NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 3, ISSUE 9, Sep.-2016

SECURITY CHALLENGES AND STRATEGIES FOR THE IOT IN CLOUD COMPUTING

LAKSHMISRI SURYA,
Data Scientist & Department of Information Technology California, USA
lakshmisri.suryaa@gmail.com

ABSTRACT
The Internet of Things has reshaped the way things are performed across the computing world. This is why integration between cloud computing and IoT devices is crucial because the amount of data being produced by IoT devices requires proper and secure storage as well as a processing system. Even so, security concerns remain more important because people share a wide range of cloud computing resources in their devices in numerous ways. Privacy is much more critical in a world where our wellbeing could be jeopardized by unsecured data. Therefore, the internet of things in cloud computing must always ensure the security and privacy concerns of users are always guaranteed. This research paper looked at issues like the security and strategies that can be applied in IoT in cloud computing. The findings indicate that there are major security problems and threats that still need to be addressed. To design architecture and to make changes to current software to achieve that goal. This paper discusses multiple security challenges facing the IoT in cloud computing especially concerns surrounding privacy and cybersecurity threats of the users.
Keywords: Internet of Things, Security, Cloud computing, privacy

INTRODUCTION
IoT and cloud are working together to form a data-storage-intensive framework where security is the most critical consideration for the protection of data. Cloud Computing refers to services that provide highly scalable, flexible, and storage computing resources on a pay-per-use basis [1]. Cloud computing services for computation and storage are becoming more prominent and several companies are already opting to transfer their data from the in-house network infrastructure to the Cloud Storage Providers (CSPs). With the rise in the demand for certain IoT devices, there will also be a rise in the development of apps that will have security challenges while connecting to cloud services. In the future, a new generation of Internet of Things systems will be able to provide more sophisticated services focused on increasingly fine-grained data collection in a world densely packed with smart things. In the past years, there has been a large number of IoT devices like advanced building management systems, public surveillance, smart city services, and even participatory sensing that allow users to do their work easily [1]. To handle time-varying workloads and big data in IoT applications, both traditional processing and cloud computing will present a challenge to achieving the intended goal. Furthermore, the encryption methods are not yet as powerful as they ought to be, and the third-party auditors tasked with handling the data and maintaining its integrity are also in their early stage of development. The amount of data collected on individuals by many government departments is growing faster annually, and becoming harder, for people to understand its impacts. This form of data makes privacy issues more likely. Ignorance about these problems can have long-term negative effects causing non-acceptance of the technology, failure of new technology due to credibility issues, and expensive lawsuits [2]. The study will present the evolution of IoT in cloud computing, the security challenges in IoT, and the numerous strategies that can be implemented to resolve the issues. The main objective of the study is to understand the security challenges and strategies that can be adapted by IoT in Cloud Computing to enable secure storage and safe transfer of IoT data in Cloud computing.

RESEARCH PROBLEM

What this paper aims at resolving are the security challenges that face the users while using IoT devices in cloud computing. The Internet of Things technology is being used and is constantly being perfected into a more live-centered, ubiquitous computing service requiring enormous quantities of data processing and storage. However, there are still issues that affect the industry which must be addressed. Looking at the security challenges in this paper will help in identifying the source of the issues and find strategies that can address them. IoT and cloud are working together to form a data-storage-intensive framework where security is the most critical consideration for the protection of data. Privacy challenges have been a hot research subject in different technological advances that are critical enablers of the IoT vision, such as wireless sensor networks (WSN), web personalization, Radio Frequency Identification (RFID) as well as mobile apps and networks [3]. Despite major contributions from these groups a broad perspective of arising privacy concerns in the IoT is lacking, because the IoT is an everchanging concept that encompasses an increasing number of technologies and exhibits a variety of changing features. As the technological world continues to evolve, IoT devices will continue to face major security challenges that will be difficult to address [3]. Considering what these security problems can do to people's lives, the privacy issues in IoT devices accessing cloud computing services need to be considered and resolved.

