Use of Ambiguous Threat Intelligence for Safe Diagnosis of Software Utilizing Cyber Threat Intelligence in SDN Security

[1]A.Prakash, [2]M.Praveen, [3]A.Venu Gopal, [4]B.Ramesh

[1]Associate Professor, [2,3,4]Assistant Professor
Department of CSE
KPRIT, Hyderabad, India

Abstract: **As the number and variety of cyber threats increase, it becomes more critical to share intelligence information in a fast and efficient manner. However, current cyber threat intelligence data do not contain sufficient information about how to specify countermeasures or how institutions should apply counter measures automatically on their networks. Flexible and agile network architecture is required in order to determine and deploy countermeasures quickly. Software-defined networks facilitate timely application of cyber security measures thanks to their programmability. In this work, we propose a novel model for producing software-defined networking-based solutions against cyber threats and configuring networks automatically using risk analysis. We have developed a prototype implementation of the proposed model and demonstrated the applicability of the model. Furthermore, we have identified and presented future research directions in this area.**

Keywords**: Software defined networks; cyber threat intelligence; SDN; CTI; Network security.**

I.INTRODUCTION Now a days, as cyber threats are increasingly encountered in an increasing number and variety of cyber attacks, it is important for cyber security to share intelligence-related information about cyber threats quickly and effectively. However, the shared cyber threat intelligence data does not contain enough information to prevent countermeasures against threats or provide solutions to how institutions should automatically take measures in their own networks. A flexible and agile network is needed to determine the measures against cyber threats from the institutions and to implement them at the earliest time. The software's network allows programmable structures to be applied safely to the cyber safety precautions. In this study, a new model is proposed, which allows institutions to create network-based threat prevention solutions for their own networks by assessing collected cyber threat intelligence data from different sources and to automatically construct networks with a risk-based approach. A prototype has been developed for the proposed model and the feasibility of the model has been demonstrated and future research topics have been identified.

Today, the increase in services offered over the internet has changed the requirements of computer networks such as bandwidth, topology, networking [1]. Technologies such as cloud computing and the Internet of objects require dynamic and expansive networks [2]. However, it is not possible to meet these requirements completely and easily with traditional computer network infrastructure [3]. In order to meet these requirements, more dynamic computer networks such as software-defined networks (SDN), network function virtualization (NFV) have begun to be used [1]. Using the software defined network, the network can be easily controlled by programming the software without changing the current network topology. The development of innovative applications on this site enables independent updating of network devices and the easy loading of new network applications into the network. The rapid expansion of the Internet has also led to the intent of all devices connected to the Internet to become the target of the cyber attacks. Today, when we encounter new, more complex and different types of cyber attacks every day, it is necessary to share information about cyber threats quickly, identify precautions for threats, and eliminate threats as soon as possible. In this context, it is of utmost importance that cyber threat intelligence (CTI) data is shared among computers, which they can interpret [4].

Today, shared cyber threat intelligence data does not contain sufficient information about how to take measures against most threats or does not provide a solution to how institutions should take measures in their own networks. In addition, if the number of alleged cyber threat intelligence data from different sources is too high, it is necessary to decide on which intelligence data should be taken in consideration of network performance and risk analysis [5]. There is a need for tools to analyze shared cyber threat intelligence data to enable institutions to produce threat prevention solutions for their own networks and to reconfigure the network according to the solutions.

In this study, we analyze the data of cyber threat intelligence using the capabilities of the written language, a model has been proposed to provide solutions for threats identified by threat intelligence data and to enable them to be implemented in corporate networks.

In the following sections of this report, (Chapter VI), the prototype work prepared for the proposed model (Section VI), the current work is summarized (Section IV), the proposed model is described (Section VI), and the general information about the cyber threat intelligence (Section III) and work outcomes and future work (Chapter VII).

II. DEFENSE DEFINED AIMS

Software-defined Lanes are architectures that manage the data routing plane and the control plane in computer networks by separating them from each other. The ability of software to be defined includes the ability to provide centralized management, centralized programming with open standards, network management protocol, infrastructure and recovery network solutions, virtualized networking, and central monitoring units [6]. It is widely used in data centers, backbone networks, corporate networks and wireless networks because it is flexible, programmable and easier to maintain [7].

