SDN: A New Approach for Secured Distributed Networking

Puneet S, Krishna Reddy S, Veeranna K, Nazimunisa
Sree Dattha Institute of Engineering & Science, Hyderabad, India.

Abstract – Computer networks typically interconnect hosts using network switches and routers which provide data packet forwarding and routing functionality. Switches transfer data among nodes on the same local area network (LAN) segment, whereas routers function as gateways enabling the routing of packets between hosts in different networks. These forwarding devices usually run proprietary operating systems and vendor specific protocols that have to be configured through a process in which network operators translate high-level network policies into device specific low level commands, and often manually input these commands using command line or graphical user interfaces. Script sand tools significantly reduce the operational work load and errors in the configuration process, but this approach still requires network administrations to reason carefully about the network, and find the right balance between the use of automation, the situation requirements, and the changing state of the network. The lack of unified network control makes network management challenging, and the pain staking error- prone configuration process is the leading cause of network faults, bugs, and security lapses, Furthermore, due to this in flexibility, net-work innovation has essentially stagnated, contributing to what some term the Internet ossification phenomenon. The recently emergent Software Defined Networking (SDN) paradigm addresses this challenge by separating the packet forwarding functionality of the forwarding devices, known as the data plane, from the control element, known as the con troll plane.

Index Terms – Network security, SDN, virtualization, enterprise networks.

1. INTRODUCTION

Computer networks are typically built from a large number of network devices such as routers, switches and numerous types of middleboxes (i.e., devices that manipulate traffic for purposes other than packet forwarding, such as a firewall) with many complex protocols implemented on them. Network operators are responsible for configuring policies to respond to a wide range of network events and applications. They have to manually transform these high level-policies into low-level configuration commands while adapting to changing network conditions. And often they need to accomplish these very complex tasks with access to very limited tools. As a result, network management and performance tuning is quite challenging and thus error-prone.

In the current scenario of networks, proprietary routers and switches firmware tells the network device where and how to forward the packets. Each network device (switch/router) has its own applications (routing protocols-OSPF, IS-IS), Network operating system and packet forwarding hardware make decisions solely on local logic as shown in fig 1. The switch task is sent every packet to the destination along the same path and treats all the packets the exact same way.

The current networks were built on the notion of Autonomous Systems (AS). This notion allows networks to scale and extend by connecting junctions that forward packets to a next hop based on information learned from the network and interconnection [9]. This process is easy and has proven sustainable, flexible and scalable for data networks. But the downside of current scenarios is AS principle does not allow the any designated destinations to move without changing their identity. This architecture relies on a treelike structure of Ethernet switches and routers. Initially VLAN technology confined to design network segment where virtual LAN controllers can change or add workstations, manage load balancing and bandwidth allocation without involving physical movement of nodes like conventional LANs. These standards on the other hand, have increased complexity in network element specifications and configuration of network interfaces by network operators. Thus such flexibility does not come without cost.

The current network is designed on specialize operating system, hardware and application which are designed by a particular vendor, which is closed propriety, vertically integrated and relatively slow innovation[8]. But SDN designed with open interface where everybody (network admin, security manager) able to use it and publish it, which introduce a system with horizontally integrated, open interface and rapid innovation. SDN also provides backward compatibility with Ethernet, IPV4, MPLS, and VLAN and construct a new and easy mechanism for forwarding with technology independent of switches and routers [10].

2. OBJECTIVE

The Scope of the project is Enterprises today face a barrage fever evolving security threats, and have little choice buttorely on a combination of security solutions that are complicated, distributed, and limited in scope security policies are typically implemented as complex, topology dependent access control lists. Trust is distributed across multiple components, such as switches, Domain Name System (DNS) servers, and

authentication services and Remote authentication Dial in user Service and each of these individual components need to be protected in turn.

In the existing system, task of document summarization aims to generate a very short summary for a given document or document set. Various methods have been proposed for document summarization, including rule-based methods graph-based methods learning-based methods ILP-based methods etc and not covered not so efficient if there is heavy interaction between branches and Data should be carefully maintained.

