Launching into Cyber Security September 2020

« Collaborative Learning Discussion 2

Lewle Seneviratne

Initial Post - Cloud and Wireless Sensor Networks

20 days ago

4 replies

Last 9 days ago

The revolution in the digital transformation through networking-dependent and data-based technologies such as cognitive, IoT, blockchain, and advanced analytics is fuelling adoption of connectivity advances. This rapidly changing operational technology landscape poses a major cyber security concern for their users. To manage these risks while talking about the full benefits of digital transformation, it is vital to understand today's advanced-network-technologies while assessing their vulnerabilities.

Cloud

Cloud computing presents a new model for the operational technology landscape, fundamentally changing the way organisations' strategies and operate. Today, it has completely flipped the architecture of hosting hardware in a local (physical) space to one of four cloud service models through service providers like Google Cloud Platform (GCP), Amazon Web Services or Microsoft Azure, making organisations trust all of their systems and data in a third-party environment.

Regarding security and uptime though providers must meet certain legal and industry standards, it is not possible for users to outsource all their security responsibilities. However, with each service model (BPaaS, IaaS, PaaS, SaaS and CaaS), levels of control over data and ability to see specifically how it is handled once it reaches the cloud varies.

For example, when you delete data from a local system, probably it is difficult to have visibility to verify that deleted data have been deleted in Cloud as requested, and thus it is difficult to be certain of its security. Actual data storage and deletion processes vary among providers and considering the structure of Clould there is a good chance that data is spread over various devices and in various physical locations for redundancy. Reference to the 2017 Apple iCloud hacking, if a file is deleted on the local instance, but there is no internet connection, that file could still be stored on two other backups (Dunn). Many celebrities had their personal photos stolen as a hacker could gain access to your cloud account and have access those files (Gupte, 2017).

Going back to the incident in 2013, cloud provider Nirvanix that went bankrupt gave only two weeks to their customers to retrieve their data before the system would be closed and everything lost. The shift of assets and operations to the Cloud, poses decreased visibility and control compared to in-house operations. This was the same situation experienced by Nirvanix's customers and it was a near impossibility to retrieve all their data before the deadline. As the only option though Nirvanix established an arrangement to shift data to IBM, this prevented customers having the possibility to choose their service providers such as Google, Microsoft, Amazon, or another alternative (Bocetta,2019).

Wireless Sensor Networks (WSN)

The emergence of Wireless Sensor Networks (WSN) has gained significant attention due to its vast range of applications in areas such as manufacturing, mobilePay, mobile banking, homeland security, telemedicine, climate monitoring, agriculture, battlefield, etc.

A Wireless Sensor Network also needs tools to protect against both insider and outsider attacks. Such attacks could compromise the network to get sensitive data from legitimate devices and disrupt the network to deny service through inserting Trojan horse device and impersonating networks. Such vulnerabilities call the need to have successful network security techniques to support authentication, authorisation and attack detection (Cisco Systems Inc., 2020).

Due to recourse-contained nature of sensor node, data corruption is one of the significant security risks to Wireless Sensor Networks (WSNs), which can result from both cyber and physical attacks. For example, use of fake sensors nodes to inject false data, which cause confusion in the entire network (Sahoo, Sarkar, and Ray, 2019).

Reference List

Bocetta, Sam. (2019) Seven Steps for Improving Cloud Security with Business Integration. *InfoQ*. Available from: https://www.infoq.com/articles/improving-cloud-security/ [Accessed 20 October 2020]

Carroll, Mariana, Van der Merwe, Alta & Kotzé, Paula. (2011). *Secure cloud computing: Benefits, risks and controls*. Available from: https://www.researchgate.net/publication/224259118_Secure_cloud_computing_Benefits_risks_and_controls/citation/download [Accessed 1 November 2020]

Cisco Systems Inc. (2020) *Industrial Automation for Process Control and Refineries*. Available from: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Verticals/Oil_and_Gas/DG/Oil_and_Gas-DG.pdf [Accessed 30 October 2020].

