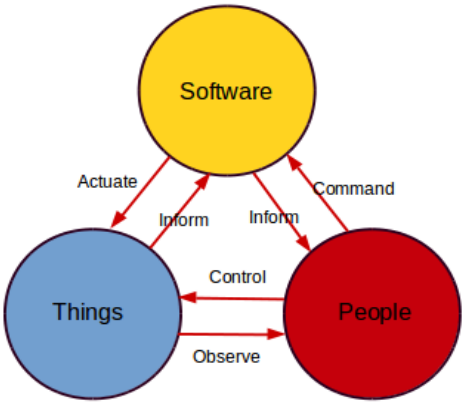


Fig. 1: A typical user high level view of IoT ©2016 Duncan and Whittington

Since we may not know what resources we may require, or when we may require them, we can programme a cloud system to automatically add, and remove, resources and storage as our needs dictate, as and when these needs arise. And, for those who are not sure what "big data" really is, data is data.

But “big data” is data at huge volume. We can consider “big data” volume to mean volume at such a level that far exceeds our capability to physically analyse the data without the assistance of programmatic tools.

In Figure 1, on page 13, we show a sample high level view of the layout for an IoT system. This shows the typical view from the user’s perspective, without the underlying system architecture showing for clarity. The idea here is to remove the need for constant physical monitoring by individuals, allowing them instead to “manage by exception”, which allows better use of their time (and more cost-effective monitoring by organisations).

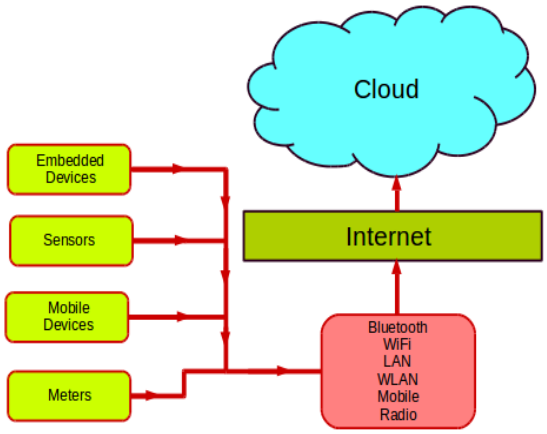


Fig. 2: An example of IoT connections at the edge ©2016 Duncan and Whittington

In Figure 2, on page 14, we show the architecture of connections at the extreme outside edge of the IoT to illustrate the data flow. The data flows from these, usually small and cheap devices, frequently through a data collection point, where data is aggregated, and sometimes filtered, before its onward journey to cloud storage, where further aggregation, filtering and subsequent deep analysis may also be carried out. Connections are made using Bluetooth, WiFi,

LAN, WLAN, Mobile or Radio connections to pass the data on through to the internet.

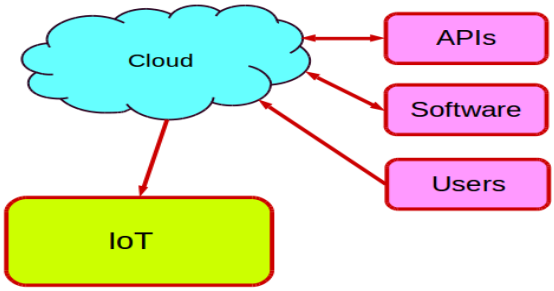


Fig. 3: An example of IoT connections at the control end ©2016 Duncan and Whittington

In Figure 3, on page 15, we show how users can access the collected information, using various tools, Application Programming Interfaces (API)s and software to understand what is going on, and to pass control instructions down the line.

These, then, are the building blocks we need to run seamless IoT systems, at scale if we need to. However, we do have to consider the security challenges, which we look at in the next Section.

4 What are the Security Challenges?

Cyber security with conventional distributed systems is challenging. Cyber security in the cloud takes the challenge to new heights. Add the IoT and Big Data on top, and the challenge grows exponentially. So what exactly are the challenges, and where do they come from.

Let us start with conventional distributed systems. Are they secure? Not exactly. The problems are well understood by industry, particularly by large

corporates, and they understand well how to mitigate those weaknesses, and set up a secure corporate firewall to protect their systems. Of course, the advent of mobile computing, smartphones and the bring your own device (byod) movement, opened up new vulnerabilities. Again, these threats are well understood by large corporates. These problems are less well understood by small to medium sized enterprises (SME)s, and for private users, this remains a concern.