3. LITERATURE SURVEY

Aaron Gember, Christopher Dragga, ECOS: Leveraging Software-Defined Networks to Support Mobile Application Offloading in 2012, In this paper, Offloading has emerged as a promising idea to allow resource-constrained mobile devices to access intensive applications, without performance or energy costs, by leveraging external computing resources. However, we must address three practical road blocks to make offloading amenable to adoption by enterprises: (i)ensuring privacy and trustworthiness of offload, (ii) decoupling offloading systems from their reliance on the availability of dedicated resources and (iii) accommodating of-fload at scale.

DiegoKreutz and Fernando M. V. Ramos, Towards Secure and Dependable Software-Defined Networks in 2013, in this paper, we Software-defined networking empowers network operators with more exibility to program their networks. With SDN, network management moves from codifying functionality interms of low-level device configurations to building software that facilitates network management and debugging. By separating the complexity of state distribution from network specification, SDN provides new ways to solve long-standing problems in networking | routing, for instance while simultaneously allowing the use of security and dependability techniques, such as access control or multi-path.

Xiao Wen and Yan Chen ,Towards a Secure Controller Platform for Open Flow Applications 2013, the Open Flow (OF) paradigm embraces third-party development efforts, and therefore suffers from potential trust issue on OF applications (apps). The abuse of such trust could lead to various types of attacks impacting the entire network.

Rajesh Narayanan, Geng Lin, A Framework to Rapidly Test SDN Use cases and Accelerate Middle box Applications, 2013, Software-defined networking (SDN) is envisioned to provide a centralized interface to programmatically manage networking elements. However, despite its conceptual simplicity, Current switch and SDN architectures have poor performance with little support to innovate and test novel SDN applications.

4. PROPOSED WORK

The proposed approaches the Researchers have proposed that specialized middle boxes be defined entirely as virtualized software modules, and managed via standardized, open APIs. Proposed is an application development Framework facilitating the design of sophisticated threat detection and mitigation modules. This technique is very efficient if there is heavy interaction between branches and we can store the data normally and efficiently.

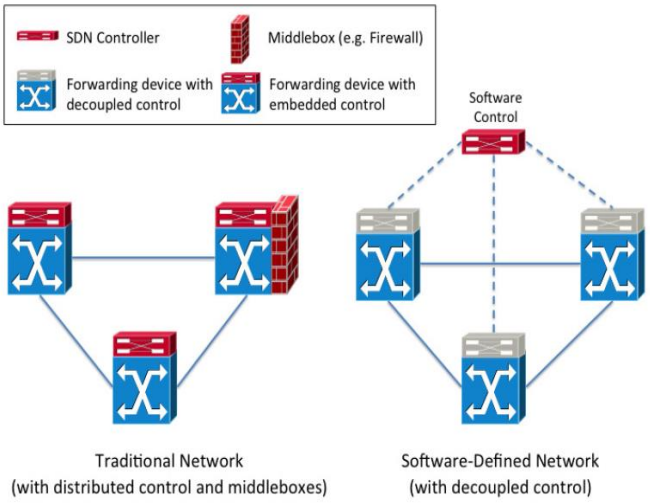

Fig. 1. The SDN architecture

Data communication networks typically consist of end user devices, or hosts interconnected by the network infrastructure. This infrastructure is shared by hosts and employs switching elements such as routers and switches as well as communication links to carry data between hosts. Routers and switches are usually “closed” systems, often with limited and vendor-specific control interfaces. Therefore, once deployed and in production, it is quite difficult for current network infrastructure to evolve; in other words, deploying new versions of existing protocols (e.g., IPv6), not to mention deploying completely new protocols and services is an almost insurmountable obstacle in current networks. The Internet, being a network of networks, is no exception.