LITERATURE REVIEW

A. Security Challenges in Internet of Things

Some of the security concerns surrounding the IoT devices in cloud computing include hijacking of IoT devices or ransomware, theft of IoT devices, unauthorized use of the internet, rogue devices, home invasions, and a variety of other potential risks.

1. Hijacking and Ransomware

Smart- Home devices, wearables devices, and audio-video devices that are connected to cloud services can become targets of Ransomware. Malicious malware that gains access to a user's files, encrypts, and blocks the user from accessing their sensitive files. When a hacker attacks an IoT device with ransomware, they can take control of the device and demand money if the victim hopes of seeing their encrypted files unlocked. Fortunately, it is a rare reality as of yet. But, this is a serious challenge in the hacking community and among the hackers themselves [4]. This security concern can put a smart home, healthcare trackers, and wearable technologies at risk. It is a disturbing thing to learn someone's smart house is hacked and locked down or even a smart vehicle that cannot be started until a ransom is paid. If the ransomware threats like some that have gone on in recent times win the battle, this could shut the user out of their devices and potentially lead to a loss of the user's data. The rapid expansion in the Internet of things technologies will cause some security concerns that will be unpredictable [5]. Even so, the bottom line regarding data theft is that most of the information is stored in a highly encrypted cloud, so it is very unlikely the person will have any worthwhile information to steal. According to one report, some IoT manufacturers do not provide necessary security and software updates [6].

2. There are insufficient testing and a lack of updates.

Another security challenge with the Internet of Things (IoT) is that many companies producing IoT devices are not properly chosen and often too disorganized to properly fix security-related software updates. Since consumers usually trust manufacturers who are often confident that they are in control of product safety, it becomes a big problem to the user in case of a security failure [7]. Although there is indeed a rapid growth of the Internet of Things platform, it is also true that a lot of manufacturing companies are swooping into the market without offering the marketing research much consideration. Web sites that offer shorter periods also

don't usually offer consistent updates. The reason for these updates is because of the rise in a shortage of devices. As a result, they make the new generation of devices that they ask the users to start using them without proper security measures [8].

If the IoT device has outdated software installed in it, it may be prone to numerous malicious attacks from hackers and other security breaches. There is also another risk of downtime when an IoT device sends its information to the cloud. During an upgrade, some parts of the app might stop functioning while others search for updated components of the app and submit the updated data. Firmware versions that are A49 and B06 have bugs that may lead to a more insecure router, so it is advisable to upgrade the firmware versions as soon as possible [9]. Given the many "internet of things" security risks, proper automatic updates are of paramount importance. The manufacturer of IoT devices has a duty of updating their devices into the latest software as soon as a vulnerability is detected and when a malware attack is discovered.

3. Home invasion

The most distressing scenario of the Internet of Things (IoT) security challenges is when users of IoT devices experience home invasions. Smart devices are currently extending into every part of our lives. The fact that many of our homes are connected to the Internet, has given rise to the concept of smart homes. The biggest problem with smart home systems is that, if there is any security loophole, there is a big risk of them broadcasting IP addresses to nearby hackers. The search engine Shodan can help out hackers in finding out the location of the user of the device. In terms of abuse, what can be concluded is that this technology can reach criminal circles and can be sold to the public [10]. As an introduction, the way to prevent that IoT security flaw from occurring is by configuring each device to connect through VPNs, considering the importance of passwords, and securing the login details.

4. Financial crime resulting from the Internet of Things.

As the Internet of Things payment companies deploys their internet of things, they should anticipate an increase in future identity theft and other financial crimes A few of these firms have focused on automation and artificial intelligence, while most of them will eventually need to be able to acknowledge the significance of integrating security measures on different company levels. To ensure that fraud detection programs remain more effective, they must continuously monitor their data source for new fraud patterns. All financial firms will experience reservations about the adoption of these new models because they face several issues on compliance and operational aspects [11]. In simple terms, IoT security breaches can take many different shapes, including (but not limited to) attacks of different systems, smart-protocol failures, and IoT device hacks.