When we add cloud to the equation, the major point most users fail to grasp, is the added risk that comes from using a system running on someone else's hardware. Even large corporates sometimes miss the point that moving their secure software to the cloud is not a smart thing to do, as most of their software is custom configured to suit their own secure environment, and once migrated to the cloud, most of the security features become redundant. Cloud is also highly scalable, and can be configured to automatically scale up, and down, as needed to service varying demand. Often, little things like system logs and audit trails are not properly thought through. Yet, it is too late to think about it after a breach has occurred and you suddenly realise that every time the unwanted instances shut down, the server logs and audit trails vanish along with them. Unlike with conventional systems, where your forensic scientist can recover a remarkable amount of data, with cloud, it is a completely different matter. As soon as an instance is shut down, the resources are then added to the resource pool and re-utilised as quickly as possible by the cloud service provider. This can happen in seconds, and certainly by the time you realise you have had a security breach many weeks later, all hope is lost for any sort of recovery of the lost forensic data. This remains one of the key unsolved challenges of cloud computing.

Then, when we add IoT on top of this equation, we really open up a can of worms. We are generally adding a huge range of heterogeneous "things" to a poorly secured system. Most of the "things" are cheaply made, with scant regard

for security, resulting in a potentially exponential increase in attack vectors to our overall system.

So what is the source of these problems? Let us first start with companies themselves. There are a great many security challenges which need to be addressed, and, Duncan and Whittington (2016b) have developed a useful list of ten key security goals that must be addressed, which we see in Table 1 below.

Number	Key Security Challenges
1	The definition of security goals
2	Compliance with standards
3	Audit issues
4	Management approach
5	Technical complexity of cloud
6	Lack of responsibility and accountability
7	Measurement and monitoring
8	Management attitude to security
9	Security culture in the company
10	The threat environment

Table 1. Duncan and Whittington 10 Key Security Issues — 2016
Duncan and Whittington (2016b)

The list in Table 2 outlines ten key security goals that must be addressed in any system which will implement any form of cloud computing, without which there will be potential for weakness of security and privacy in these systems. We do not get into any detail on on any of these issues, as this is beyond the scope of this article. We merely point out that these are issues which must be addressed.

However, of those ten key challenges, the last on the list — the threat environment will itself need to be considered in more detail. Generally, we can break the threats down as coming from 5 different types of serious attacker:

These all represent serious threats in their own way. The first will be virtually impossible to guard against effectively. These actors are so skilled, that you are unlikely to even be aware that they have been inside your system. On the plus side, they are not usually after your money, they just want to know what you

Number	Attacker Types	Capabilities
1	State Sponsored Actors	Very High Expertise, Well Funded
2	Industrial Spies	High Expertise, Reasonably Funded
3	Hacktivists	Motivated, High Expertise, Poorly Funded
4	Serious Criminal Actors	Motivated, Can Buy In Expertise
5	Amateur Hackers	Skills Vary, Motivated

Table 2. Duncan and Whittington 5 Attacker Types — 2016

are up to. The second group is of more concern, as they will be looking to steal your intellectual property or trade secrets. An obvious piece of advice would be never to put any of this on a cloud system. The third type, hacktivist actors are usually out to make a point, or to embarrass your company. Their favourite approach is to compromise or take over your web site. The fourth type will definitely seriously affect your bottom line. They are out to relieve you of as much cash as they are able to remove from you. The last group are generally not out for your cash, but they can cause a lot of damage to your systems. So, in their own way, each will be of some concern.

The third source of security problems comes from the very technology you are trying to use to run your business. Using out of date software, un-patched security fixes, mis-configured server, database or network systems, or applications, can cause serious security issues. These are often relatively easy, and cheap to fix, but this seldom actually happens.

A rather more difficult problem lies in undiscovered software bugs, the holy grail of the attacker. These are extremely difficult to spot, and most companies have neither the expertise nor the budget to do anything about this area. However, an effective approach is to keep up to date with security reports which highlight when these vulnerabilities are discovered. There is a constant battle between security companies and the bad guys. As soon as one patch is fixed, another vulnerability is found, and this arms race constantly evolves, which is

why it is important to keep on top of these reports, and more importantly, to actually install the released patches.

However, for the IoT, probably the two most important weaknesses can be found in the title — Internet and Things. First, the internet, since this is the main means by which the architecture functions. The internet being a web based technology, the most important consideration is to look at all forms of web based technology vulnerabilities. To this end, one of the best sources of information can be found from the work of the Open Web Application Security Project (OWASP), who publish a top ten list of web security vulnerabilities every three years. They are not the only providers of this information, but they do provide the most comprehensive list of the most dangerous vulnerabilities and a number of very good mitigation suggestions. The last three OWASP lists for 2007, 2010 and 2013 are provided in Table 3 below.

2013	**2010**	**2007**	**Threat**
A1	A1	A2	Injection Attacks
A2	A3	A7	Broken Authentication and Session Management
A3	A2	A1	Cross Site Scripting (XSS)
A4	A4	A4	Insecure Direct Object References
A5	A6	-	Security Misconfiguration
A6	-	-	Sensitive Data Exposure
A7	-	-	Missing Function Level Access Control
A8	A5	A5	Cross Site Request Forgery (CSRF)
A9	-	-	Using Components with Known Vulnerabilities
A10	-	-	Unvalidated Redirects and Forwards

Table 3. OWASP Top Ten Web Vulnerabilities — 2013 - 2007, OWASP (2013)

This list is based on the result of analysis of successful security breaches across the globe, which seeks to highlight the worst areas of weakness in computing systems. It is not exhaustive, but merely illustrates the worst ten vulnerabilities in computing systems globally. It is clearly concerning that the same vulnerabilities

recur year on year, which clearly indicates the failure of companies to adequately protect their resources properly.