Software-Defined Networking was developed to facilitate innovation and enable simple programmatic control of the network data-path. As visualized in Figure 1, the separation of the forwarding hardware from the control logic allows easier deployment of new protocols and applications, straightforward network visualization and management, and consolidation of various middle boxes into software control. Instead of enforcing policies and running protocols on a convolution of scattered devices, the network is reduced to “simple” forwarding hardware and the decision-making network controller(s).

We analyze and design an effective /load balancing algorithm that spreads the multimedia service task load on servers with the minimal cost for transmitting multimedia data between

server clusters and clients, while the maximal load limit of each server cluster.

In the existing system, task of document summarization aims to generate a very short summary for a given document or document set. Various methods have been proposed for document summarization, including rule-based methods graph-based methods learning-based methods ILP-based methods etc.

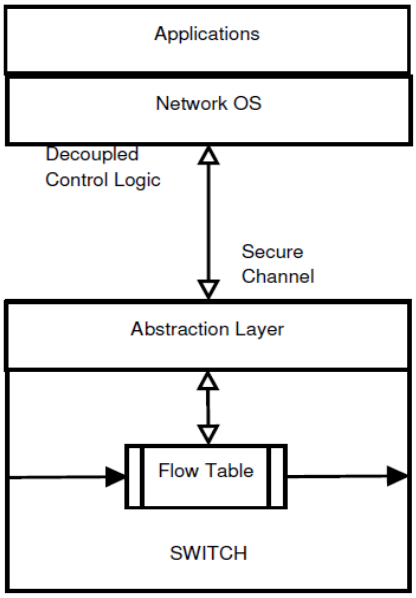

Fig. 2. The separated control logic can be viewed as a Network

5. IMPLEMENTATION

The Scope of the project is Enterprises today face a barrage fever evolving security thetas, and have little choice buttorely on a combination of security solutions that are complicated, distributed, and limited in scope security policies are typically implemented as complex, topology dependent access control lists. Trust is distributed across multiple components, such as switches, Domain Name System (DNS) servers, and authentication services and Remote authentication Dial in user Service and each of these individual components need to be protected in turn.

Modules:

1. Admin: Authentication, Verify the Employees Request Details ,Send The Web Link
2. Employees: Authentication, Internet Browser page, Request page, Received web link Page, Received web link Access Page.

Authentication: If you are the new user going to login into the application then you have to register first by providing necessary details. After successful completion of sign up process, the user has to login into the application by providing username and exact password. The user has to provide exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself.

Verify the employees requests: In this scheme Admin Verify the Employees Requests based on the employees Id in That If Admin Accept That request Admin Will Send Web Link to Employees based On Employee Id. this Link Will Get the Employees.

Send web link to employees: The admin will verify the employees requests in that admin if accept employees then admin will send web link to employees.

Send request to admin: The user after the successful login goes to Employees Homepage In that employees open The Internet browser If They Want to access the protected keyword that time employees send request to admin. These requests will get The Admin.

