Security in Fog Computing

By: Will Grise &

Matthew Holston

Executive Summary

Fog computing is a next-gen technology that brings the cloud closer to the end user. It does so through the use of fog nodes, which are edge devices such as routers and switches that do most of the processing of data before sending it to the cloud for further processing. This system allows for the cloud to be closer to the user thereby eliminating latency and requiring less broadband to transfer data due to the shorter distance the data must travel to reach the user. This is a major benefit when a company implements a fog network into their network.

Not only does a fog network allow for quicker access to data, it helps to increase the productivity of an organization. It does this by giving an organization the flexibility to change the system to fit their growing needs. However, this does not mean fog computing is without its disadvantages. One such disadvantage is the data processed on the fog node is stored on the device for a rather lengthy amount of time, and if the device is stolen and the credentials to the device cracked could cause the data to be compromised.

Disadvantages such as this are why it is so important for organizations to have security at the forefront when designing these systems. Organizations not only have to worry about the threat of a physical attack but should be aware of attacks that can happen remotely. Thus, organizations should looked to secure the system physically via securing the fog nodes and by getting insurance should a disaster occurs which requires the replacement of the fog nodes. Organizations should also look to secure the system via software controls such as passwords for access and firewalls to prevent unwanted access.

In conclusion, fog computing is part of the next generation of technology that will give organizations increased flexibility in the marketplace, while also providing for faster access to

information for the organizations and its clientele. This is not a one-way street since fog computing still has its own drawbacks. However, most of these disadvantages can have their impact reduced through the organization getting proper security technology and by following a standard security procedure. An organization when using a properly secured fog network is truly on the cutting edge of modern business technology and they will be prepared to face whatever technical challenges face the organization in the future

Introduction

Fog computing is a cutting-edge technology developed by Cisco that uses edge devices, such as routers and switches to do the majority of data processing. This is in contrast to the centralized cloud architecture, which uses a centralized point for the collection and processing of data. Fog computing, according to the Cisco website, is brought to the forefront of computing due to its ability to connect with the Internet of Things (IoT) (Cisco, pp 3). The IoT is the modern-day network where most devices that we use during our daily lives are connected to the internet. This includes devices such as our phones, smartwatches, TVs, and even your refrigerator. Fog computing was created for this environment since it allows for the cloud to essentially be closer to the IoT devices allowing for faster data processing. This happens through the use of fog nodes which are the edge devices positioned so that they can be closer to the end user allowing for faster access to the global cloud network. These fog nodes are sent data from the end user, which is then processed by the fog node and then sent to the cloud for storage and further processing. The data still remains on the fog node for some time after it is sent to the cloud in case the data must be accessed at a later time. This leads into one of the major benefits of fog computing.

Benefits of Fog Computing

The connection to fog nodes is one of the major benefits to fog computing. This is a benefit since it allows for the user to access information in a timely manner, allowing them to do more with less of their time wasted waiting for data to process. This occurs since the fog nodes are so close to the user it reduces the latency to almost nothing and not as much bandwidth is required to move the data since it is on a nearby edge devices (Sakovich, paragraph 31). This allows for much faster data access. Data access is a major issue when it comes to emergency situations. Fog computing helps to relieve this issue since it gives first responders quicker access to items such as medical records for a victim suffering from an allergic reaction to see what they are allergic to.

Another major benefit of fog computing is it can help to increase the productivity of an organization. Fog computing increases productivity since it allows for the organization to setup the system to only detect certain events. This allows for the IT department to be able to correctly triage the situation and respond only to events that are of the utmost importance. This gives the entire TI team the ability to do more work and less time filtering thru data which is likely of no true importance. Fog computing also gives the organization the ability to do business anywhere there is an internet connection since the fog nodes are not limited in number; it allows for a massive network of them giving the business a global reach without the need for massive data centers all over the world.

