LITERATURE REVIEW

Academic Year 2019-2020 / Even Semester (20192)

Subject : Digital Literacy
Student : Ahmad Hudori
Study Program : MM-Tech

Technology SD-WAN For Internet of Things (IoT)

Ahmad Hudori
MMTech Student of President University

Abstract

A software-defined wide-area network (SD-WAN), is a network that is abstracted from its hardware, creating a virtualized network overlay. Operators can remotely manage and quickly scale this overlay, which can span over large geographical distances. It is an application of software-defined networking (SDN). SD-WAN can connect several branch locations to a central hub office or cover multiple locations in a large campus such as a university campus. SD-WAN simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism. This concept is similar to how software-defined networking implements virtualization technology to improve data center management and operation. A key application of SD-WAN is to allow companies to build higher-performance WANs using lower-cost and commercially available Internet access, enabling businesses to partially or wholly replace more expensive private WAN connection technologies such as MPLS. The Internet of Things (IoT) shall be able to incorporate transparently and seamlessly a large number of different and heterogeneous end systems, while providing open access to selected subsets of data for the development of a plethora of digital services. Building a general architecture for the IoT is hence a very complex task, mainly because of the extremely large variety of devices, link layer technologies, and services that may be involved in such a system. Many IT organizations have found implementing and integrating IoT systems challenging due to network complexity, visibility issues and potential security breaches. Moreover, IoT has high requirements for availability and accessibility of real-time data. SD-WAN encompasses several important features that enable IoT growth. The Internet of Things and advanced robotics, industrial biotechnology, 3D printing, new materials and nanotechnology. Some of these technologies are already used in production, while others will be available in the near future. All are developing rapidly. As these technologies transform the production and the distribution of goods and services. SD-WAN's segmentation capabilities enable the separation of private data from IoT traffic.

Keyword: SD-WAN, Internet of Things (IoT), MPLS

A. Introduction

SD WAN is As networks have grown, they have become increasingly complex, especially to manage. SD-WAN is an important step in the evolution of networking as it helps simplify WAN management. A WAN connects your office to your other locations, and the wider world via the Internet. So essentially without a WAN your office wouldn't be able to connect to do business. SD-WAN or software defined Wide Area Network, uses software to manage and make your network connections work smarter and faster, which helps improve resiliency.

It provides a better way to build networks by monitoring connectivity to manage traffic. As we continue to move more and more data and applications to the cloud, one connection is no longer viable to provide the up time & performance levels required. SD-WAN provides the ability to decide what traffic is connected to what network, so you can better prioritise data such as voice. (Dixon & Mather, 1981)

SD-WAN uses software and cloud-based technologies to sim- plify delivery of WAN services to branch offices. Software- based virtualization enables network abstraction that results in simplification of network operations. SD-WAN enables IT and business managers to deploy Internet-based connectivity (with its benefits of ubiquity, high bandwidth and low cost) easily, quickly and with quality, reliability and security. (Uppal et al., 2015)

The evolution of IT technologies has altered traffic flows within distributed organizations. Not only do remote users require significantly more bandwidth (for example, when using video), but they also need to directly access SaaS/cloud- based applications such as Saleforce, Office 365, Lync and off-premise storage (such as Dropbox, Evernote, and so on).

Traditional MPLS networks which transmit all traffic from the branch to a centralized data center can't offer low latency/ high performance access to cloud applications. In addition, the security and management requirements associated with disparate traffic flows have added to the complexity of manag- ing branch operations – thus increasing operational (staffing) costs for many IT organizations. (Uppal et al., 2015)

In general, operating systems used in SD-WAN nodes (edge router, controller, orchestrator, etc.) are built on general-purpose GNU/Linux distributions like Ubuntu, Debian, CentOS as well as other network software products. In this regard, one of the most important question is existence of zero-day and known vulnerabilities in the kernel of the operating system

and in other its software modules. It was shown [9] that many of the SD-WAN products leak information related software versions (e.g., operating system, kernel, build versions). (Gordeychik & Kolegov, 2018)