5. Remote Smart Vehicle Access

The hijack of smart cars is close to a security threat of home invasion. Vulnerable Internet of Things (IoT) devices can lead to vulnerabilities in smart cars, such as remote hijack of the car's access [12]. Compromising the vehicle's functionalities can affect the vehicle's autonomous capabilities to operate like self-driving functionalities and detection of other vehicles. There have been many cases of threats to public safety concerns that have caused injuries. Losing access to the car can also be subject to a tie into remote hacking especially when a hacker locks the car's doors and demands payment for unlocking or enabling the engine.

Many cars and IoT device manufactures are paying close attention to the many security breach issues. However, car manufacturers like BMW and Honda are also paying attention to these security breaches. Microsoft and Ford Motor have come up with an infotainment system that is completely vulnerable and open to these types of attacks [12]. The developers addressed several forms of these attacks, with their preferred

solutions one of the simplest of which was a deliberate upgrade to a more secure infrastructure and software package. The future introduction of remote-control cars will pose a major security threat to IoT devices.

6. Rogue and fake IoT devices

A significant security challenge is the ability to protect a system from being accessed from any one device. There's a challenge with using the IoT in one's home as it can become bulky if one chooses to install more home devices. Users end up mounting rogue and substandard IoT in secured networks without any network authorizations. These devices replace the original network units and/or integrate into the network to obtain confidential information and data, violating the secure perimeter of the network [12,13]. These smart devices have the potential to be turned into rogue access points, thermostats, video cameras, and other forms of devices to intercept network communications without the knowledge of the user.

7. The lack of user knowledge about the internet of things (IoT) security.

There are a large number of people who are still learning the quirks and traits of the Internet of Things (IoT). Most users have now perfected their security issues regarding phishing, malware, and viruses on computers or internet fraud. Before they perform internet banking, they spent some time learning about securing their internet connection and also learning how to safeguard their credit cards online.

But, as is has been reported, IoT devices still fail, not only due to the manufacturers' limitations but also due to the users themselves, who didn't take the required measures to protect their devices and networks. The lack of computer awareness is the biggest issue with the Internet of Things because it opens up the possibility of abuse by both users themselves, as well as those who would be connected with their own IoT networks [13]. Social engineering hackers target the human factor because it is the most easily bypassed using the Internet of Things. A serious case of the unprepared human factor is the 2010 attack on a nuclear site in Iran, which was and will always be very tragic. The attackers targeted the IoT tool called a programmable logic controller, which meant that the device only needed only one worker to insert a small flash drive into the controller, thus allowing an attacker to penetrate the system in the internal network and make that network public.

B. Strategies of responding to insecure IoT device

1. Changing passwords regularly and making them strong.

Changing/updating passwords, regularly, on internet accounts, mobile devices, and computers have become a social norm nowadays. As sophisticated as the Internet of Things has been, it should become a standard by now. It is important to make sure that:

- Every other IoT device is assigned a unique password.
- Making sure that passwords are changed at least multiple times during the year.

Avoiding known and common terms.

- Using special codes that are very difficult and tricky to crack.

Overreliance on password managers will lead to an increased risk of someone snooping on all or even only a few of the passwords. Users need to use a traditional method instead, whereby instead of relying on password managers, write down your passwords securely and store them carefully.

2. Generating a backup by storing the files and data locally

Cloud technology is very advantageous, but at the same time, it is also very vulnerable technology that is prone to attacks. Technological companies often give users cloud storage space free for the electronic gadget they purchase [14]. Although it is appealing to have a free item, users must also be careful about the security measures.

- Accessing cloud services requires an active connection to access any files and/or data.
- This cloud service can be accessed and hacked into while accessing the account.

If they have a Dropbox or Google account, the users should carefully go through the security precautions that come with their choice. They must also make sure that they secure the data and store their data locally beyond the reach of hackers.

3. Avoiding Universal Plug & Play functionality.

The Universal Plug & Play feature makes it easy for multiple devices to connect, such as when one computer is plugged into another computer. This allows several different devices to be shared and installed in one workgroup [15]. Among the users who use this platform experience obvious convenience. However, the users need to be careful of this product because of the ease of exploitation.

