ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 5 Issue -03 March, 2016 Page No. 15966-15970

Security Ecosystem in IoT & Cloud

Pokuri Rajani, Parupally Anuja Reddy
Department of Computer Science and Engineering
G Narayanamma Institute of Technology & Science
Hyderabad, India
pokurirajanigupta@gmail.com
Department of Computer Science and Engineering
G Narayanamma Institute of Technology & Science
Hyderabad, India
anujareddy1996@gmail.com

Abstract*— The cloud computing and the Internet of things are tightly coupled with each other . The rapid growth of the Internet of Things (IoT) and the development of technologies created a widespread connection of "things". This results in the production of large amounts of data which needs to be stored, processed and accessed. Cloud computing is a paradigm for big data storage and analytics while the Internet of Things is exciting on its own that the real innovation will come from combining it with cloud computing . This can enable sensing services and powerful processing of sensing data stream. More things are being connected to address a growing range of business needs. In fact, by the year 2020, more than 50 billion things will connect to the Internet—seven times our human population. Insufficient security will be a critical barrier to large-scale deployment of IoT systems and broad customer adoption of IoT applications using cloud. Simply extending the existing IT security architectures to the IoT and cloud will not be sufficient. The IoT world requires new security approaches, creating fertile ground for innovative thinking and solutions. This paper discusses key issues that are believed to have long-term significance in IoT and cloud computing security and privacy, based on documented problems and exhibited weaknesses.*

Keywords— Internet of things (IoT), Cloud Computing , analytics , Internet, Broadband, Things

INTRODUCTION

Internet of Things or IoT has become a very hot topic nowadays for consumers and businesses alike. Some claim that IoT will totally transform how people use the internet and computer networking in the next decade or century. Current predictions estimate that by 2020, there will be over 20 billion connected devices, thus creating a huge potential for IoT to impact our lives in an innumerable number of ways.

Cloud computing is defined as a type of computing that relies on *sharing computing resources* rather than having local servers or personal devices to handle applications.

I. SECURITY ISSUES IN IOT

Despite providing great benefits and conveniences for our lives, there are some significant risks involved with wearable. To better understand these risks, here is a sample from what tech leaders in the sector are saying with regards to wearable usage and its security implications:

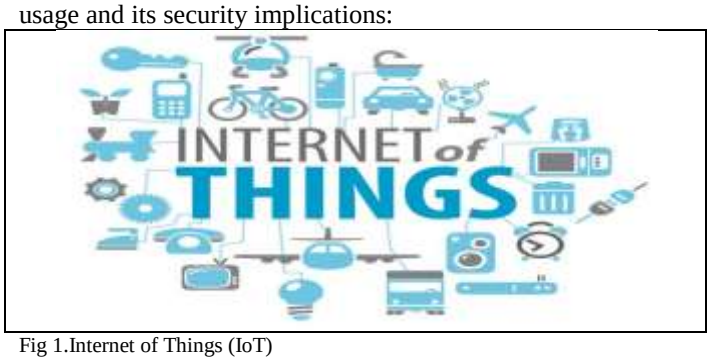

Fig 1.Internet of Things (IoT)

A. Wearables are secretly jeopardising privacy and security

Teena Hammond, a contributor of TechRepublic states that consumers are unknowingly exposing themselves to possible security breaches as well as ways that personal data might be used by organizations with consumers ever knowing. We are entering a world where every detail is documented and catalogued, and governments and companies will be basing their decisions on a person's data trail. Thus, privacy protection is very important if we are to be considered as individuals, rather than just data points. The main reason behind possible security breaches in IoT wearable is due to the very high value of personal data. Information that your wearable device collects and stores locally on your phone or the cloud is much more valuable than your credit card details. Credit card breaches are very easy to deal with; just a simple cancellation of what was done during the breach. A very short lifespan in the black market. However, information collected on wearable does not go away. It is impossible to change personally identifiable data like date of birth and social security details. With health data, security breaches pose even a greater risk.The article states that the main problem with securing wearable is that most producers are in a rush to get their products to the market. When companies are only interested in getting their products ready as fast as possible, they are essentially producing extremely vulnerable devices. Even if they supply security patches afterward, you cannot expect all users to keep updating their devices.To reduce these

risks, the article suggests that companies build security and privacy in their development process. This will help with fixing future errors, doing investigations and also dealing with industry regulators.

B. WT VOX believes wearables trigger shocking security risks

The results of an investigation by HP into popular wearable devices are discussed. The devices included webcams, sprinkler controllers, door locks, home alarms and home thermostats among other common wearable devices. Out of the total ten devices that HP investigated, eight triggered key privacy concerns by failing to demand passwords of adequate length and complexity, while still presenting a risk of data interception through cloud services.