CLI is used remotely and locally to interact with SD-WAN services. Most of them, as we have already known, employ GNU/Linux as a basic operating system thereby inheriting the general management mechanisms and tools like Telnet, SSH, command shells, and so on. In the most cases, restricted shell is used as a command shell. That shell limits user abilities and only allows to perform a specified subset of system commands or a subset of high-level commands. Another approach is to provide a special restricted account. These approaches are traditionally considered as a common best practice, but their implementations often contain the following weaknesses:

- Hardcoded accounts and passwords
- Weak default passwords
- A use of a special unlimited system user account that is able to access an operating system command shell directly
- Permissive sudo configuration
- Incorrect access control configuration
- Vulnerabilities in GNU/Linux components (local privilege escalation)
- Vulnerabilities in restricted shells The examples are as follows:
- "_spsshell" command in Silver Peak allowing to access BASH shell directly [21]
- " CBVWSSH " user account in Citrix NetScaler SD-WAN used by design to access debugging facilities
- "admin" user account with predefined password in Cisco (Viptela) SD-WAN A use of SSH and Telnet protocols for remote management causes well-known threats.

At the same time, it was found that some SD-WAN products additionally employ web-based tools like "AjaxTerm" and "Shell in a Box". This extends an attack surface over web technologies and could allow an attacker to commit traditional Web attacks like DNS Rebinding, XSS, CSRF, Command Injection, and so on. Also, there are vendors (e.g., Viprinet) which use cleartext HTTP protocol without SSL/TLS. (Gordeychik & Kolegov, 2018)

1. SD-WAN Benefits

In contrast, SD-WAN provides a wide range of benefits for distributed organizations, including:

✓Business agility. Rapid deployment of WAN services (such as bandwidth and firewall) to distributed branch operations without the need to send IT personnel on-site. Bandwidth can be easily added (with additional circuits) or reduced as business requirements evolve.

✓Internet economics. Internet connectivity (including cable, DSL and ethernet) is widely available, quick to deploy and a fraction of the cost of equivalent MPLS circuits. SD-WAN provides the benefits of reliable, secure WAN service at Internet price points.

✓Optimized cloud architecture. SD-WAN eliminates the backhaul penalties of traditional MPLS networks and l everages the Internet to provide secure, high- performance connections from the branch to cloud. With SD-WAN, remote users will see significant improvements in their experience when using the cloud/SaaS-based applications.

2. Highlighting SD-WAN Buying Considerations

If you're an IT or business manager, consider the following criteria when evaluating SD-WAN deployments:

✓Ease of adoption and management. A key benefit of SD-WAN is that it makes deploying WAN services at the branch fast and simple. SD-WAN solutions must be straightforward to deploy, and they leverage centralized provisioning to eliminate the need for trained personnel to visit remote sites.

✓Ability to migrate to hybrid WAN. The majority of distributed organizations already have MPLS deployed to the branch offices. Organizations should be able to seamlessly deploy SD-WAN solutions (Internet circuits) without changing the existing MPLS network. Those orga- nizations can, over time, migrate traffic growth toward cost-effective Internet bandwidth.

✓Automation – traffic steering. SD-WAN gives organiza- tions the ability to prioritize traffic. The key is providing managers with easy-to-use tools for setting priorities and with features that automatically changes traffic flows according to current network conditions.

The increased deployment of cloud, SaaS, video and mobile applications has challenged IT and business managers to pro- vide high-quality WAN services to the branch. Deploying and managing the WAN has become more challenging and costly as traffic flows decentralize.

SD-WAN offers compelling advantages for distributed organi- zations with critical branch operations, including the benefits of business agility, improved application performance and lower costs of bandwidth. Distributed organizations should consider SD-WAN solutions on the basis of their ease of use and management, ability to integrate with their existing MPLS network and the intelligence to automatically adjust traffic flows to current network conditions.

Software-Defined WAN (SD-WAN) is the extension of SDN that is transforming the enterprise branch office. With SD-WAN, no longer are the advantages of SDN limited to the data center. SD-WAN abstracts network hardware into a control plane and multiple data planes that can be used with cloud-based man- agement and automation to simplify the delivery of services to the branch office. This work is all done with the manage- ability, performance and reliability assurances that enter- prises expect.