Thus in any IoT cloud based system incorporating big data, these vulnerabilities are likely to be present. However, there are likely to be additional potential vulnerabilities which will also need to be considered, due to the differences in the mechanics of the IoT. Since many IoT systems use mobile technology for their communications channels, then we might also look at the OWASP Mobile top ten list of vulnerabilities in Table 4 below.

2013 Code	**Threat**
M1	Insecure Data Storage
M2	Weak Server Side Controls
M3	Insufficient Transport Layer Protection
M4	Client Side Injection
M5	Poor Authorization and Authentication
M6	Improper Session Handling
M7	Security Decisions via Untrusted Inputs
M8	Side Channel Data Leakage
M9	Broken Cryptography
M10	Sensitive Information Disclosure

Table 4. OWASP Top Ten Mobile Vulnerabilities — 2013
OWASP (2013)

But, of course, it is not quite as simple as that. The IoT mechanics extend beyond traditional web technology and mobile technology. In 2014, OWASP developed a provisional top ten list of specific IoT vulnerabilities, which we outline below in Table 5.

It is worth bearing in mind that the above list represents just the OWASP top ten vulnerability list. OWASP are currently working on a list of 130 possible IoT vulnerabilities which might need to be taken into account.

It is rather worrying that as far back as 2012, Trustwave, Trustwave (2012), report an average of 6 months between breach and discovery. It is also rather worrying to see that three years later, Verizon (2015), see Figure 4, that 75%

2014 Code	Threat
I1	Insecure Web Interface
I2	Insufficient Authentication/Authorization
I3	Insecure Network Services
I4	Lack of Transport Encryption
I5	Privacy Concerns
I6	Insecure Cloud Interface
I7	Insecure Mobile Interface
I8	Insufficient Security Configure-ability
I9	Insecure Software/Firmware
I10	Poor Physical Security

Table 5. OWASP Top Ten IoT Vulnerabilities — 2014
OWASP (2014)

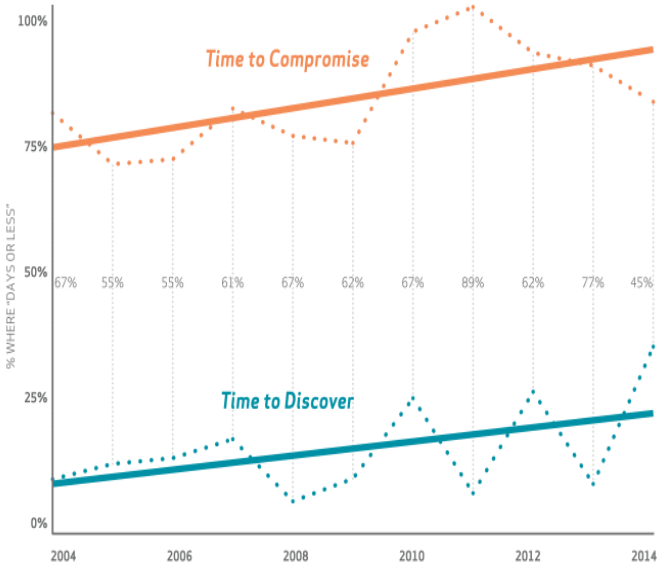
of breaches happen within days, yet only 25% of discoveries are actually made within the same time-frame. This still leaves a large gap where compromised systems may still be under the control of malicious users.

This presents a clear indication that very few firms are actually scrutinising their server logs. Back in 2012, Verizon, Verizon (2012) highlighted the fact that discovery of security breaches often took weeks, months or even years before discovery, with most discovery being advised by external bodies, such as customers, financial institutions or fraud agencies.

As we mentioned earlier in this section, the other source of concern are the "Things" themselves. At the cheaper end of the spectrum, the devices used usually have very limited system resources, meaning there is little space to house any security resources. Often, there is little thought to ensuring proper secure passwords are used. How many systems are set up with default user name and password of 'admin'/ 'admin'? This failure also can extend to some of the more expensive hardware. Users do not help this situation by simply buying the cheapest devices, without regard to the security and privacy implications.

So, we can see that there is currently no complete security solution for cloud. Can we offer a solution to cloud security? No, we cannot. There is no such thing as a complete solution to cloud security, and it is unlikely that there will be,

Fig. 4. The Lag Between Breach and Discovery © 2015 Verizon



while the current ennui exhibited by many cloud users and indeed some cloud service providers, persists. Likewise, while the constant battle between security experts and outside attackers continues back and forth, this will continue to be a very difficult goal to achieve.