The third major benefit of cloud computing is the devices allow for more control in terms of privacy. This is true since the fog nodes can be setup to wipe their data every so often preventing a hacker from gain all the data ever on the device. The devices themselves, also hold only a certain amount of data this prevents

Disadvantages of Fog Computing

While fog computing has its benefits, it is not without its downside. The first major disadvantage with fog computing is the sheer number of devices involved. Fog computing does the majority of it computing on devices such as routers and switches. This means that if you need a large number of these devices, it can be very expensive to purchase them all. Another issue with the number of devices involved are the amount of connections in a network. If you are using a widespread fog computing network, if a hacker manages to compromise one of your devices it could mean that all of your devices have been compromised. This is a major security threat which will be covered later on.

Another disadvantage is that most of the data processed will be stored on the local devices (Shoemaker pp.10). This is a disadvantage since if the device is stolen and the security algorithm is hacked, the data stored on the device will be free for the taking if the system is not configured to wipe the data off the device every so often. Not only do the fog nodes need to be secured in a way that prevents unwanted access, the security software must be strong enough to prevent a breach even if the devices are stolen. This is especially important if the devices are holding valuable data such as credit card numbers.

Why Security is important for Fog Computing

Security is defined as the state of being secure (Webster). This very important for fog computing since it prevents the unauthorized access of the fog node, whose compromising could cause the centralized cloud architecture behind the science to be illegally accessed. This could cause the loss of a massive amount of data or worse the data is published on the Internet for everyone to see. This would cause the large organization’s reputation to be tarnished and a large enough attack on a small organization could cause it to go out of business. This is where security comes in to help alleviate the risks involved with the usage of a fog computing architecture. When discussing security in fog computing, it is important to have security in mind when it comes to the operation and installation of the system, the physical security of the hardware the system is comprised of, and the software applications and programs, which allows for the organization to configure the system to its needs as well as to prevent unauthorized usage.

The Operational and Installation Aspects of the Fog Computing Architecture

The first step in the installation of a fog computing system is understanding the needs of the organization and how the organization wants to implement said system. The needs of the organization will vary over time, so the system should not be created to only deal with a current problem but should be thought of as a way to push the organization towards the future, allowing for more growth and more flexibility in the organization's network.

There are two main setups when it comes to the fog network. First, you can put a fog node every where you do business at constantly. This setup is often recommended for smaller organizations or organizations that have a lot of different locations such as franchises. By using this setup, an organization allows all of its employees to be able to access the network at the location they work, and, in the case of payment, allows for the quick usage of credit cards since devices such as pin pads only have to connect with the fog nodes rather than taking more time to send their data the cloud to process transactions. The other major setup for fog computing is the usage of a wide range network. This would be recommended for global corporations whose employees are located all around the world. In this setup, the organization will place a fog node at certain distance intervals, allowing for constant access all over the country or world. This way the organization allows for its employees to access important data at any point in time so long as a fog node is in the nearby vicinity.

Another major issue to consider when implementing a fog network is the cost of such a project. Not only do you have to buy all the software and hardware for the network, but you have to buy extra of all the key components in case of a hardware failure. This is why many organizations try to limit the number of fog nodes to an acceptable level of coverage since instant access is nice, but even having the fog node nearby will still be faster than data going to the cloud and back. One way that organizations can offset some cost is by buying the equipment refurbished or used from another company, but this acquisition strategy could bring the equipment’s reliability into question. Another strategy of acquisition is to negotiate with the manufacture of the routers, switches, etc. and see if they will give the organization a price reduction if they purchase a certain amount of equipment. However, all of this purchased equipment will be wasted if the security given to it is not up to par.