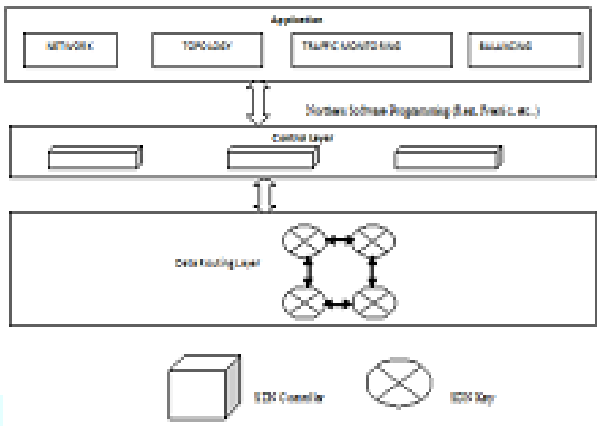

Fig.1: Software Defined Architecture

The software defined network consists of three layers and inter-layer communication interfaces as shown in Figure 1 [8]. The SDN keys in the data routing layer route incoming traffic according to the rules in the table contained in the device and collect statistical information about traffic during routing. If the incoming packet does not match any of the rules in the device tables, it is routed to the SDN controller in the control layer as the default behavior. The SDN controller decides which operations (forwarding, updating, downgrading, etc.) to be performed for packets coming from the SDN switches.

The SDN key can identify new rules. The SDN controller can collect statistical information from the SDN switches at regular intervals. Applications that are in the application layer and communicate with the SDN controller (networking, topology, traffic monitoring, etc.) can make changes or monitor the network with the SDN controller tool.

III. SIDING THREATS

The increased number of techniques that can be used for chilli attacks also increases the incidence of assault. This situation makes the security concerns of the institutions even more serious. In the classical approach, cyber threats are gathered, identified, grouped by experts in the field, and countermeasures are taken to counteract identified threats. Today, it is imperative to use proactive chiropractic approaches in view of the intentions and competencies of the attackers [5].

Cyber-threat intelligence is generally identified as evidence that is gathered and confirmed from multiple sources in order to counteract threats that are approaching [5]. It is necessary to create intelligence data so that the case studies and threats can be understood by the computers. Various standards (Open IOC, IODEF, STIX, etc.) have been identified for the sharing of these data [9], but these standards are being used to make people understandable [9], [10]. The following headings provide information on standards related to cyber threat intelligence.

1) Structural Threat Disclosure Statement (STIX) Standard Structured Threat Information expression (STIX) [11] is a standard with the following features that can be used to identify event cases with cyber threats.

• To be able to express all the information about the cyber threat area
• Human and machine readable
• Customizable by usage
• Use existing data definitions instead of redefining all cyber threat definitions
• It is possible to use it to make a lot of use by reducing the required areas.

The STIX v1.2 standard basically relies on the data model shown in Figure 2 [11].

• Observable, measurable event or information related to network and computer. This includes information such as files (name, size, summary value etc.), Network information (IP address, connection point, etc.) and directory information expressed in Cybox [12].
• Techniques, Tactics and Methods (TTP) are used to describe behaviours that define the event. TTP uses malware, attack patterns and Weaknesses.