However, it is encouraging to see initiatives, such as the Association for Information Systems (AIS) who aim to develop what is known as the Bright Internet, which aims to drastically reduce cyber-crimes by achieving the Principles of Origin Responsibility, Deliverer Responsibility, Rule-based Digital Search Warrant, and Traceable Anonymity, which they are now developing along with the International Telecommunication Union. Meantime, what we can do is to make some reasonable suggestions, based on our research over many years, to help companies mitigate these vulnerabilities by paying particular attention to all the specific threats they face, many of which we share in this article.

There are a number of security standards in existence, and many companies have achieved compliance with these standards. Will this solve their problems? We shall address this question in the next Section.

5 Does Compliance Help?

All companies and businesses based in the UK are subject to legislation. All large companies are subject to corporate governance rules. Many companies work in regulated industries, such as healthcare, agriculture, energy supply, transport, and water, and are subject to tight regulation. Consequently, many of these companies seek to gain compliance with security standards. But the big question here is, which standard should they comply with? Here is a list of all the organisations who have worked on cloud security standards:

- American Institute of Certified Public Accountants (AICPA);
- Association for Retail Technology Standards (ARTS);
- Basel 3;
- The Technology Policy Division of the Financial Services Roundtable (BITS);
- Cloud Security Alliance (CSA);
- Cloud Standards Customer Council (CSCC);
- Control objectives for information and related technology (COBIT);
- Cloud Standards Organisation (CSO);
- Data Protection Act (DPA);
- Distributed Management Task Force (DMTF);
- European Telecommunications Standards Institute (ETSI);
- Federal Risk and Authorisation Management Program (FedRamp);
- Generally accepted privacy principles (GAPP) ;
- Global Inter-Cloud Technology Forum (GICTF);
- Health Insurance Portability and Accountability Act (HIPAA);

- Information Assurance Technology Analysis Center (IATAC);
- Information Systems Audit and Control Association (ISACA);
- International Standard on Assurance Engagements (ISAE) 3402;
- International Organisation for Standardisation/International Electrotechnical Commission (ISO/IEC);
- Information technology infrastructure library (ITIL);
- International Telecommunication Union Telecommunication Standardisation Sector (ITU);
- Jericho Forum;
- National Institute of Standards and Technology (NIST);
- North America Electric Reliability Corporation (NERC);
- Organisation for the Advancement of Structured Information Standards (OASIS);
- Open Cloud Consortium (OCC);
- Open Grid Forum (OGF);
- Object Management Group (OMG);
- Payment Card Industry Data Security Standard (PCIDSS);
- Storage Networking Industry Association (SNIA);
- The Open Group;
- TM Forum;

The cloud has been around for barely a decade, during which time each of the above organisations have been working on cloud standards. With so many different organisations working on cloud standards, there are no surprises to discover we have yet to see a complete and comprehensive cloud security standard. The situation with big data, and especially the IoT, is even worse, with the IoT to all intents and purposes

Many large corporates have traditionally sought to gain compliance with the global standards published by the ISO/IEC, and in respect of security, the ISO/IEC 27000 series of standards.

However, for those companies adhering to any of the above standards, accreditation is achieved through compliance or audit. The authors have already written on a number of these issues, addressing some of the inherent weaknesses in approach, including: compliance and standards issues, Duncan and Whittington (2014a), audit issues, Duncan and Whittington (2014b), management approach, Duncan and Whittington (2015a), lack of accountability, Duncan and Whittington (2015b), measurement and monitoring, Duncan and Whittington (2015c), cloud audit issues, Duncan and Whittington (2016a), and issues with the cloud audit trail, Duncan and Whittington (2016b).

The pace of evolution of new technology far outstrips the capability of international standards organisations to keep up with the changes, Willingmyre (1997), meaning that the time taken for standards to be implemented, merely adds to the problem. Cloud computing started to gain traction around 2006, and while NIST produced a definition of cloud computing in 2009, followed up by a more comprehensive definition in 2011, along with suggestions for mitigating strategies, it took the ISO/IEC until 2014 to even mention the cloud word in their standards.

On the plus side, standards such as ISO/IEC 27002 are now generally well understood by large corporates, and we are finally starting to see the introduction of cloud standards in the ISO/IEC 27000 series. ISO/IEC 27017:2015, which provides guidance for cloud specific security controls based on ISO/IEC 27002:2013, was finally approved in 2015. During the current decade, there has been a shift in the ISO 27000 series of standards from a compliance based approach to a risk based approach, and this is to be welcomed. ISO/IEC 27018:2014 was published in 2014, and covers the use of personally identifiable information

(PII) in public clouds. ISO/IEC 27036–4:2016 provides guidance on the security of cloud services. This standard does not address business continuity management or resiliency issues for cloud services. These are addressed in ISO/IEC 27031:2011, although this has been improved on in ISO 22301:2012.