After getting all the equipment purchased and installed for your fog computing network, the greatest threat of all to the system will emerge, the organization’s own employees and the endpoint users. The main reason that the employees of an organization or users of a system are the biggest threat is that they are often tricked into giving out sensitive information by hackers via social engineering. They will send phishing emails that look like the user’s boss telling them they need to sign in to access a document the organization sent to all employees regarding their 401k(s). The user enters in their credentials and without much effort the hacker has access to the system to do whatever they want to do with it. This type of attack is especially effective when dealing in fog computing since there are far more users and the users may not be trained to know how to detect security threats such as phishing emails. Therefore, it is highly recommended that companies of all shapes and sizes conduct training on an annual basis on the subject of the detection of security threats and how to report those threats to management. This will at least decrease the chance of such an attack occurring and may very well be enough to prevent most of these attacks from ever happening. The other reason that employees are a major threat is due to possible mistakes that they can make when using the system. This is why companies should require all employees to undergo job training and if it is possible have multiple employees audit each other’s work before it is allowed to enter the system. This is necessary in fog computing since a mistyped command or incorrect logic could cause the system to crash, costing the company a large sum of money depending on how long the system is down, and the potential damage done to the system.

Physical Security of Fog Nodes

Before placing all of the software to prevent a hacker from accessing the fog node remotely, the organization must first place the correct amount of physical security in place to protect the fog node and the cloud terminal that the fog nodes report to. Physical security is ensuring the safety of the equipment from physical threats such as robbery or flood damage. It is imperative that organizations focus on physical security since not only does the loss of equipment hurt the business, it also will look bad to those who may want to invest in the organization. For if an organization, can't protect its own equipment, how well will they protect my investment? These are the situations organizations find themselves in following attacks that could have been prevented had they followed proper security procedure.

The fog nodes are the first thing an organization should secure physically since without this component the entire system can't function. The location of the fog node is most important factor when it comes to securing it. Fog nodes can be located almost anywhere whether it be in a network cabinet, server room, or on top of a telephone pole. If one were to analyze a restaurant setting, the fog node is often times located in the manager's office away from the rest of the restaurant. This helps to restrict access since customers are not allowed into the back of the restaurant, and the network cabinet will be locked with either a key-based or combination-based mechanical lock. Locking the cabinet prevents unauthorized access from anyone that works near the cabinet such as a malicious employee who intents to steal company information. Another example of securing a fog node is if the fog node is located in a server room or within an office building it is recommended that organizations keep the nodes behind a locked door and, if necessary, have guards patrol the building looking for suspicious activity. There is more need for security in an office setting since the data stored on the nodes will often times contain sensitive information such as financial and customer information. A recommended approach to securing a fog node with an office build is requiring a two-factor lock for entry into the server room and a system for monitoring the technicians once inside the room. This two-factor lock often times requires an authorized employee to scan a keycard and enter in a combination to unlock the door. Once inside the room is monitored with cameras so the technician is under constant monitoring, which discourages any criminal behavior. This system is efficient at discouraging illegal activity but can be expensive to operate.

Cost is a major factor when it comes to physical security in fog computing. It is a fine balance between cost efficiency and security when an organization is determining how to protect its fog nodes. On one hand, you could have state of the art biometric locks and titanium lock boxes protecting your equipment, but if you had thousands of different fog nodes the cost would be substantial. This is not to say that such a protection system is not of great benefit, it may even be necessary in certain situations. For example, within an office building there is a fog node with the financial data of the company's investors on it, that fog node should be more heavily secured than one which contains less sensitive information. This is why companies should do a through analysis of all their fog nodes and determine what type of data is on each fog node, which should help them to determine the level of physical security which a fog node should be given.

Another major factor to consider is the conditions the fog node will be operating in. As previously stated, fog nodes can be placed anywhere and that means they could face some rather harsh conditions. These conditions could damage the equipment, if it is not properly protected.

Some of these conditions are extreme temperature changes, high humidity, storms, snow, and flooding. These conditions are not as difficult to manage if the fog node is located within an office building. This is due to the temperature and humidity being controlled by the HVAC system. The building will also protect the equipment from rain and snow. This is not the case when an organization puts a fog node outdoors. When placing a fog node outdoors, the organization must analyze the conditions of the area and determine what protections to put in place. For example, if the location is know for high winds it would not be a good idea to put the node on top of a telephone pole. Therefore, in this situation placing it on ground level or even underground would be the recommended action.