• The Universal Plug & Play protocols exploit local networks for connecting.
• These networks, as we've seen, are also very vulnerable to outside hacks and can be easily accessed.

4. Using the Secondary Network

WiFi users frequently come up with several networks that personalized networks that can only be accessed in their house. This method of creating private networks should also be extended to IoT and smart devices to:

- Blocking the public from accessing confidential information.
- Block any efforts of controlling the IoT units and wreaking havoc using offensive software.
- Ensuring the system is out of control by intruders by encrypting the system.

5. Making sure to periodically update the IoT device

Users need to update the IoT system while automatic updates must be enabled by the manufacturing company itself so that the device check for official updates automatically. This will ensure the automatic installation of security updates on the IoT devices and stops unauthorized persons from finding new ways of accessing the system [16]. Frequent updates on IoT devices occasionally provides:

- Safety of the device as it is upgraded with improved security measures to prevent attacks such as Distributed Denial of Service (DDoS) and malware.
- High security for the house or office against remote invasions.

As a result, that new security protocols will be developed that will concentrate on and bring forward new developments in:

- Stable cloud computing in IoT
- IoT system security structures
- IoT device security techniques
- Detection of attacks on Internet of Things networks and detecting intrusions utilizing artificial intelligence.
- Stable IoT systems structure
- Protection of personal data and the security of IoT devices

The debate on IoT protection in cloud computing is complex. There are possible integrity violations that come from many, mutually exclusive sources. IoT technologies in cloud computing have only been around for a relatively short period [17]. This technology is still at its infancy stage and searching for what works best for consumers and manufacturers alike. With the IoT, we have seen one of the main security problems that stem from.

- Attacks from Malware and the frequent hijacking of smart IoT devices
- Rogue IoT units.
- Lack of system updates

- Low quality in manufacturing
- The low user competence due to a lack of awareness.
- •An unequal norm of production.

Some of the security strategies that can be used to address these issues include:

- Separating IoT network from other networks
- Ensuring passwords are unique and strong
- Avoiding Plug & Play features
- Utilizing backups to store the files

SIGNIFICANCE OF THE RESEARCH TO THE U.S

This research will be significant to the United States in creating the minimum cybersecurity standards especially those owned and controlled by the federal government. Having understood how the vulnerabilities occur in various devices, there will be more strategies aimed at bringing order to the IoT device security chaos. The recent intrusion of Amazon's Ring devices like doorbells and cameras caused a lot of worry to many consumers who had installed these devices. Understanding the strategies on how to protect themselves will be beneficial in preventing any remote access to smart houses and self-driving cars. This research will also help the manufacturers IoT on meeting the required standards of security to protect the users from cyber-attacks. It will also be good for innovation as more security features will be integrated into the IoT systems that access cloud services.

CONCLUSION

Although there are increasing concerns on the security of IoT devices in cloud computing, there is ongoing research from various stakeholders to understand its source and how to mitigate them. In the future businesses will recognize the potential of IoT in cloud computing as the industry expands. This means that the developers will have to double the cybersecurity measures to fulfill corporate demands. To prevent some of the more frequent threats, consumers must learn some of the security measures to be aware of any security threats on their IoT devices. As with all technological advances in IoT usage in the government will also play a bigger role through legislation. New rules will be coming into effect to mandate that IoT devices that are purchased come with certain minimum safety measures. There are several companies currently selling items with embedded security in them. There are certain aspects in which the wireless technologies are being optimized such as increasing contact speeds and processing capacity, Convex minimization, Machine learning, AI-based optimization that takes advantage of hybrid approaches, Heuristic methods, Artificial neural networks, and Evolutionary algorithms. Cloud computing is undoubtedly a valuable technology that has been adopted by many companies. However, there is no guarantee that it can be trusted to store and transfer data securely due to data security challenges. Every organization must take responsibility for managing its data protection footprint and put systems in place to cope as well as deal with any flaws that are found. Additionally, considerations must be made by a user on service transparency, vendor lock-in, and visibility before committing to a specific manufacturer. Although technology and resources like these provide quick fixes, there should be other measures focusing on long term strategies. The fact that there is no Security standard is a problem since IoT devices became popular years back, through their growing use outpacing the sector's capacity to agree on how to protect them. To ensure that newly found problems are still fixed, manufacturers must address the challenge of making sure that there be easy to fix for customers. But the burden also falls on the users who should upgrade their IoT applications, rather than continuously pressing the 'Ignore' button. The manufactures must also ensure that the IoT devices are capable of keeping the data registers up-to-date.