SD-WAN is in the spotlight and is gaining popularity in the IT world. With any new disruptive technology, existing incum- bents and many adjacent solution providers go into a frenzy to gain a piece of the market. This activity is part of the IT hype cycle. However, vendors who provide solutions with real, measurable benefits often emerge as industry leaders and go on to define the technology space.

Businesses and their IT teams face three major challenges:

✓ Increased access cost for MPLS-based bandwidth to support application performance

✓ High complexity in branch deployments

✓ Architectural issues with traditional WAN that is both static and private, inhibiting the migration to dynamic and public cloud environments.

3. Analyzing SD-WAN Architecture

The SD-WAN architecture has these three layers (from bottom to top), which you can see in Fig 1:

✓ Secure cloud network

✓ Virtual services delivery

✓ Orchestration and analytics

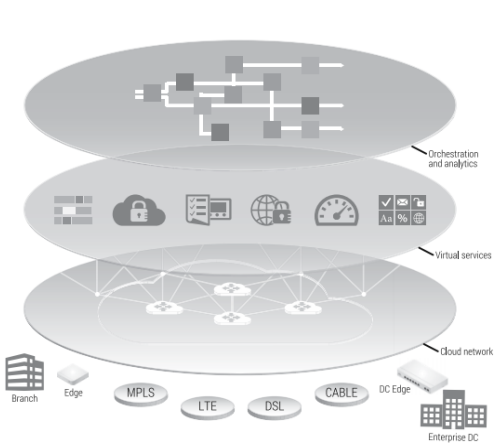

Figure 1: SD-WAN Archtechture

Address the issues with traditional *WAN* is a traditional *WAN* delivers security and performance across private links to applications that reside on a customer data center, an arrangement that has two issues:

✓Traditional WAN ties a customer to a private circuit for enterprise grade security and performance. In this s cenario, the customer loses the flexibility of transport independence.

✓Backhauled SaaS applications experience performance penalties because of the traditional WAN.

Internet of things (IoT) technology is getting adopted rapidly. Number of IoT enabled devices is increasing and it is predicted to reach about 25 billion by 2021. These devices produce immense volume of data. Generally, device data is sent over cloud for further processing, this demands high bandwidth and high computational resources at the cloud end. Edge and fog computing are evolving as complementary processing architectures to eliminate these shortcomings.

Blockchain technology initiated as decentralized electronic cash system. It gradually evolved to support smart digital contract and platform for developing decentralized application. This paper proposes using blockchain based architecture for developing decentralized IoT edge processing. The paper is structured as follows. Section 2 explains the basic concepts of edge computing and blockchain. (Mendki, 2019)

B. Literature Review

The Internet of Things (IoT) is a network of physical devices and software components that are connected together in order to exchange information and to fulfil an IoT service. IoT applications are supposed to empower interconnected objects in order to build powerful and added-value services.

The hardware devices used for building IoT applications are al- ready available, but there are only a few management systems that support the design, deployment and maintenance of such applications. These tasks are particularly ambitious due to the specificities of IoT applications that are by nature highly distributed, heterogeneous and dynamic. Indeed, IoT applications induce a high level of concurrency, distribution, and collaboration.

Designing concurrent applications is by nature a difficult and error-prone task. Moreover, IoT applications have to deal with heterogeneous IoT hardware and communication layers. Therefore, there is a need for a common model for specifying all objects and the way they interact altogether.

Last but not least, modern systems are no longer designed and implemented once-for-all, but they may evolve over time, which requires simple techniques for updating and changing those applications. In this paper, we present the IoT Composer tool, which sup- ports all the steps of the design, composition, and deployment of an IoT application by selecting, configuring and binding available objects. (Krishna et al., 2019)

Just over three decades ago, Microsoft's Windows 3.0 was hailed as a remarkable achievement. As an operating system capable of running on the 8086 processor, it had the capability of operating on just 384KB of memory. It amazed people with its intuitive graphical user interface and multitasking abilities.

Now, if we fast forward to the current day, we can observe that we are surrounded by the Internet of Things (IoT) devices and systems which are operating on minuscule memory but capable of performing far more complex calculations than Windows 3.0 did in the 90's. IoT has created a massive network of linked devices which are constantly communicating with millions of other Internet con- nected "Objects".