Lastly, in terms of physical security there are some controls that can be put in place to minimize damage to the system. The first thing a company should do is to make sure they get the system some form of insurance. This will help to recover the system following a disaster which requires the organization to replace most if not all of the equipment. Another control that should be put into place is to lock down the ports going into the fog nodes. There is no reason for all of the ports on the fog nodes or for exterior ethernet ports, if the fog node is within a building to allow for access. It is highly recommended that organizations take the time to ensure the only way to access the fog node is remotely or thru an authorized technician connecting to the device directly. Its is possible to simply lock the fog node up in a network cabinet or in another secure location, but one of the best ways to protect the fog node is via the software installed to defend against various attacks launched by hackers

Software Security in Fog Computing

Software security is the idea to protect software against attacks that might breach the information of the intended user/users it was meant to protect. Software security's main pillars are access control, integrity, data confidentiality, and privacy. Any compromise to these pillars will make the software unsecure. An effective security software should be able to adapt to new and improved types of malicious attacks. Every day hackers with either good or bad intentions are attempting to gain access to vital information of unaware users (What is Software Security?).

Access control is a security technique that monitors and coordinates who or what can view the information within the software. Access control minimizes risks to the business or organization that holds that software. There are two steps in access control, the physical and the logical. In short, the physical security controls access to buildings, rooms, IT assets, and more. Logical security limits the connections to the nonphysical – computer networks, system files, and data.

Access control systems identify the authenticity and authorization of users by assessing the required login credentials; including passwords, personal identification numbers (PINs), security tokens, or other authentication factors. There's also multifactor authentication, which requires a two-step process to gain entry to a place or online information. The multifactor authentication plays an important role in layered defense of information to protect access control systems. These security controls work to identify an individual or entity and verifying that the person or entity is who is claims to be, while simultaneously authorizing the access levels and allows a set of actions to be performed by that person or application. There are different types of access control that change depending on an organization's requirements and the security levels of information technology they are trying to protect (What is access control?).

Integrity involves that the data being sent and received is real, accurate, and is still in its original form with no alterations, when it's received. One component to ensure that this stays true is to incorporate either a one key or two key system. This can also be referred to as a token rather than a key. This method is secure way to send and receive important documents or information to another user. This causes problems for potential hackers because the only way to access the information is by having the correct and corresponding keys/tokens. This type of security can also be known as encryption. The data is encrypted once it has been sent and the keys are used to decrypt the information.

Data confidentiality is centered around the data and is protected from any unauthorized parties. Confidentiality can be referenced to the main reason why security is implemented in the first place. Confidentiality could be seen as the most important aspect of the whole system. If the confidentiality is breached, then that means someone who is unauthorized has gained access to the information. With many of these breaches of information, you may not know that there was even a breach. The only way you really get an alert is if your information has been made public. At that point, it’s too late to completely cover-up what has been released. The type of information that could be made public can range from bank account numbers, home addresses, cell or home phone numbers, emails, or even social security numbers. Some of these examples are a lot easier to handle than others. But by ensuring that the data confidentiality aspect isn’t breached might be a better option.

Data Privacy

One software that’s being utilized in the real world to ensure security and privacy is called Cisco IOx. This application combines Cisco IOS and the Linux OS, for a highly secure network. When examining potential software that will ensure safety and privacy there are three main categories to consider: data privacy, usage privacy, and location privacy. Location privacy can only be accomplished if the identity masking remains covered such that even though the fog node knows a fog client is nearby, it cannot identity the fog client. Vehicular Networks (VN) fall under the location privacy category. When using a vehicles GPS system, you are essentially logging your exact location at all times when using your car. Vehicular networks must be secure enough so that unauthorized access would not occur at any given moment. If there was a breach in this information, the hacker if they had bad intentions, would have access to your most common routes you take, your home address, where you work, and your most frequent visited locations. This could be viewed as having a constant GPS on someone (Security and Privacy Issues of Fog Computing Page 7*)*.