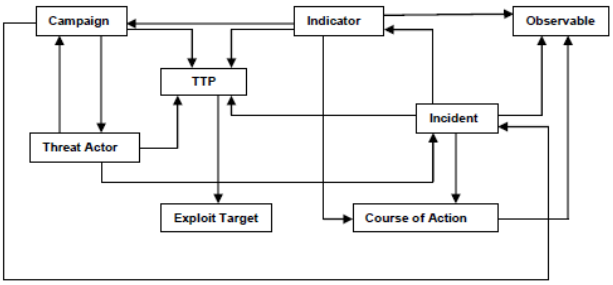

Fig.2: STIX 1.2 Data Model

• Indicator is an indicator that is defined to express an asset or behaviour in relation to the safety of a cigar. Indicators may include observations, other relevant indicators, related actions, the associated traceability, and the TTP information used.
• Incident is the data that represents an actual event. Past events and other events may include methods used, remedial measures, requested measures and observations.
• Campaign is used to identify the activities carried out on an organization and organization.
• The Threat Actor is used to identify the characters of the actors involved in harmful activities. Other activists explain their previous actions and the methods they use.
• Exploit Target is used to identify weak or fragile objects that are used by tactics, techniques and methods of harmful actors and which are in software, systems, networks, or building. Other target abuses related to target abuse and precautions that can be taken for this abuse can also be identified.
• The Course of Action describes the precautions that can be taken for an event or demonstration and the way to be followed for the measure.
The STIX standard is updated at regular intervals. STIX Work continues for the v2.0 standard. The data model is foreseen to be updated with STIX v2.0. This updated standard is intended to be compatible with the graphic representation of the data model, to share the data in the JSON data format, to include the CYBOX data format, and to make the data sharing between the machines more systematic.
2) Reliable Automatic Indicator Information Change (TAXII) Standard-The Trusted Automated Exchange of Indicator Information (TAXII) standard [13] is a standard that allows automatic sharing of threat data. TAXII standard.
The following supports the sharing of threat data by the methods described [14]:
• Endpoints generate and / or use data in the Hub and Spoke method. A central server bridges all of this communication.
• Subscribes to the source of the endpoints that want to use data in the Source / Subscriber method, and up-to-date information is shared with the subscriber.
• In Peer to Peer method, any two bits can share the data they want when they want it.

IV. AVAILABLE WORKS

Anchieta and Rothenberg [15] evaluate threats from the Brochure detection system in their work and convert the data from the trusted sources into a form that can be used by Bro IDS. Authors have tested their systems for shutting down and attacking a harmful website. It has been stated that the proposed method is capable of working proactively and reactively for threats. The rules created using information learned from cyber threat intelligence data are applied proactively to the SDN keys. When a threat is detected, the flow is stopped reactive and the traffic is directed to the honeycomb for detailed analysis. The proposed method does not include a component that would allow different prevention solutions to be implemented.
Jabiyev [16], taking STIX data from TAXII servers providing sample cyber threat intelligence data; has performed a work that creates rules that can be used by the Surakarta IDS / IPS attack detection and prevention system for seized IP addresses, domain names that are reported to be harmful, URL addresses, and harmful content signatures. The study focused on cyber threats that could enable threats to be prevented by IDS / IPS before re-configuring in computer networks.
Lu and Kokar [17] proposed a theory of state-based knowledge-based de duplication mechanism to determine whether cyber threat intelligence data would be taken into account by the institution. The suggested frame indicates that the threat queries can be answered automatically to determine special cases to be taken in the STIX data. Qamar et al. [5] proposed an OWL-based threat analysis framework to allow large volumes of cyber threat intelligence data to be described as standard, logically derived from data, and link analysis. Using the STIX data, vulnerability data and network topology data in the study, information such as threats to the organization, threats, probability, threats, threats, traffic patterns and threat agents are tried to be determined by means of outsourcing. Using this information, risk management is carried out. In the last stage, the components that the threats can affect in the organization are determined. There is no mention of how the construction will be done for the threats in the work. Different prevention methods can be used against the threats in the model we propose in the present study. In this context, in addition to the general security measures that can be taken using SDN capabilities, it is envisaged to use the methods in the following works.
Parker et al. [18] have used the SDN capabilities to build an infrastructure that tests the techniques to be applied to cyber attacks. This infrastructure has been used to develop training applications for monitoring network users, controlling traffic flow, black hole, routing, and poisoning techniques. The study was tested with pre-defined scenarios without using cyber threat intelligence data.

In the method named OF-RHM (Open Flow Random Host Mutation) proposed by [19], the SDN controller gives the virtual IP address to the servers and the real IP address is hidden from the unauthorized systems. In the proposed method, a moving target defensive technique is used with Open Flow. For DNS servers, virtual IP addresses are stored for the Internet addresses of the other servers, and these virtual IP addresses can be converted to real IP addresses from the SDN controller to provide access to the target servers. Virtual IP addresses are constantly updated to make the servers move logically.
Defence Flow [20], developed as a commercial product, selects the device to be protected for detected DDOS attacks, creates protection policy and flow system, and applies the changes to be made to the SDN. The aggressive traffic is also directed to the prevention device.