Deloitte. (2020) *Cloud Fluent Helping you thrive in a digital world*. Available from: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/digital-hub/deloitte-cloud-fluency-guide.pdf [Accessed 30 October 2020].

Financial Stability Board (FSB). (2019) *Third-party dependencies in cloud services - Considerations on financial stability implications*. Available from: https://www.fsb.org/wp-content/uploads/P091219-2.pdf [Accessed 30 October 2020].

Gupte, Rohan. (2017) *Recoverable Cloud Data Which Has Been Permanently Deleted*. Available from: https://www.cs.tufts.edu/comp/116/archive/fall2017/rgupte.pdf [Accessed 1 November 2020]

Kaloudi, Nektaria. (2018) *Security and Privacy Issues in Smart City Infrastructure with Emphasis on Mobility*. Available from: https://hellanicus.lib.aegean.gr/bitstream/handle/11610/18252/MSc_Thesis_2018.pdf?sequence=1 [Accessed 1 November 2020]

Mawlood Hussein, S., López Ramos, J. A., & Álvarez Bermejo, J. A. (2020). *Distributed Key Management to Secure IoT Wireless Sensor Networks in Smart-Agro*. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7218854/ [Accessed 1 November 2020]

Radanliev, Petar. et al. (2019). *Cyber Risk Management for the Internet of Things*. Available from: https://www.researchgate.net/publication/332347809_Cyber_Risk_Management_for_the_Internet_of_Things [Accessed 1 November 2020]

Sahoo, R., Sarkar, S. and Ray, S. (2019) 'Defense Against On-Off Attack in Trust Establishment Scheme for Wireless Sensor Network'. *2019 2nd International Conference on Signal Processing and Communication (ICSPC)*, Coimbatore, India, 2019, pp. 153-160.

916 words

Reply

4 replies

1

Post by Laura Rivella

15 days ago

Peer Response - Re: Initial Post - Cloud and Wireless Sensor Networks

Hi Lewle,

I would like to expand on the great points you made about Cloud data security.

John Chambers, the CEO of Cisco Systems, stated in 2009 that cloud computing is a "security nightmare". (McMillan, 2009) He was not wrong. Even though we know more about cloud computing nowadays, security is still a major concern.

In a literature survey on cloud computing, Rao and Selvamani, 2015 found that data security and privacy represent 70% of critical concerns, and that only 2% of respondents considered data segregation and protection not to be important.

All these points are an excellent chance to re-examine a case we touched upon in week 4 and 6 (seminar 2 and 3), namely, the NHS Scotland case.

Our case begged a question: what is the current data storage solution for hospitals?

The trend is moving towards cloud solutions, so much so that the NHS published a guidance on off shoring and use of public cloud services. (NHS, 2018)

If we consider all security threats to a cloud data storage such as data spread (Hoover, 2013), employee/service provider misuse, configuration errors, and increased "attack surface" (Jansen & Grance, 2011) to name a few; why still do it at risk of being held legally responsible for losses of information?

In my experience in the field of healthcare, data has grown exponentially in the last few years. The key challenges of on-premise data storage in healthcare are, for instance, the inability to afford downtimes, very high maintenance costs of power supply, cooling and staff, and space to expand server rooms. So even though an on-premise could be considered a more secure option, there are quite a few drawbacks that help explain the move to the cloud.

A very interesting solution that needs further examination is a hybrid model in which organizations may choose to store more bandwidth intensive data, such as images, on an on-premise server so they can be accessed quickly.

Reference list:

Hoover, N. J. (2013) Compliance in the Ether: Cloud Computing, Data Security and Business Regulation. *Journal of Business & Technology Law* 8(1): 255-273. Available at: https://digitalcommons.law.umaryland.edu/jbtl/vol8/iss1/18

McMillan, R. (April 21, 2009) Cloud Computing a 'Security Nightmare,' Says Cisco CEO. *Computerworld*. Available from: https://www.computerworld.com/article/2523825/cloud-computing-a--security-nightmare---says-cisco-ceo.html [Accessed 6 November 2020].