There are three security studies currently being conducted by the ISO/IEC on: cloud security assessment and audit; cloud-adapted risk management framework; and cloud security components. Beyond that, the following four areas have been proposed: guidelines for cloud service customer data security; the architecture of trusted connection to cloud services; the architecture for virtual root of trust on cloud platforms; and emerging virtualization security.

One minor issue with these standards is that they provide an idea of what needs to be done in order to be compliant, but little detail on how this can be achieved is provided. Where the understanding of the issues involved is not clearly understood, this may lead to compliance being achieved, without any useful level of security being present, leading to a false sense of security.

Thus, it is clear that there is no comprehensive security standard yet in place for cloud, nor is there likely to be for some time. As yet, we still have no clear idea on what form IoT security standards will take. This leaves a glaring weakness which bad actors are only too keen to take advantage of.

6 What Happens When These Weaknesses Are Exploited?

The "things" in the IoT are only little. Where is the harm in that? The problem with the "things" in the IoT is not the small size of the hardware resources, rather it is in the scale of "things" involved.

Take the recent large scale DDoS attacks perpetrated over the last six to nine months against, among others, the Dyn company's DNS system attack, resulting

in big names including GitHub, Twitter, Reddit, Netflix, AirBnb and others, who were among hundreds of websites rendered inaccessible to millions of people around the world for several hours. Another recent attack resulted in hundreds of thousands of TalkTalk and Post Office broadband customers affected. Deutsche Telekom, KCOM and Irish telco Eir have also been affected. These attacks were perpetrated as a result of many "things", in this case surveillance cameras, being infected with the Mirai virus, which were vulnerable due to poor security, and were turned into a large Bot-Net.

If your personal computer gets infected, you will very quickly notice, as it will slow down significantly, usually because the malware takes over as many of your system resources as it can. However, in this case, the perpetrators took a rather more smart approach. They left just enough system resources for the camera to function properly, and send images on to the data collection point. The software simply used the unused portion of system resources. Since the cameras continued to function normally, nobody noticed that they had been compromised. It is estimated that some 1.2 million IoT devices are currently infected with the Mirai virus. It is further estimated that only 125,000 cameras were used to carry out the attacks, achieving some of the highest attack speeds ever seen, in the order of up to 1,200 Gigabits per second. The really worrying aspect of this is that the Mirai virus was recently ported to Windows, meaning that once an insecure IoT device has been compromised, then all the Windows devices in the network, including desktops and servers, could then be easily compromised and taken over, and could then seek out other machines to compromise.

Here are a few more of the weaknesses that have been exploited. For IoT breach research, 2015 was a productive year. Researchers managed to use the on board browser to hack into a Tesla S vehicle, Wired.com (2015b), having plugged in a laptop behind the dashboard, and were able to start the car and drive it off. Researchers were able to take control of a Jeep on the freeway, and amongst other

things, shut off the engine at 70mph Wired.com (2015a). In another worrying piece of research Zetter (2015a), it was possible to send a fatal drug overdose to a hospital drug pump. Researchers used a cheap insurance company dongle plugged in to the dashboard of a Corvette to disable the brakes Wired.com (2015c). Researchers were able to 'kill a dummy' by switching off its pacemaker Koebler (2015). This research activity drove a medical doctor to embark on a crusade to try to improve security of medical devices Zetter (2015b).

Researchers had a 'lightbulb' moment in 2016Pritchard (2016), when they realised how the humble lightbulb could be used as an attack vector. Next the importance of protecting waste water became obvious Kumbhar (2016). Researchers managed to hack an industrial dishwasher Newman (2017b), to give them a springboard to attack other devices on the network. More warnings about medical device insecurities Newman (2017a), followed. Uber's former top hacker admits securing autonomous cars is a really hard problem Greenberg (2017).

Shell is a company renowned for its future forecasting and a look round its scenario web pages Shell (2017), shows anticipation of rapid applicability of connected solutions in transport, health, water and for the efficient zero emission city of the future. In one of their future reports Shell (2016), they discuss the future benefits of a healthy life, which they forsee being enabled by IoT technology. No real surprise that there will continue to be an increasing demand for IoT technology. However, with up to 50 Billion IoT devices in operation by 2020, and no proper security yet, this starts to get more than a little concerning. There is no doubt that we need to take action now, but how? In the next Section, we will consider how we might address these challenges.

On the bright side, we have seen the occasional IoT vigilante throw their hat into the ring. In 2015 Symantec (2015), the Linux.Wifatch virus was released by persons unknown. This virus actively sought out vulnerable IoT devices, proceeded to infect them, but rather than doing harm, instead downloaded ad-

ditional patches to make the systems more secure. Contrast this approach with the very latest BrickerBot virus Coppock (2017), which similarly infects vulnerable IoT devices, but instead of improving their security, this virus makes sufficient changes to the system to render ir unusable following a reboot, which it forces on the device after infection. This essentially 'kills' the device, rendering it completely secure, but useless. It does not appear to be selective, which means it could cause serious problems if mission critical devices were infected.