V. PROPOSED MODEL

The model proposed in this study is presented in Figure 3. The model consists of four components and two databases. With the components in the model; (CTI Analyzer) determines the indicators to be taken on the SDN networks by analyzing these data and generates rules that meet the precautions to be taken in SDN networks for identified indicators SDN Threat Prevention Producer) and the database is recorded. While some of the measures prepared may need to be implemented immediately in SDN networks, some may include measures to be taken in the event of a possible future attack. For this reason, it is governed in detail which proposals should be applied to the network (SDN Threat Prevention Implementation). The capabilities of the components in the proposed model and the basic functions they perform are summarized below.

1) CTI Toys

The CTI Toys compares the cyber threat intelligence data with the pre-determined TAXII servers in the configuration file. The STIX data packets are retrieved by querying the returned answers and the database is saved.

2) CTI Analyzer

The CTI Analyzer filters the data received from the CTI Display through various analyzes. It examines each indicator included in the data and evaluates it according to the following situations:

• Measures can be taken with SDN capabilities for the indicator (feasibility): By examining the cyber threat intelligence data, SDN whether or not the rules can be established. SDN rules are used to select the data that can be generated, and others are sifted.

• The reliability of the threat data in the indicator: The cyber threat intelligence can have high, medium and low reliability values in the data. Data with a high confidence level, medium confidence or no confidence is selected, and those with low reliability value are filtered.

The results obtained by evaluating the constructs are combined and scored in neat shape, and threats given higher scores than a certain threshold are selected to produce measures.

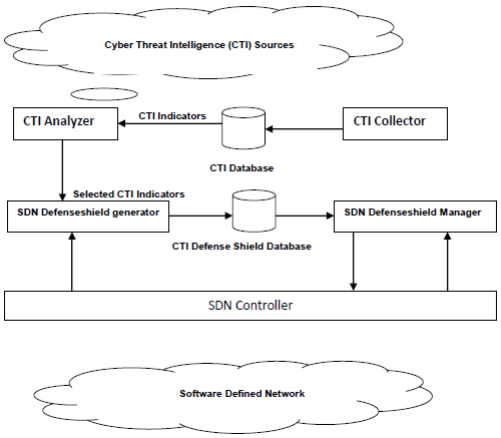

Fig 3. Proposed CTI-based model for increasing security in SDN networks (Proposed CTI-based model for software-defined networks)

3) SDN Threat Prevention Producer

SDN Threat Prevention The producer uses filters and indicators from the CTI Analyzer to determine which Open Flow rules should be applied to which switch of the SDN controller using the current network topology. This component primarily decides whether or not to take preventive measures for the indicator that it operates and then specifies the measures to be taken if the threat poses a threat. These measures are recorded in the SDN Threat Prevention Database.

4) SDN 7HKGLW GQOH\LFL Application

The SDN Threat Prevention Application reads the solutions found in the SDN Prevention Database and determines what needs to be immediately implemented and sends them to the SDN controller. In addition, it examines traffic and statistics on the SDN network and determines and enforces other rules that it can apply. This component contains a structure that allows dynamic application of rules using detailed statistics and network statistics.

VI. Prototop

A sample application that provides proof of concept of the proposed model has been developed with the Python programming language in order to increase the security of the software by using the cyber threat intelligence data.