NHS (2018) Guidance on Off Shoring and Use of Public Cloud Services. Available from: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services-guidance [Accessed 6 November 2020].

Velumadhava, R. & Selvamani, K. (2015) 'Security Challenges and Its Solutions in Cloud Computing', *International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014)*. Interscience Institute of Management and Technology, Bhubaneswar, Odisha, India. Procedia Computer Science 48: 204-209. DOI: 10.1016/j.procs.2015.04.171 Data

Jansen, W. & Grance, T. (2011) *Guidelines on Security and Privacy in Public Cloud Computing*. National Institute of Standards and Technology. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf [Accessed 6 November 2020].

Other sources:

Gov.UK (2017) Guidance on Data Security and Protection for Health and Care Organisations. Available from: https://www.gov.uk/government/publications/data-security-and-protection-for-health-and-care-organisations [Accessed 6 November 2020].

Gov.UK (2014) National Information Board's Personalised Health and Care 2020 Framework. Available from: https://www.gov.uk/government/publications/personalised-health-and-care-2020 [Accessed 6 November 2020].

Svantesson, D. & Clarke, R. (2010) Privacy and Consumer Risks in Cloud Computing. *Computer Law & Security Review* 26(4): 391-397. DOI: 10.1016/j.clsr.2010.05.005

Vurukonda, N. & Rao, T. (2016) A Study on Data Storage Security Issues in Cloud Computing. *Procedia Computer Science* 92: 128-135. DOI: https://doi.org/10.1016/j.procs.2016.07.335

595 words

Reply

2

Post by Keir Coford

Peer Response – Cloud and Wireless Sensor Networks

15 days ago

With the changes in global circumstances it is true that more and more organisations are switching to cloud based computing solutions. It is true, however that many business may be sceptical on switching to a cloud based solution as this will involve the transfer of potentially sensitive and/or crucial data. A survey (Cloud computing – 2020) found that there was wide distrust of cloud computing within the financial sectors with 85% of participants citing distrust. Control of this data is no longer in the hands of the business.

If an organisation finds they have an issue with the online based cloud, they may have to wait for the cloud provider to fix or create a work around for the issue. Or worse, if the cloud becomes inaccessible then the organisation may be unable to operate effectively resulting in major damage for the business. Cloud based computing allows for an organisation to become much more flexible at how they run the business. A businesses employees that utilise physical onsite storage will have to content with the limitation that their data can only be easily accessed from a few key locations. However, cloud computing allows for the data to be accessed from anywhere in the world that has a secure connection. Greatly improving efficiency.

Many different types of organisations rely on wireless sensor networks (WSN) from the operation of the business. These sensors need to working accurately in order to provide the information that the organisation requires. A breach in this network may cut off connection with one or more of the sensors or allow the sensor to submit inaccurate data. This would severely effect the ability of business to process this data and may cause incorrect information to be produced. These WSN's have the disadvantage of being costly to set up and maintaining the sensors and network can incur additional costs. Keeping them secure can also be a challenge as WSN are often established in remote locations, meaning hardware improvements will be time consuming and software updates will require a reliable and constant connection.

Reference

Fstech. *85% of FS workers distrust cloud computing*: https://www.fstech.co.uk/fst/85_Per_Cent_FS_Workers_Distrust_Cloud.php [Accessed 5th November 2020]

370 words

Reply

3

Post by Shiraj Ali

Peer Response - Re: Initial Post - Cloud and Wireless Sensor Networks

13 days ago

Hi Lewle, This topic of Wireless Sensor Network, found it very interesting and made me look into it bit further and here are few facts.