7 How Can We Address These Challenges?

This might all sound rather overwhelming. However, it is worth bearing in mind that in addition to providing these comprehensive lists, OWASP also offers advice on how to mitigate the weaknesses highlighted in their lists, OWASP (2016). Thus, it would be a good idea for all IoT users to take full advantage of this advice when seeking to safeguard their IoT systems. There are also many other agencies who have been working on cloud security, such as the CSA, ENISA, NIST and PCIDSS who all have sensible recommendations to make, and it would be useful to take their recommendations into account.

When engaging cloud services, here are a few useful things to consider:

Item	Weakness	Action Required
1	CSP Sales Talk	Do not believe the hype. Do your own due diligence
2	Business Continuity	Prepare a proper disaster recovery plan
3	Cloud Security	Remember, there is no single solution
4	Rapid Deployment	Don't try to do it all at once
5	Ongoing Ennui	Do not relax. Be vigilant at all times
6	Other Approaches	Look out for the loopholes
7	After a Breach	Have a plan for what to do after a breach

Table 6. Common Mistakes, Weaknesses and Mitigating Strategies ©2016 Duncan and Whittington

While audit is unlikely to be an issue for private individuals, it most certainly will be an issue for companies, and will require to be properly addressed. Of greater concern is dealing with the question of who is responsible for security. Users should pay particular attention to the service level agreements that they sign with the cloud service providers. Careful analysis of the detailed terms contained in these agreements will ensure more clarity and a better understanding on the responsibilities of each party.

However, we can address these vulnerabilities. By carefully analysing the full details of the systems architecture of the IoT system we plan to use, we can identify which of these vulnerabilities the system might be exposed to. There are many defences which have been proposed for each of these vulnerabilities, and providing the right steps are taken, it will be possible to mitigate the risks faced. The OWASP foundation provides a comprehensive set of mitigation strategies for a whole variety of different vulnerabilities, and it would certainly be sensible to take this advice, which is free to download OWASP (2017). In addition, Acunetix (2017), have developed a web vulnerability scanner which you can use to check whether your system is vulnerable. You can run a vulnerability scan for free, although you can also subscribe for a more comprehensive paid version.

The first major step we must take is to recognise the extent of the challenges faced when using an IoT system, just as we must do when using mobile systems, or cloud systems, or conventional distributed systems. Recognition is a key first step to achieving a successful cyber security outcome. Then, we must abandon the practice of relying on default settings for all installed components in the system. If the components do not include proper security, we should vote with our wallet, and buy elsewhere, from someone who can provide proper security.And remember, that if we fail to do this, then we are aiding and abetting the bad guys, and are consequently no better than them. We are all responsible for doing our bit to improve our own security.

While cyber security for the IoT certainly would appear on first sight to be an unsolvable challenge, it is clear that taking sensible steps can certainly help you sleep better at night, and we outline a number of these sensible steps in the next section..

8 A Possible Solution

There is currently no guaranteed solution to the IoT security problem. However, we can take a pragmatic approach at this stage, which is not likely to be overly expensive, and should ensure we achieve a reasonable level of protection.

1. We should scrutinise cyber breach reports daily to identify any newly discovered vulnerabilities;
2. We should scan our system for the most common vulnerabilities Acunetix (2017);
3. We must ensure we use a very robust router, or routers for larger systems. There should be no known back door in the router, and we should ensure that we use sufficiently strong passwords to make ensure they are very difficult to break;
4. We must ensure that every single 'thing' attached to these routers has the same level of security available and we should ensure that we use sufficiently strong passwords to ensure they are very difficult to break;
5. Ensure that every piece of non-compliant hardware is identified and removed from the system;
6. Every piece of software with known vulnerabilities should be either patched or changed for more robust software;
7. All software security patches should regularly be identified and updated;
8. All open ports should be identified, and any non required ports should be closed;

9. An Intrusion Detection System (IDS) should be installed, and monitored;
10. Where wireless or Bluetooth technology is in use, the most secure version should be used and properly configured;
11. We must ensure we retain a proper forensic trail. Thus all system logs, user access traffic, including commands used, should be logged securely to an immutable database Duncan and Whittington (2017), which is stored on a secure server in a different location. Conventional databases are wide open to attack, and this is the primary target for bad actors so that they can delete all trace of their visit. Using an immutable database makes this substantially more difficult for them to carry out;
12. Every piece of web based software used should be made more robust by following the OWASP security recommendations;
13. Some form of monitoring and data capture for all attached devices should be installed and regularly reviewed;
14. Strong access controls should be used and enforced at all times;
15. All system components should be regularly scanned to test for the presence of malicious software;
16. There should be a well defined strategy developed for business continuity management in the event of a breach occurring.

We would stress that this possible solution can not be guaranteed 100% effective, but by following these suggestions, any IoT user can vastly reduce the number of vulnerabilities which need to be addressed.