Open day light SDN controller as SDN controller[21] and the corporate network topology defined in the context of network infrastructure use. The network topology was created in a realistic virtual network using the Mininet [22] emulation environment in the Linux Ubuntu 16.04 operating system . Elastic search [23] infrastructure has been used to store and update intelligence data and SDN defense methods.
Version 2.0 of the STIX standard has not been published yet and has been drafted. Since the cyber threat intelligence data sources are not yet compatible with STIX v2.0, studies conducted for CTI collection have been performed with STIX v1.1 and v1.2, and cyber threat intelligence data from CTI test TAXII servers [24] - [27] have been collected.
Within the scope of the CTI Analyzer prototype operation, the cyber threat intelligence data was selected which includes the command control server, IP list and data in the form of anonymous connection. The other data are filtered.
SDN Threat Prevention Filtered indications by the CTI Analyzer with the producer and the current network topology to be sent to the Open daylight SDN controller there are constructs in which switch which Open Flow rules will be applied. With these structures, methods such as field defense, interior protection, routing to another network, routing to a honeycomb, defending a moving target, disrupting traffic data can be described. In the context of the prototype, field defenses have been used as a method of prevention. In this method, the entrance and exit points of the defense network are detected and transmission of the traffic determined from these points is prevented. Other methods are planned to be used in subsequent workshops.
The SDN Threat Prevention Implementation component allows the SDN Threat Prevention to take precedence over the precautionary measures in the Database, sending Open daylight to the SDN controller and organizing the network. It is planned to develop rules for updating the priority of threats by using traffic and statistical information in future studies.
The developed prototype application has been tested on 6 different datasets. Table 1 summarizes the solutions produced by field defense method for cyber threat intelligence data in data sets.

Since all threat information included in the guest.MalwareDomainList_Hostlist dataset is included in the IP list, the SDN rule can be generated for all of them. The "guest.phishtank_com", "user_AlienVault", and "guest.Lehigh_edu" data sets used for the test are filtered because they do not contain data on the IP list, command control server, and anonymous connection type. In the developed prototype SDN rules are not produced at this stage for intelligence data such as the domain list, the URL list, and the harmful file summary value list. In this context, these data in the "guest.Abuse_ch" and "stix-data" data sets are filtered.
In future studies, it is planned to work for SDN rule generation for other types of threats other than the command control server, IP list and anonymous connection type data.

Data set	**Data set ADO**	**Total**	**SDN**
Source is		CTI data	karlon
			Produced
			CTI data
http://hailtaxii .com	Guest malware dom	1236	1236
	ainlist_Hostlist		
http://hailtaxii .com	Guest abuse_ch	549	296
http://edge.thr eatact	Stix-data	381	92
Orlab.com			
http://hailtaxii .com	guest.phishtank _co	9730	0
https://atxaali envault.com	user_AlienVaul t	889	0
http://hailtaxii .com	guest.Lehigh_e du		

VII. RESULTS AND FUTURE RESEARCH CONSIDERATIONS

In this study, a new model is proposed for increasing the security of computer network
by using the capabilities of the software described and cyber threat intelligence information.
A sample application has been developed and tested with test data for the proof of concept of the proposed model.
Below is a list of studies planned to develop a system for analyzing Cyber threat intelligence data and using these data to increase security in SDN networks.
• Developing models to determine the degree, importance, reliability and priority of Cyber threat intelligence data on SDN security,
• Using existing network topology to develop additional defense methods such as domain defense (internal network protection, routing to another network, routing to honeypot, defending a moving target, etc.)
• Developing methods to select the precautions to be taken before and during threats using existing network topology,
• Converting the specified security measures to SDN's controller to be transmitted to the network devices,
• Prioritization of the security measures developed by risk analysis,

• Updating security measures for threats according to varying network topologies,
• Changing the priority of safety measures by using existing traffic statistics and information.