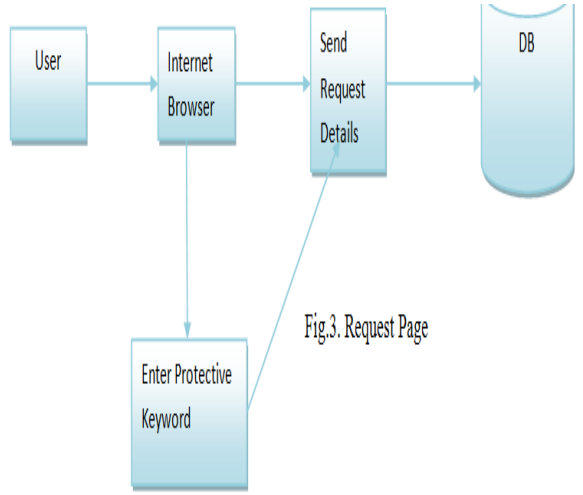

Fig.3. Request Page

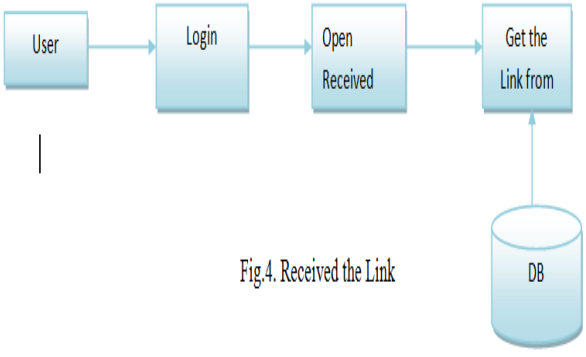

Fig.4. Received the Link

Anomaly detection algorithms: To protect user privacy, the author makes the following recommendations. First, he proposes that ISPs or home users obfuscate System addresses

in flow statistics. Second, he suggests that anomaly detection algorithms process aggregate data using System prefixes rather than individual System.

6. SYSTEM ARCHITECTURE AND RESULTS

The users or nodes involved in our projects are Sender, Intermediate and Receiver. In order to send file, the sender has to find out the list of nodes which are connected with the sender. From that available list he can choose receiver. Then the sender has to analyze the performance of each and every node which is connected with the sender. The performance analysis list will return the priority based result so that sender can choose the intermediate to send the file. The Intermediate will receive the file from sender then it will analyze the performance so that it can send data to another intermediate or receiver. In the receiver side, the receiver has to select the file path to receive the file from sender or intermediate. Then the receiver can view the file received file.

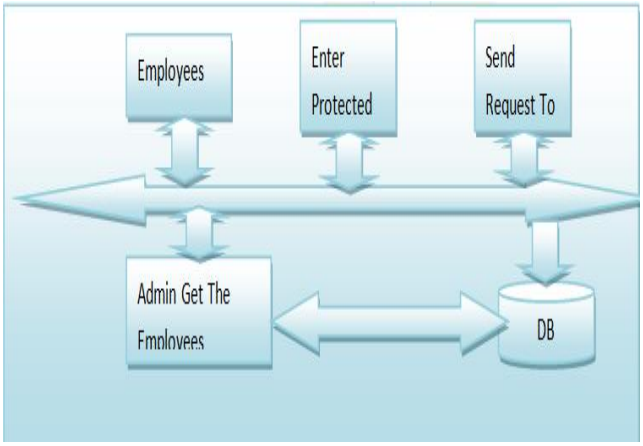

Fig. 5. System architecture

Table 1. Register Table

SPIRO21.software...dbo.programmerreg*

Column Name	Data Type	Allow Nulls
employeeid	varchar(50)	☑
username	varchar(50)	☑
lastname	varchar(50)	☑
password	varchar(50)	☑
gender	varchar(50)	☑
dateofbirth	varchar(50)	☑
emailid	varchar(50)	☐
designation	varchar(50)	☑
address	varchar(50)	☑
mobilenum	bigint	☑
		☐

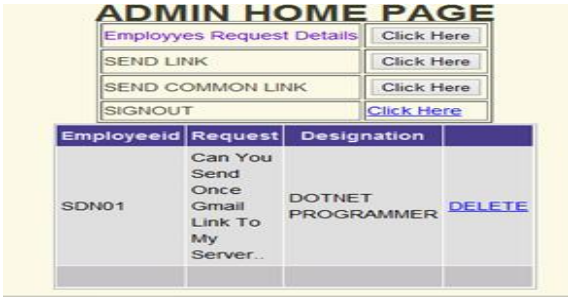

Fig.6.Modules

7. FUTURE ENHANCEMENT

In future work, we will improve our time saving suppose if some team employees ask same link to access that time admin no need to send each employee that link simply admin send to common browser based on the common browser that team employees can access. Whenever admin will delete that link team employees cannot access again.