This massive growth within the IoT industry has had enormous positive effects on the population and IoT is playing a key role in bringing man even closer to technology. Whereas in commercial sector, one of the positives of this technology is its abil- ity to provide partial support for Industry 4.0, automation, efficient data acquisition, lower production and maintenance costs,

among many others. It is safe to say that the rapid and widespread uptake and adoption of IoT has left many researchers, academics and the market expert's surprised. (Saleem & Ande, n.d.)

The first railroads had a few miles of track, with trains that were not much faster than a horse. At its height, more than a century later, a vast rail network covered the United States with complex locomotives moving at speeds that trains or cars today cannot match. When it comes to networks of computing devices, we are still closer to the horse than the 20th Century Limited express train, but like trains, rapid, incremental improvements are propelling us into a new environment of social and economic transition.

Computers are not trains. They appear to think and to make decisions. This is largely an illusion, although an understandable one given the speed at which machines execute their programs. The computing devices we have today are not truly autonomous, but the fear of autonomous devices (think "Skynet," the self-aware intelligence that challenged humans in the "Terminator" films) lies at the edge of a discussion of the Internet of Things, a fear that the future may see interconnected "thinking" machines challenge or replace their human masters.

The fear that machines create new dangers or will replace humans began with the industrial age and remains both powerful and powerfully wrong. The Internet of Things is only the latest tool that expands human performance, the latest phase in the automation of routine activities that dates back to the start of the industrialization, but it has been greeted with similar fears.

The devices that will make up the Internet of Things usually have an IP address, onboard computing power, some kind of sensing device that lets them sense their environment, and most have network connectivity (often wireless). A device can be anything from a consumer product to a giant industrial machine. IoT devices will run software programs that let the device "decide" when to take a specified action or to select among different actions. IoT devices may have vulnerabilities not present in a non-IoT device.

IoT will automate many routine activities, allowing machines to make decisions without human interaction. Autonomous devices will control inventory, authorize commercial transactions over the Internet, and arrange for shipping and delivery without human intervention. Interactions will be rapid and automatic, executed according to a series of preprogrammed rules whose composition and nature may not be accessible to the user. (Lewis, 2016)

1. A Short History of the Future: Enabling Platforms Already

Already in the 80-ies have we seen the need for such ‘separation of concerns’ approach in the electronics industry, although predominantly in the technology area. Socio economic considerations were lagging, as usual. In the 80-ies the electronics industry was predominantly analog and the design, manufacturing & application required (scarce) deep and wide knowledge. Chip application engineers, designers and technologists were very much from the same origin and closely working together. But once IC technology was mastered, one could massively apply transistors as switches and a digital technology platform was established.

While one breed of engineers worried about making a good transistor switch and replicating them hundred thousand times without flaw, a new generation of engineers that never had seen a transistor was enabled with tools to create complex computing circuits with those large numbers of transistors, not requiring deep transistor and technology knowledge but using instead simulation models (‘digital twins’). Separation of concerns.

Integrated Circuit Designers started using standard building blocks and those building blocks were combined in standard IC’s such as, microprocessors, microcon- trollers and communication chips. Again establishing a digital platform enabling a new breed of engineers to run away with them building programmable computers, com- munication networks and automation and control systems. (Smuts et al., 2019)

2. Issues Driving The Standards Discussion In The Iot Industry

IoT is knownto be marred with issues of reliability and security. The whole IoT industry is facing enormous challenges, which are growing in severity as its adoption increases and evolves. Vulnera- bilities across IoT devices provide easy access to attackers, leading to further malicious attacks, data theft, destruction of data, damage to the hardware. Furthermore, “pwned” devices facilitates large- scale coordinated attacks on IT infrastructure, the impact of which is can be felt across geographic boundaries by victims [9]. Some of the major issues affecting IoT. (Saleem & Ande, n.d.)

Offerings of IoT Platforms and Services An offering represents data or functions offered by its provider, i.e., IoT platforms, things, or services. An offering is defined by an offering description that can be registered by the provider on an IoT marketplace. The marketplace is used by consumers (e.g., applications) to discover offerings and possibly pay

for the access. An offering description shall contain a syntactic and semantic description of resources provided to a consumer, once the offering is accessed.