Wireless sensor networks include a large number of tiny sensor nodes, which are densely deployed within or very close to the phenomenon to be detected. Sensor nodes include sensing, data processing and communication components. The location of sensor nodes does not need to be designed or predetermined. Sensors allow random deployment in inaccessible terrain or disaster relief operations. Which also means that sensor network protocols and algorithms must have self-organising functions (Wireless Sensor Networks - an overview | ScienceDirect Topics, 2020).

Another unique feature of sensor networks is the joint efforts of sensor nodes. The sensor node is equipped with a built-in processor. Instead of sending the raw data to the node responsible for fusion, they use their processing power to perform simple calculations locally and transmit only the necessary and partially processed data.

The following lists are some differences between wireless sensor networks and traditional wireless ad hoc networks (Wireless Sensor Networks - an overview | ScienceDirect Topics, 2020).

- The number of sensor nodes in wireless sensor networks can be several orders of magnitude higher than the number of nodes in traditional wireless ad hoc networks.
- In wireless sensor networks, sensor nodes are densely deployed.
- The topology of a wireless sensor network changes very frequently.
- Sensor nodes mainly use the broadcast communication paradigm, while most traditional self-organising networks are based on point-to-point communication.

While designing a WSN, one could consider a few of the point listed below (Zhang, 2014).

- In many applications, sensor nodes are powered by batteries and are limited by energy supply.
- Fault tolerance is required.
- The sensor networks with limited resources (e.g., CPU, storage, energy, wireless bandwidth)
- Self-configuration and reconfiguration
- Low maintenance cost (no maintenance in some applications)
- There needs to be High reliability.
- Also, require High security as they are known to be vulnerable to various attacks.

References:

Sciencedirect.com. 2020. Wireless Sensor Networks - An Overview | Sciencedirect Topics. [online] Available at: https://www.sciencedirect.com/topics/computer-science/wireless-sensor-networks [Accessed 8 November 2020].

Zhang, J., 2014. TNE090 Wireless Sensor Networks Lecture 1. [online] Webstaff.itn.liu.se. Available at: http://webstaff.itn.liu.se/~jinzh29/TNE090/LectureNote4in1/TNE090_Letcure_1_4in1.pdf [Accessed 8 November 2020].

381 words

Reply

4

Post by Lewle Seneviratne

Summary Post - Cloud and Wireless Sensor Networks

9 days ago

Dear all,

Thank you for all your well-researched, great contribution.

Cloud

Significant vulnerability in the Cloud is that everything is shared, and it only requires hackers to pass through the boundaries that Cloud providers established to prevent users from accessing each other's data storages. This is the critical factor where hackers relay upon to make their way into the backend of the Cloud. As highlighted by Keir, there is always a risk when cybersecurity becomes the responsibility of another party, and the risk is magnified, especially in a situation when it involves the use of shared platform with other users with limited access control.