8. CONCLUSION

In this paper we have a briefed SDN most prominent security issues arise while deploying it in enterprise networks. Conclusion of the work is how to protect the internet application by using software defined networking. In particular we described the SDN architecture in detail as well as the Open Flow [85] standard. We presented current SDN implementations and testing platforms and examined network services and applications that have been developed based on the SDN paradigm. Other issues are related to centralized control which always addresses issues like availability, scalability and interoperability because till now no standards defined in controller [2]. Some of the issues are related to the integrity and confidentiality of flow which added by controller [3].

REFERENCES

[1] E. Banks, Automation is a Logical Next Step in the SDN Migration Journey, Network World, Sep.9,2014 [Online]. Available:http://www.networkworld.com/article/2603534/sdn/incremental-Sdn automating network device configuration.html.

[2] S. Hall, Why Enterprises Struggle With IT Automation, ScriptRockBlog, May 29, 2014 [Online]. Available: http://www.scriptrock.com/blog/why-enterprises-struggle-with-it-automation.

[3] P. Release, "Hacking Habits" Survey Cites Misconfigured Networksas the Main Cause of Breaches, Tufin Technologies, Aug. 31, 2010[Online]. Available: http://www.tufin.com/about-us/news-and-media/press-releases/2010/august-31,-2010/.

[4] R. J. Colville and G. Safford, Configuration Management for Virtual and Cloud Infrastructures,GartnerInc.Oct.27,2010[Online]. Available:http://www.gartner.com/id=1458131.

[5] A. Feldmann, M. Kind, O. Maennel, G. Schaffrath, and C. Werle,Network Virtualization—An Enabler for Overcoming Ossification,European Community in Information Technology (ERCIM)News,retrievedJun.14,2013[Online].Available:http://ercimnews.ercim.eu/en77/special/network-virtualization-an-enabler-for-overcoming-ossification.

[6] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson,J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovationin campus networks," *ACM SIGCOMM Comput. Commun. Rev.(CCR)*, vol. 38, no. 2, pp. 69–74, 2008.
[7] N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, andS. Shenker, "NOX: Towards an operating system for networks," *ACMSIGCOMM Comput. Commun.Rev.*, vol. 38, no. 3, pp. 105–110, 2008.
[8] S. Shin, P. Porras, V. Yegneswaran, M. Fong, G. Gu, and M. Tyson,"FRESCO: Modular composable security services for software-definednetworks," in *Proc. ISOC Network and Distributed System Security Symp.(NDSS)*, 2013.
[9] V. Mann, A. Vishnoi, K. Kannan, and S. Kalyanaraman, "CrossRoads:Seamless VM mobility across data centers through software definednetworking," in *Proc. 2012 IEEE Network Operations and ManagementSymp. (NOMS)*, 2012, pp. 88–96.
[10] OpenFlow Network Research Center, retrieved Jun. 14, 2013 [Online].Available: http://onrc.stanford.edu/

Authors

Mr. Puneet S received M.Tech (CSE) from Visvesvaraya Technological University, Karnataka. His research interest includes image Processing, Network Security, Computer Networks. Presently he is working Assistant Professor in CSE Dept, Sree Dattha Institute of Engineering and Science**,** Hyderabad.

Mr. Krishana Reddy S received M.Tech (CSE) from Jawaharlal Nehru Technological University (JNTUH), Hyderabad. His research interest includes Computer Networks. Presently he is working Assistant Professor in CSE Dept, Sree Dattha Institute of Engineering and Science**,** Hyderabad.

Mr. Veeranna K received M.Tech (CSE) from Visvesvaraya Technological University, Karnataka. His research interest includes image Processing, Computer Networks. Presently he is working Assistant Professor in CSE Dept, Sree Dattha Institute of Engineering and Science**,** Hyderabad.

Ms. Nazimunisa received M.Tech (CSE) from Jawaharlal Nehru Technological University (JNTUH), Hyderabad. Her research interest includes Data Mining, Computers. Now she is working as an Assistant Professor in CSE Dept, Sree Dattha Institute of Engineering and Science**,** Hyderabad.