This includes information about the syntactic data types needed as input to access the offering as well as the description of the output data received when accessing the resources. Besides the syntactic definition, it is important to include semantic types of inputs and outputs. Furthermore, the offering description needs to entail meta information and Non-Functional Properties (NFPs) about the offering, such as the spatial extent (e.g., a city or region) where the resources relate to, price for accessing the resources, or license of the provided data. (Thuluva et al., 2017)

3. Security

IoT frameworks need to accommodate security by ensuring endpoint nodes and their physical equivalents (i.e., device, process, virtual machine, enclave) have a secured identity, protected cryptographic keys and appropriately provisioned roles, credentials, and access policies. Endpoint security capabilities should protect sensitive data that is stored, transmitted, or manipulated locally outside of the IoT framework.

Software and firmware should be protected when transmitted, installed, stored, and loaded for execution. Framework processing of encrypted data, access control decisions, and identities should be protected within an appropriately hardened Trusted Execution Environment (TEE) or isolated from non-framework aware services and interfaces. IoT device roots of trust should be used to protect device identities and ensure the appropriate firmware and software is loaded and executed. (Cheruvu et al., 2020)

While providing services, IoT nodes in the fog environment are also facing with more security challenges. For example, when IoT nodes provide malicious information, it may affect other objectives so that attackers may have more opportunities to using sensors to interfere with other nodes. From the setting and state information, attackers may understand and predict user behavior and abuse data.

In order to deal with security problems of the fog environment in IoT, we consider starting from the guarantee of data source trustworthiness, combining Blockchain and TEE technologies to design a security scheme for the IoT fog environment exhibited in Fig.2. Based on the recognition of identities of fog nodes, the goal is to ensure the information

stored in fog nodes will not be modified. Meanwhile, under the premise of ensuring information security in the local fog environments, the trustworthiness of data in the entire fog environment is realized. (Fan et al., 2019)

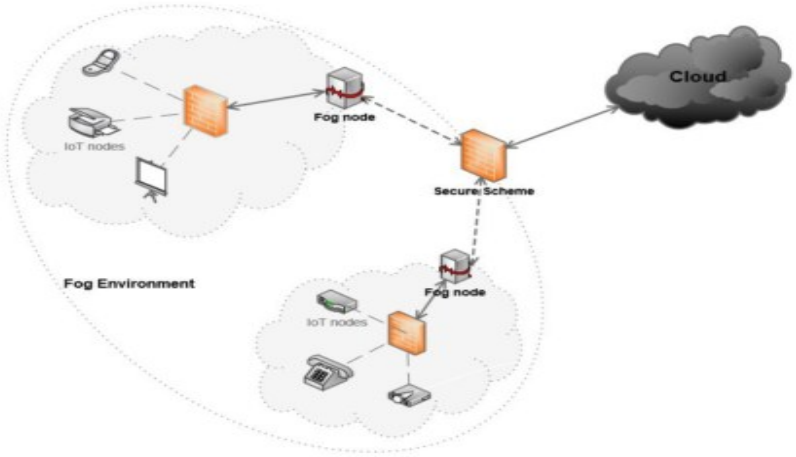

Figure 2: The overview of the application scenario

C. Usecase

Usecase Edge level video analytics usecase is selected for implementing the above solution. Surveillance cameras are getting used widely for the security reasons. The volume of video data produced by these cameras is huge. Global data generated by surveillance cameras is about 560 petabytes per day.

This makes them a good candidate for deploying edge-based analytics solution. One of the possible usecases is to analyze the content of videos and storing that as searchable indexed repository for the video content. A simplified version of this usecase is detecting different objects present in video frames using deep learning image classification techniques. This processing will be executed over worker nodes provided by resource lenders.

CCTV camera is connected to Raspberry Pi using camera module. Raspberry Pi acts as a client/requester that captures the video frames and constructs a batch for processing. Detecting objects in a set of captured images is a job. Hyperledger Sawtooth is used for setting up the blockchain network in this setup. This framework doesn't support ARM architecture, but it provides REST based APIs that can be consumed from Raspberry Pi. Because of this limitation, the current implementation does not include Raspberry Pi as a node on the blockchain network.