BIBLIOGRAPHY

[1] S. Mehdi, J. Khalid, and S. Khayam, "Revisiting Traffic Anomaly Detection Using Software Defined Networking", Lecture Notes in Computer Science, c. 6961, p. 161-180, 2011.
[2] M. Vizváry and J. Vykopal, "Future of DDoS attacks mitigation in software defined networks", Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), c. 8508 LNCS, ss. 123-127, 2014.
[3] I. Alsmadi and D. Xu, "Security of Software Defined Networks: A Survey", Computers & Security, c. 53, pp. 79-108, 2015.
[4] C. Goodwin and J. P. Nicholas, "A framework for cybersecurity information sharing and risk reduction", 2015.
[5] S. Qamar, Z. Anwar, M. A. Rahman, E. Al-Shaer, and B. T. Chu, "Data-driven analytics for cyber-threat intelligence and information sharing", Computers and Security, c. 67, pp. 35-58, 2017.
[6] S. Scott-Hayward, S. Natarajan, and S. Sezer, "Survey of Security in Software Defined Networks," IEEE Communications Surveys & Tutorials, c. 18, No. 1, pp. 623-654, 2016.
[7] Y. Cui et al., "SD-Anti-DDoS: Fast and Efficient DDoS Defense in Software-Defined Networks", Journal of Network and Computer Applications, c. 68, p. 65-79, 2016.
[8] Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran, "Security in Software-Defined Networking: Threats and Countermeasures," Mobile Networks and Applications, pp. 1-13, 2016.
[9] E. Asgarli and E. Burger, "Semantic ontologies for cyber threat sharing
standards "in 2016 IEEE Symposium on Technologies for Homeland Security, HST 2016, 2016.
[10] D. Rhoades, "Machine actionable indicators of compromise", in 2014 International Carnahan Conference on Security Technology (ICCST), 2014, pp. 1-5.
[11] "STIX Project". [Online]. Available at
http://stixproject.github.io/getting-started/whitepaper/. [Access: 28-May-2017].
[12] S. Barnum, R. Martin, B. Worrell, and I. Kirillov, "The CybOX TM Language Specification", 2012.
[13] J. Connolly, M. Davidson, and C. Schmidt, "The Trusted Automated eXchange of Indicator Information (TAXII TM)", 2014.
[14] "TAXIDI for". [Online]. Available at:
http://taxiiproject.github.io/about/. [Access: 28-May-2017].
[15] J. R. Q. Ancieta and C. E. Rothenberg, "IntelFlow: Towards Adding Cyber Threat Intelligence to Software Defined Networks", 2015.
[16] B. Jabiyev, "Generating Application Layer IDS Rules from Cyber Threat Intelligence", Đstanbul Şehir University, 2016.
[17] S. Lu and K. Mieczyslaw, "A Situation Assessment Framework for Cyber Security Information Relevance Reasoning", 18th International Conference on Information Fusion, 2015, pp. 1459- 1466.
[18] T. Parker et al., "Defensive cyber operations in a software-defined network", Proceedings of the Annual Hawaii International Conference on System Sciences, 2016, c. 2016-March, pp. 5561-5568.
[19] JH Jafarian, E. Al-Shaer, and Q. Duan, "Openflow Random Host Mutation: Transparent Moving Target Defense Defined Networking", 1st Workshop on Hot Topics in Software Defined Networks (HotSDN 2012) pp. 127-132.
[20] J. Smith-perrone and J. Sims, "Securing Cloud, SDN and Large Data Network Environments from Emerging DDoS Attacks", 7th International Conference on Cloud Computing, Data Science & Engineering, 466-469.
[21] "Opendaylight". [Online]. Available at:
https://www.opendaylight.org/. [Access: 27-May-2017].
[22] B. Lantz, B. Heller, and N. McKeown, "A network in a laptop: Rapid Prototyping for Software-Defined Networks", in Proc. Of the Ninth ACM SIGCOMM Workshop on Hot Topics in Networks - 2010, ss. 1-6.
[23] "Elasticsearch". [Online]. Available at:
https://www.elastic.co/products/elasticsearch. [Access: 27-May-2017].
[24] "alienvault". [Online]. Available at: http://otx.alienvault.com.
[Access: 30-May-2017].
[25] "Threat Actor Lab". [Online]. Available at: http://edge.threatactorlab.com/. [Access: 30-May-2017].

A.PRAKASH, currently working as Associate Professor, CSE, Kommuri Pratap Reddy Institute of Technolgy. He completed his M.Tech in Software Engineering from JNTUH, He had an experience of more than 13 years in teaching and his areas of interest are Education Technologies, Computer Networks, Cryptography and Security

M. Praveen, working as an Assistant Professor , CSE Department, Kommuri Pratap Reddy Institute of Technology. He done his M.Tech in Computer Science And Engineering from SMEC Affiliated to JNTUH. He had an Experience of 2 years in teaching and His areas of interest are computer networking and Cloud computing.

Mr Aluri Venugopal Completed MCA from kakatiya university and Mtech from Acharya Nagarjuna University He has four years industrial experience , seven years teaching experience and two start up entrepreneurial ventures.

Mr.B.Ramesh completed his M.tech from NIT, Jalandhar. He has 3 years of teaching experience. His areas of interest is Information Security.