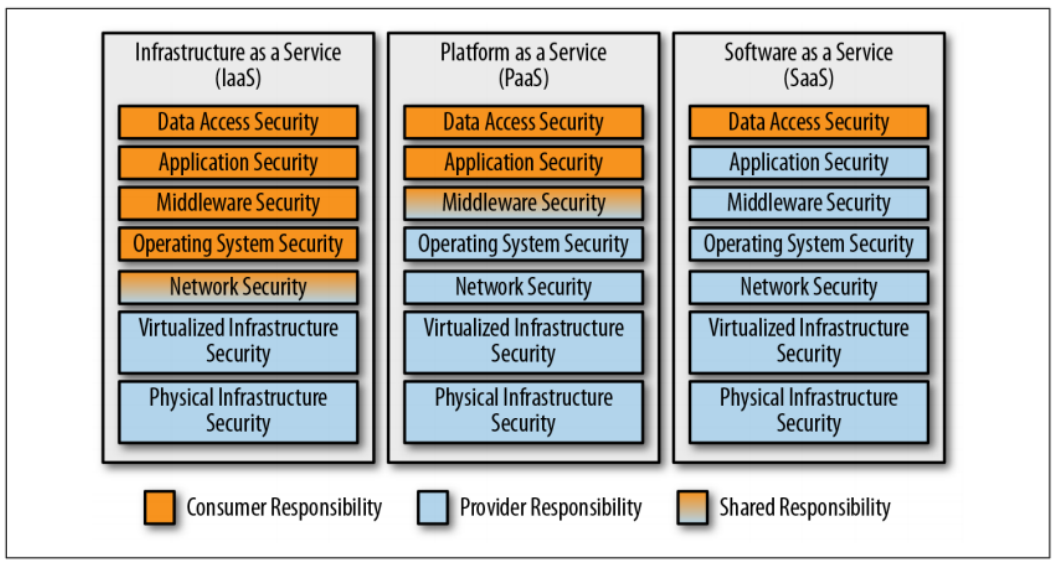

Figure 5-1. Cloud shared responsibility model (Dotson, 2019: 81)

It is equally important to consider the fact that "Cloud" identity has been the target of attacks due to interrelated vulnerabilities. In 2017 Microsoft Security Intelligence Report (Vol 22) it was revealed that '300 percent increase in Microsoft cloud-based user accounts attacked year-over-year Q1-2016 to Q1-2017' (Microsoft, 2017).

Having emphasised the vulnerabilities above, I would like to expand on Laura's question and contribution on why still organisations go for Cloud-based solutions knowing the vulnerabilities?

Cloud's incomparable flexibility, accessibility, and capacity make it one of the fastest growing technologies today. Elaborating some of these benefits, such as overcoming the fear of safeguarding organisation's server room during large- scale disasters such as fires or terrorism; scalability to increase or reduce the required resources as the demand changes; remote access and mobility; it is understandable why organisations are still adapting Cloud.

Wireless Sensor Networks (WSN)

As stated in Shiraj's well-presetned introduction, WSN comprises a mass of rigorously energy constrained multifunctional sensor nodes. As well-explained by Keir, in terms of security requirments, it is crucial to maintain confidentiality; integrity (trustfullness and accuracy); authentication (unwavering quality by distinguishing its root); availability and timeliness of information gathered through these sensor nodes.

A security attack to WSN could impact various infrastructure levels such as data communication layer managing end-to-end connections; network and routeing layer maintains effectively routeing the data from and between nodes; physical layer in charge of frequency setup, data encryption and signal detection or data layer multiplexing data streams and error control (Hari & Singh, 2016).

High vulnerability to numerous security attacks based on its resource constraints and mobility, WSN has surely gained attention equal attention from attackers as well as designers, developers, and security professional regards to security management.

Reference List

Diogenes, Y. & Ozkaya, E. (2018) *Cybersecurity – Attack and Defense Strategies*. 1st ed. Birmingham: Packt Publishing.

Dotson, C. (2019) *Practical Cloud Security*. 1st ed. Sebastopol: O'Relly Media, Inc.

Hari, P. & Singh, S. N. (2016) Security issues in Wireless Sensor Networks: Current research and challenges, *2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring)*, Dehradun: 1-6. DOI: 10.1109/ICACCA.2016.7578876.

Kazza, J. (2014) *Computer Network Security and Cyber Ethics*. 4th ed. North Carolina: McFarland & Company, Inc.

Microsoft (August 17, 2017) Microsoft Security Intelligence Report Volume 22 is now available. Available from: https://www.microsoft.com/security/blog/2017/08/17/microsoft-security-intelligence-report-volume-22-is-now-available/ [Accessed 8 November 2020].

Raza, A., Romman, A. A. & Qureshi, M. F. (2019) Security issues in Wireless Sensor Network Broadcast Authentication, *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*, Amman, Jordan: 1-7. DOI: 10.1109/ICTCS.2019.8923026.

538 words

Reply

Add your reply

Your subject

Type your post

Choose Files No file chosen

Submit

Use advanced editor and additional options

Older discussion
Initial Post

Newer discussion
Initial Post – Data Loss Prevention (DLP) and Network Segmentation