Of course, in the longer run, there is certainly a need for a more robust approach, and we are involved in four areas of ongoing research into IoT vulnerabilities which will hopefully lead to a more robust long term solution.

- We are researching a means of providing tighter controls by default;
- We are researching a means of highlighting and removing vulnerable software by default;

- We are researching a unikernel based solution to eliminate the problems brought about through the ever increasing complexity of modern systems Duncan et al. (2016);
- We are involved in research into the Bright Internet — a global research collaboration with the goal of ensuring all traffic sent by servers in the Bright Internet will be virus free. Another goal is that all users will have full anonymity for all their day to day activities, but in the event that they perpetrate a criminal act, they will be identifiable, thus ensuring proper accountability.

Of these above research areas, the first two are likely to show most promise in the short term. The unikernel based approach is likely to deliver results a year or two down the line, and the Bright Internet a little further down the line again.

There is little doubt that serious action on IoT security must take place, and soon. There is no way that we can possibly leave the status quo to continue, otherwise, there will be serious repercussions to contend with in the future. There is a real danger that the potential future benefits could be lost to society if we collectively do not take the action required now.

9 Conclusion

We have looked at the history of the IoT, and considered what kind of things it can do, which provides a very exciting insight into what the future of this technology could bring to all of us. We had a brief look at IoT architecture, and how it works at various levels. We have considered the many security challenges which we face in using this technology safely.

We have also considered whether compliance with cloud security standards can help. We have had a brief look at the potential for disaster when we do not take enough care to ensure proper security is provided, often at minimal cost,

and resulting in these weaknesses being exploited, a horrifying prospect. And we have briefly considered how we might address these challenges.

The IoT at this time is an unregulated space. We must all recognise this, and take such steps as are necessary to ensure bad actors cannot get access to our IoT resources to create mayhem for the rest of society. We all bear a responsibility to play our part in this, whether we are a large corporate, an SME, a one man band, or a private individual using the IoT to run their home more efficiently.

Our research was initially focussed on identifying key management issues which if not addressed properly would lead to weaknesses in security for cloud users. We are also working on some technical solutions to specific problems, such as: ensuring proper audit trails can be effectively maintained; the use of audit to help provide integrity assurance for data; the use of unikernels to provide a more robust environment for running cloud based systems, including those for the IoT; the use of adaptive soft security measure to police cloud based systems in operation; the development of immutable data base systems to ensure data cannot be compromised; investigating the threat environment to help develop better responses to ongoing security threats; and working further on the weaknesses of people in the organisation to security.

Of course, technical solutions alone are not the answer to this problem. The business architecture of a company is a combination of people, process and technology, not technology alone. Thus it is necessary to take a much broader approach to trying to resolve this problem. And it is no longer a question of "if" your company will suffer a breach, it is a simple matter of time before it will happen. The real question is will you be able to recognise that it has happened, and what will you be able to do about it when it does?

Bibliography

Acunetix (2017). Scan Your Website for OWASP Top 10 Critical Web App Vulnerabilities.

Ashton, K. (2009). That 'Internet of Things' Thing. *RFiD J.*, 22(7):97–114.

Aziz, B., Arenas, A., and Crispo, B. (2016). Engineering secure Internet of Things systems.

Bentley (2016). Bentley Used NASA Tech to Create This 53-Gigapixel Car Photo.

Bojanova, I., Hurlburt, G., and Voas, J. (2013). Today, the Internet of Things. Tomorrow, the Internet of Everything. Beyond that, perhaps, the Internet of Anything - a Radically Super-Connected Ecosystem Where Questions About Security, Trust, and Control Assume Entirely New Dimensions. *information-development*, page 4.

Bughin, J., Chui, M., and Manyika, J. (2010). Clouds, Big Data, and Smart Assets: Ten Tech-Enabled Business Trends to Watch. *McKinsey Q.*, 56(1):75–86.

Chang, V., Newman, R., Walters, R. J., and Wills, G. B. (2014). Review of Economic Bubbles.

Coppock, M. (2017). New 'BrickerBot' malware attack kills unsecured Internet of Things devices.

Duncan, B., Happe, A., and Bratterud, A. (2016). Enterprise IoT Security and Scalability: How Unikernels can Improve the Status Quo. In *9th IEEE/ACM Int. Conf. Util. Cloud Comput. (UCC 2016)*, pages 1–6, Shanghai, China.

Duncan, B. and Whittington, M. (2014a). Compliance with Standards, Assurance and Audit: Does this Equal Security? In *Proc. 7th Int. Conf. Secur. Inf. Networks*, pages 77–84, Glasgow. ACM.

Duncan, B. and Whittington, M. (2014b). Reflecting on Whether Checklists Can Tick the Box for Cloud Security. In *Cloud Comput. Technol. Sci. (CloudCom), 2014 IEEE 6th Int. Conf.*, pages 805–810, Singapore. IEEE.