Generally, 70% of the wearable were deemed highly vulnerable to hacking. Some of the greatest points of weakness discovered in the investigation include:

- Insufficient authorization
- Privacy concerns
- Insufficient software protection
- Insecure web or cloud interface
- Lack of sufficient transport encryption

C. SYMANTEC has also analysed the security risks of variables

The recent Symantec Internet Security Threat Report Vol. 20 discovered that the hacking risks of IoT devices have increased greatly, possible due to how Smartphones are used as the controlling point. Symantec discovered that in 2014, 52% of health applications, most of which have connectable wearable devices, did not have privacy policies in place. Furthermore, 20% of the health apps used clear text to send personal information, passwords, and logins. According to Symantec, consumer wearable are not the only ones being attacks, as differing industries that use IoT are also under attack. In 2014, a pipeline explosion that occurred in Turkey was found to be caused by cyber-attacks. Besides financial gain, criminals are also intent on destroying a company's brand image or simply to prove vulnerabilities. Symantec notes that security needs to be inclusive and comprehensive, rather than an added feature. Security programs must be built into the devices for better protection. With the rising number of wearable and other IoT devices, security concerns are also going to increase significantly, and Symantec is in a unique position to share cyber security intelligence on quickly evolving threats.

D. Computer world suggests that wearable computers have an array of hidden dangers

The list of key security concerns includes vulnerabilities of life-blogging tools, embedded or wearable medical devices, cop cams, smart clothing, smart watches and fitness bands. The article highlights the major uses of these wearable devices and how they could be compromised. Life-blogging tools are essentially wearable cameras that are GPS-enabled and allow people to document every moment of their day and share. The tiny cameras are always on and are specifically designed to repeatedly capture thousands of photographs a day. The obvious threat is that even though these cameras can create detailed journals of a person's life, they essentially invade the privacy of other people being photographed without their permission or knowledge. For wearable in the health sector, their wireless feature poses a great risk. For instance, someone could easily hack a patient's insulin pump and deliver a lethal dose. Another research has discovered how having poorly secured pacemakers offers exploitation opportunities where a hacker can send a fatal shock to a person wearing the medical device.

II. SECURITY ISSUES IN CLOUD

A majority of enterprise organizations are embracing cloud computing in one form or another. According to ESG research, 67% of enterprises use public or private cloud infrastructure today, while 66% use one or several SaaS applications. So what about network security? It's a bit of a struggle today as many organizations move to cloud computing long before they have the right infosec skills, processes, or tools in place.

Failure to ensure appropriate security protection when using cloud services could ultimately result in higher costs and potential loss of business, thus eliminating any of the potential benefits of cloud computing.

The aim of this guide is to provide a practical reference to help enterprise information technology (IT) and business decision makers analyze the security implications of cloud computing on their business. The paper includes a list of steps, along with guidance and strategies, designed to help these decision makers evaluate and compare security offerings from different cloud providers in key areas.

Fig. 2: Security in cloud

When considering a move to cloud computing, customers must have a clear understanding of potential security benefits and risks associated with cloud computing, and set realistic expectations with their cloud provider. Consideration must be given to the different service categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) as each model brings different security requirements and responsibilities. Additionally, this paper highlights the role that standards play to improve cloud security and also identifies areas where future standardization could be effective.

This paper provides an overview of the security and privacy challenges pertinent to cloud computing and points out considerations that organizations should weigh when migrating data, applications, and infrastructure to a cloud computing environment. It discusses the threats, technology risks, and safeguards for cloud computing environments, and provides the insight needed to make informed IT decisions on their treatment.

E. Cloud Security Landscape

While security and privacy concerns1 are similar across cloud services and traditional non-cloud services, those

concerns are amplified by the existence of external control over organizational assets and the potential for mismanagement of those assets. Transitioning to public cloud computing involves a transfer of responsibility and control to the cloud provider over information as well as system components that were previously under the customer's direct control.

Despite this inherent loss of control, the cloud service customer still needs to take responsibility for its use of cloud computing services in order to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of the organization. The customer achieves this by ensuring that the contract with the provider and its associated cloud service agreement has appropriate provisions for security and privacy. In particular, the agreement must help maintain legal protections for the privacy of data stored and processed on the provider's systems. The customer must also ensure appropriate integration of cloud computing services with their own systems for managing security and privacy.