There are four types of actors in the application; requester, validator, resource lender and worker node. Requester is a Raspberry Pi device. Hyperledger Sawtooth node constitutes these two primary components; REST based APIs and transaction processors. REST APIs are used to interact with blockchain whereas transaction processors are used to validate the submitted transactions as per the business rules. Resource lender and worker node are Ubuntu server 16.04 based virtual machines. IFPS is setup on Ubuntu server 16.04 virtual machine

D. Conclusion & Future Work

We have taken an integral perspective on the development of IoT, beyond technology and clearly the Internet of Things holds many promises. But just as much as the promises, the development of IoT has many challenges requiring a new approach involving:

- Creating platforms by a strong collaborative approach beyond technology;
- Socio-economic aspects in a Human Centric IoT;
- The education and involvement of end-users;
- Privacy, security, resilience… and many more non-functional aspects;
- Critical architectural choices;
- Real scale experimentation.

Those elements and technical elements should be addressed in an integrated approach, on the one hand leveraging specialist companies and individuals, separating concerns, but linking them in an overall approach. The Alliance for Internet of Things Innovation promotes and drives such approach.

Interesting and responsible opportunities emerge for IT professionals, playing key roles in architecture and platform integration and in linking application domain spe- cialists and end-users. Edge and fog computing have been evolving as complimentary architecture to the central cloud processing and can offload the ever-increasing scaling demands.

Likewise blockchain based resource pooling solution can help edge and fog architecture to address their scaling needs. Using the proposed blockchain based solution for IoT edge can lead towards building the crowdsourced public infrastructure for IoT edge. Ongoing research in the areas like verifiable computation would strengthen the possibility of adoption of similar solutions.

Referencess

Cheruvu, S., Kumar, A., Smith, N., & Wheeler, D. M. (2020). Demystifying Internet of Things Security. In *Demystifying Internet of Things Security*. https://doi.org/10.1007/978-1-4842-2896-8

Dixon, A. M., & Mather, S. J. (1981). What is it and how does it work? *Anaesthesia*, *36*(2), 230–231. https://doi.org/10.1111/j.1365-2044.1981.tb08760.x

Fan, Y., Zhao, G., Sun, X., Wang, J., Lei, X., Xia, F., & Peng, C. (2019). *A Security Scheme for Fog Computing Environment of IoT*. 58–59. https://doi.org/10.1145/3338507.3358621

Gordeychik, S., & Kolegov, D. (2018). SD-WAN Threat Landscape. *arXiv Preprint arXiv:1811.04583*, *Journal Article*.

Krishna, A., Le Pallec, M., Mateescu, R., Noirie, L., & Salaun, G. (2019). IoT composer: Composition and deployment of IoT applications. *Proceedings - 2019 IEEE/ACM 41st International Conference on Software Engineering: Companion, ICSE-Companion 2019*, 19–22. https://doi.org/10.1109/ICSE-Companion.2019.00028

Lewis, J. A. (2016). *Managing Risk for the internet of things. A report of the CSIS strategic technologies program. May 2020*, 1–32. www.csis.org

Mendki, P. (2019). Blockchain enabled IoT edge computing. *ACM International Conference Proceeding Series*, *Part F1481*, 66–69. https://doi.org/10.1145/3320/15433/20166

Saleem, J., & Ande, R. (n.d.). *IoT Standardisation - Challenges , Perspectives and Solution*.

Smuts, M., Scholtz, B., & Wesson, J. (2019). *Issues in Implementing a Data Integration Platform for Electric Vehicles Using the Internet of Things BT - Internet of Things. Information Processing in an Increasingly Connected World*. https://link.springer.com/chapter/10.1007/978-3-030-15651-0_14

Thuluva, A. S., Bröring, A., Medagoda, G. P., Don, H., Anicic, D., & Seeger, J. (2017). Recipes for IoT applications. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3131542.3131553

Uppal, B. S., Woo, S., & Pitt, D. (2015). *Sofware-Defined WAN for dummies*. 61.