Data privacy is another essential aspect to the security world. Data privacy in fog computing involves privacy-preserving algorithms that help your data be secured. This is the aspect of security where all your data is secured without any breaches. With social media having such a strong presence today, this could be viewed as being the most crucial security aspect of the three categories of privacy. Users might not identify this, but there is much more to social media than they originally believe. How many times do the users not think before hitting the Enter/Submit button? An example that I want to mention has to do with Facebook specifically. Facebook has the ability to tag where your exact location is for any social outing. This is almost too easy for anyone looking to find your location. If this venue is somewhere the user goes to regularly, then anyone looking to do harm or maybe just watch that specific person, is almost free to do so without much effort. That’s a scary aspect today that many people don’t realize. We’re so inclined to broadcast to the world what we’re doing that there really is no privacy.

Two other important aspects in data privacy are financial privacy and medical privacy. Both of which contain very important and significant information. Information that, if it was confiscated, could have a significant negative impact someone’s life. A hacker could have access to all your financial records and possibly have access to your financial accounts. Fraud is looked at by users as something of fantasy. If you're not constantly monitoring your accounts, then you may never know that your information has been breached. They could potentially only use your information for small purchases that may never get flagged (Data Privacy).

Your medical privacy is information that is taken very seriously. There's a reason why there's the doctor to patient confidentiality, it is implemented in all medical facilities. With your information being online, there's potential that it could be breached. Information such as medical treatments, potential medical conditions that you might have, or even more sensitive information such as your social security number. Keeping this information safe and secured should be a top priority with software security.

Usage privacy involves a complex system in which a fog client creates dummy tasks which are then offloaded to multiple fog nodes. By doing this, you are able to hide the real tasks among the dummy nodes. Usage privacy can be viewed as a user transmitting when and what they are doing at any moment. If their usage privacy is breached, a hacker could monitor what a user is working on or what sensitive information their entering.

Conclusion

Fog computing has a great deal of benefits that can significantly impact a company or a simple user in a positive way. With great reward also comes great responsibility. Having strong security will benefit the user and business in the long-run. Don't cut corners in ensuring that your information is secured. You may never know if your information has been breached but by taking safe precautions, you can minimize the chance of any unauthorized users gaining access to your data. Having privacy is essential not only in real life but even more when you're on the internet. There is much more sensitive information that is able to be obtained online. Fog computing is a wonderful addition to the technology world, but there must be strong security implemented before it should be operated to its fullest capability.

References

Cisco. (n.d.). Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. Retrieved June 25, 2019, from Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are

Data Privacy - Definition & Types of Data. (n.d.). Retrieved from https://www.cleverism.com/lexicon/data-privacy/

Sakovich, N. (2018, September 10). Fog Computing vs. Cloud Computing. What are the Key Differences? Retrieved June 25, 2019, from https://www.sam-solutions.com/blog/fog-computing-vs-cloud-computing-for-iot-projects/

Security and Privacy Issues of Fog Computing: A Survey [Scholarly project]. (n.d.). Retrieved from http://www.cs.wm.edu/~liqun/paper/wasa15-fog.pdf

Security. (n.d.). Retrieved from https://www.merriam-webster.com/dictionary/security

Shoemaker, C. H. (n.d.). Fog Computing: What Is It, and What Are Its Advantages and Disadvantages? Retrieved from https://it.toolbox.com/blogs/carmashoemaker/fog-computing-what-is-it-and-what-are-its-advantages-and-disadvantages-010819

What is access control? - Definition from WhatIs.com. (n.d.). Retrieved from https://searchsecurity.techtarget.com/definition/access-control

What is Software Security? - Definition from Techopedia. (n.d.). Retrieved June 30, 2019, from https://www.techopedia.com/definition/24866/software-security