REFERENCES

1) J. Veijalainen, D. Kozlov, and Y. Ali, "Security and privacy threats in IoT architectures," in Proceedings of 7th International Conference on Body Area Networks, Oslo, Norway, September 2012.
2) S. J. Kumar and D. R. Patel, "A survey on internet of things: security and privacy issues," International Journal of Computer Applications, vol. 90, no. 11, pp. 20–26, 2014.
3) M. R. Schurgot, D. A. Shinberg, and L. G. Greenwald, "Experiments with security and privacy in IoT networks," in Proceedings of IEEE World of Wireless, Mobile and Multimedia Networks (WoWMoM), Boston, MA, USA, June 2015.
4) O. Vermesan and P. Friess, Internet of Things Applications - From Research and Innovation to Market Deployment. Aalborg: River Publishers, 2014.
5) B. Khoo, "RFID as an enabler of the internet of things: issues of security and privacy," in Proceedings of 4th International Conference on Cyber, Physical and Social Computing, pp. 709–712, Dalian, China, 2011.
6) X. Lu, Q. Li, Z. Qu, and P. Hui, "Privacy information security classification study in internet of things," in Proceedings of 2014 International Conference on Identification, Information and Knowledge in the Internet of Things, pp. 162–165, Beijing, China, October 2014.
7) X. Xiaohui, "Study on security problems and key technologies of the internet of things," in Proceedings of IEEE Fifth International Conference Computational and Information Sciences (ICCIS), Hubei, China, June 2013.
8) J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: threats and challenges," Security and Communication Networks, vol. 7, no. 12, pp. 2728–2742, 2014.
9) D. Christin, M. Hollick, and M. Manulis, "Security and privacy objectives for sensing applications in wireless community networks," in Proceedings of ICCCN, pp. 1–6, Zurich, Switzerland, August 2010.
10) A. Samani, H. H. Ghenniwa, and A. Wahaishi, "Privacy in Internet of Things: a model and protection framework," Procedia Computer Science, vol. 52, pp. 606–613, 2015.
11) T. U. Darmstadt, "Security and privacy challenges in industrial internet of things," in Proceedings of 52nd Annual Design Automation Conference, pp. 1–6, San Francisco, CA, USA, June 2015.
12) J. Daubert, W. Alexander, and P. Kikiras, "A view on privacy & trust in IoT," in Proceedings of IOT/CPS-Security Workshop IEEE International Conference on Communications (ICC), London, UK, June 2015.
13) K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," Ad Hoc Networks, vol. 32, pp. 17–31, 2015.
14) T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the IP-based internet of things," Wireless Personal Communications, vol. 61, no. 3, pp. 527–542, 2011.
15) J. L. Hernandez-Ramos, M. P. Pawlowski, A. J. Jara, A. F. Skarmeta, and L. Ladid, "Toward a lightweight authentication and authorization framework for smart objects," IEEE Journal on Selected Areas in Communications, vol. 33, no. 4, pp. 690–702, 2015.
16) G. Peretti, V. Lakkundi, and M. Zorzi, "BlinkToSCoAP: an end-to-end security framework for the internet of things," in Proceedings of Communication Systems and Networks (COMSNETS), pp. 1–6, Bangalore, India, January 2015.
17) G. Piro, G. Boggia, and L. a. Grieco, "A standard compliant security framework for IEEE 802.15.4 networks," in Proceedings of Internet of Things (WF-IoT), pp. 27–30, Seoul, South Korea, March 2014.