There are a number of security risks associated with cloud computing that must be adequately addressed:

- Loss of governance
- Responsibility ambiguity
- Authentication and Authorization
- Isolation failure
- Compliance and legal risks
- Handling of security incidents
- Management interface vulnerability
- Application Protection.
- Data protection.
- Malicious behavior of insiders
- Business failure of the provider
- Service unavailability
- Vendor lock-in.
- Insecure or incomplete data deletion
- Visibility and Audit

Cloud computing does not only create new security risks: it also provides opportunities to provision improved security services that are better than those many organizations implement on their own. Cloud service providers could offer advanced security and privacy facilities that leverage their scale and their skills at automating infrastructure management tasks. This is potentially a boon to customers who have little skilled security personnel.

III. CHALLENGES

The sheer magnitude of IoT justifiable flaws causes anxiety for many network administrators, and it also merges with another essential challenge that complicates the provision of effective security solutions – the presence of a large number of types of wearable devices – a device mesh. There are so many different capabilities, different generations, different uses and different vendors of wearable devices in the market today, which, of course, makes achieving security more challenging. You can consider the fact that today we currently have malware and spyware, but in future we are going to have specific viruses facing the IoT devices. Determining where there are vulnerabilities across several Smartphone OS types pales when compared to tracking thousands of distinctive sensors, meters, cameras, machines and other controllers. Besides the management of many interconnected things, IoT security will also involve lots of connection methodologies and protocols. That becomes nightmarish because you must support all these connected things, and you need to read every security bulletin and stay up to date on all vulnerabilities that happens in all the different types of wearable. Unfortunately, many wearable will likely never get any updates from their manufacturers, so patches are not going to help address the emerging threats.

Fig. 3: Challenges in Iot And Cloud

IV. SECURITY ECOSYSTEM: HOW CAN WE PROTECT OURSELVES?

For businesses, traditional network security approaches must be reconsidered before an organization deploys any IoT program. Realize that there is no single firewall product that is going to solve this issue. Rather, businesses need to familiarize themselves with security solutions that are designed specifically for IoT challenges.

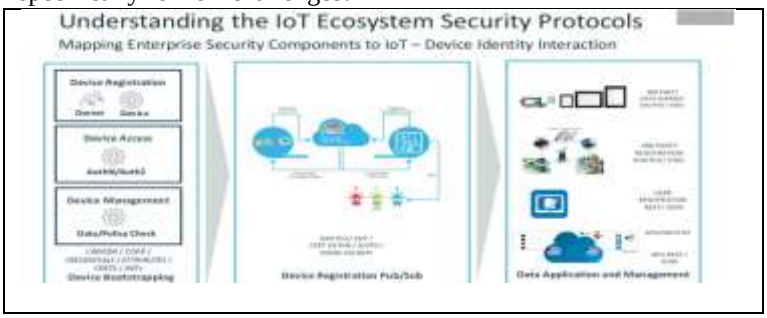

Fig.4: IoT Security Ecosystem Security Protocols

F. Separating IT and IoT:

Since firewalls might not be effective in IoT traffic, a new approach must be considered. Ultimately, security administrators may even decide on putting wearable on completely different networks, thus separating IT and IoT devices. When a hacker compromises one network, it will not allow easy accessibility to the other. While this might sound like an extreme protection strategy, but in matters that concern important data, the business must perform risk assessments to ascertain the appropriate network separation level. Staying updated with evolving improvements in IoT security and vulnerability assessments will be crucial too.

G. Health issues:

What if the device stops working or sends the wrong data? Bodily injury is another issue that wearable manufacturers have to plan for. Malfunctioning devices may cause illness, injuries and even the loss of life of patients or wearers.In such

cases, the device manufacturers can face product liability lawsuits. The following strategies may help in protecting against risks related to bodily injury:

- extensive testing during production,
- conducting a better hazard analysis,
- planning for mitigation,
- developing clear use and safety instructions
- evaluating adherence to and awareness of key standards.

Fig.5: Issues related to Iot and cloud

H. Other solutions for security in IoT:

Other than that, it advisable for anyone using any kind of wearable technology to sign up and utilize one of the many software and hardware solutions engineered to mitigate the vulnerability of these devices. A good example is the Cujo handheld and portable anti-hacking module. With such a device, you can centralize and encrypt all communication networks surrounding all your smart wearable devices making any it virtually impossible to hack or remotely control the device (s) in question. Yes, it might cost a bit extra to do this, but as you will soon realize, you could be averting the potential loss of a lot of money or even life. If everything fails, at least ensure you are ready for possible security breaches. Always have a good exit plan ready, a way to secure data quickly and render any compromised information useless without damaging the IoT infrastructure. Furthermore, it is necessary that everyone involved, including employees and customers, is properly educated about the possible security breaches. Provide instructions on how to tackle these breaches, and also how to prevent them.