Duncan, B. and Whittington, M. (2015a). Company Management Approaches — Stewardship or Agency: Which Promotes Better Security in Cloud Ecosystems? In *Cloud Comput. 2015*, pages 154–159, Nice. IEEE.

Duncan, B. and Whittington, M. (2015b). Enhancing Cloud Security and Privacy: Broadening the Service Level Agreement. In *14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. (IEEE Trust.*, pages 1088–1093, Helsinki, Finland.

Duncan, B. and Whittington, M. (2015c). The Importance of Proper Measurement for a Cloud Security Assurance Model. In *2015 IEEE 7th Int. Conf. Cloud Comput. Technol. Sci.*, pages 1–6, Vancouver.

Duncan, B. and Whittington, M. (2016a). Enhancing Cloud Security and Privacy: The Cloud Audit Problem. In *Submitt. to Cloud Comput. 2016*, pages 1–6, Rome.

Duncan, B. and Whittington, M. (2016b). Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail. In *Submitt. to Cloud Comput. 2016*, pages 1–6, Rome.

Duncan, B. and Whittington, M. (2017). Creating an Immutable Database for Secure Cloud Audit Trail and System Logging. In *Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization*, pages 54–59, Athens. IARIA, ISBN: 978-1-61208-529-6.

Gantz, J. F., Reinsel, D., Chute, C., Schlichting, W., McArthur, J., Minton, S., Xheneti, I., Toncheva, A., and Manfrediz, A. (2007). The Expanding Digital Universe: A Forecast of Worldwide Information Growth Through 2010. In *Extern. Publ. IDC (Analyse Futur. Inf. Data*, pages 1–21. IDC.

Gantz, J. F., Reinsel, D., Chute, C., Schlichting, W., Mcarthur, J., Minton, S., Xheneti, I., Toncheva, A., and Manfrediz, A. (2010). The Expanding Digital Universe: A Forecast of Worldwide Information Growth Through. *Inf. Data 2007*, pages 1–21.

Greenberg, A. (2017). Securing Driverless Cars From Hackers Is Hard. Ask the Ex-Uber Guy Who Protects Them.

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Futur. Gener. Comput. Syst.*, 29(7):1645–1660.

InnovationCities.com (2017). Innovation Cities™ Index 2016-2017: Global.

Koebler, J. (2015). Hackers Killed a Simulated Human By Turning Off Its Pacemaker.

Kumbhar, S. (2016). Critical role for the Internet of Things in wastewater.

Larson, D. and Chang, V. (2016). A Review and Future Direction of Agile, Business Intelligence, Analytics and Data Science. *Int. J. Inf. Manage.*, pages 1–25.

Mell, P. and Grance, T. (2011). The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. Technical report, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD.

Newman, L. H. (2017a). Medical Devices Are the Next Security Nightmare.

Newman, L. H. (2017b). Security News This Week: Yes, Even Internet-Connected Dishwashers Can Get Hacked.

OWASP (2013). OWASP Top Ten Vulnerabilities 2013.

OWASP (2014). OWASP Top 10 IoT Vulnerabilities (2014).

OWASP (2016). OWASP SQL Injection Cheat Sheet.

OWASP (2017). OWASP home page.

Pritchard, S. (2016). Internet of things: humble lightbulbs could become a form of attack.

Sharma, S., Chang, V., Tim, U. S., Wong, J., and Gadia, S. (2016). Cloud-based Emerging Services Systems. *Int. J. Inf. Manage.*, pages 1–19.

Shell (2016). A Better Life with a Healthy Planet. Technical report, Shell, London.

Shell (2017). Shell Scenarios: New Lenses on Future Cities.

Suciu, G., Vulpe, A., Halunga, S., Fratu, O., Todoran, G., and Suciu, V. (2013). Smart cities built on resilient cloud computing and secure internet of things. In *Control Syst. Comput. Sci. (CSCS), 2013 19th Int. Conf.*, pages 513–518. IEEE.

Symantec (2015). Is there an Internet-of-Things vigilante out there?

Trustwave (2012). 2012 Global Security Report. Technical report.

Verizon (2012). 2012 Data Breach Investigation Report: A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service and Others. Technical report.

Verizon (2015). Verizon 2015 Data Breach Investigation Report. Technical report.

Willingmyre, G. T. (1997). Standards at the Crossroads. *StandardView*, 5(4):190–194.

Wired.com (2015a). Hackers Remotely Kill a Jeep on the Highway - With Me in It.

Wired.com (2015b). Researchers Hacked a Model S, But Tesla's Already Released a Patch.

Wired.com (2015c). The Doctor on a Quest to Save Our Medical Devices From Hackers.

Zetter, K. (2015a). Hacker Can Send Fatal Dose to Hospital Drug Pumps.

Zetter, K. (2015b). The Doctor on a Quest to Save Our Medical Devices From Hackers.