I. Cloud Security Guidance:

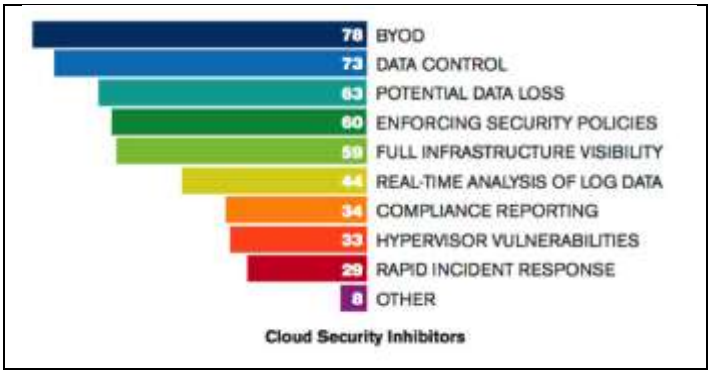

Fig.6: Cloud security inhibitors

As customers transition their applications and data to the cloud, it is critical for them to maintain, or preferably surpass, the level of security they had in their traditional IT environment.

This section provides a prescriptive series of steps for cloud customers to evaluate and manage the security of their use of cloud services, with the goal of mitigating risk and delivering an appropriate level of support. The following steps will be discussed in detail below:

1. Ensure effective governance, risk and compliance processes exist
2. Audit operational and business processes
3. Manage people, roles and identities
4. Ensure proper protection of data and information
5. Enforce privacy policies
6. Assess the security provisions for cloud applications
7. Ensure cloud networks and connections are secure
8. Evaluate security controls on physical infrastructure and facilities
9. Manage security terms in the cloud service agreement
10. Understand the security requirements of the exit process

V.CONCLUSION

The technology behind Internet of Things (IoT) assumes that related technology and underlying network devices can operate automatically and intelligently. Even if security experts addressed all the security concerns related to wearable, people have increasingly become too dependent on this kind of automation. Since this technology has yet to be made resilient, any technical malfunctions can result in physical injury and financial damages. Thus, even with the hype surrounding wearable continuing to rise, especially with the unlimited possibilities that IoT and cloud creates, sobriety is vital to ensure that manufacturers are designing their devices with security in mind and consumers are more cautious about wearable.

Either way, it is the hope of the average consumer who relies on such devices that tech experts will close the various loopholes surrounding IoT and cloud technology as soon as possible.

J. Abbreviations and acronyms :

- IoT: Internet of Things
- IaaS : Infrastructure as a Service
- PaaS : Platform as a Service
- SaaS :Software as a Service

ACKNOWLEDGMENTS

Security Ecosystem in Iot & Cloud document is a collaborative effort that brings together diverse customer-focused experiences and perspectives into a single guide for IT and business leaders who are considering adopting cloud computing using Internet of things (IoT). The major contributors to this effort are: Claude Baudoin (cébé IT & Knowledge Management), Eric Cohen (PricewaterhouseCoopers), Chris Dotson (IBM).

REFERENCES

[1] Cloud Standards Customer Council. Practical Guide to Cloud Service Agreements. http://cloud-council.org/resource-hub.htm#cscc-practical-guide-SLAs

[2] Cloud Standards Customer Council. Cloud Security Standards: What to Expect & Negotiate.

http://cloud-council.org/resource-hub.htm#cloud-security-standards-what-to-expect-what-to-negotiate
[3] ISO/IEC 27001
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534
[4]C.Chapman,W.Emmerich,F.Glan,S.Clayman,A.Galis "Elastic Service Management in Computational Clouds",12th IEEE/IFIP NOMS2010/International Workshop on cloud management,19-23 April 2010,Osaka
[5]Strassner,J.,O Foghlu,M.Donnelly "Beyond the Knowledge Plane:An inference Plane to Support the next generation Internet",IEEE GIIS 2007,2-6 July,2007
[6]Blumenthal,M.Clark.d,"Rethinking the design of the Internet:the end to end arguments vs. the brave new world",ACM Transactions on Internet Technology,Vol.1,No.1,August 2001
[7]Bijan,P.et.al."Cautiously Approaching SWRL".2006 https://www.mindswap.org/papers/CautiousSWRL.pdf
[8]V.Holub,T.Parsons,P.O'Sullivan and J.Murphy.Run-time correlation of Security and Iot & Cloud Syst.,,15:757-768,October 1999

a.