VULNERABILITY RETROSPECTION OF SECURITY SOLUTIONS FOR SOFTWARE-DEFINED CYBER-PHYSICAL SYSTEM AGAINST DDOS AND IOT-DDOS ATTACKS

Introduction to technical terms:

CLOUD COMPUTING:

--A general term used to describe a new class of network based computing that takes place over the internet

--A collection/group of integrated and networked hardware,software and internet infracture

-- These platforms hide the complexity and details of the underlying infrastructure from users and applications by providing very simple graphical

Interface or API (applications programming interface).

--Using the internet for communication and transport provides hardware,software and networking services to clients

--The platform provides on demand services,that are always on,anywhere like pay for use and as needed

--Services or data are hosted on remote infrastructure

--They contain containers to support virtualization.They dont need guest os

--Service models service models are the reference models on which the cloud computing is based.

These can be categorized into three basic service models as listed below:

1. Infrastructure as a Service (laaS) 2. Platform as a Service (PaaS) 3. Software as a Service (SaaS).

FOG COMPUTING:

- The devices comprising the fog infrastructure are known as fog nodes.
- In fog computing, all the storage capabilities, computation capabilities, data along with the applications are placed between the cloud and the physical host.
- All these functionalities are placed more towards the host. This makes processing faster as it is done almost at the place where data is created.
- It improves the efficiency of the system and is also used to ensure increased security.
- Helps in filtering important informtion from the massive amount of data and send that to cloud unlike edge computing.
- Limited storage capacity and processing power.
- Low latency
- Decentralized nature
- It is used when the data should be analyzed within a fraction of seconds i.E latency should be low.
- It is used whenever a large number of services need to be provided over a large area at different geographical locations.
- Devices that are subjected to rigorous computations and processings must use fog computing.

IOT(INTERNET OF THINGS):

- The iot is a system of interrelated computing devices,mechanical and digital machines,objects that are provided
- With unique identifiers and the ability to transfer data over a network withour requiring humam to human
- or human to computer interaction.
- Ability to access information from anywhere at ant time on any device.
- Improved communication between connected electronic devices.
- Transferring data packets over a connected network saving time and money.
- Reducing human interference.
- Save time and money.
- DATA COLLECTION BY SENSORS
- DATA STORING BY CLOUD
- DATA PROCESSESING
- DATA TRANSFER
- DATA DELIVERY BY ACTUATOR

SDN(SOFTWARE DEFINED NETWORKING):

- Software defined networking is an approach to networking that uses software based controllers or apis to communicate with underlying
- Hardware infrastructure and direct traffic on a network.
- It is a programmable interface.
- Consists of -APPLICATION PLANE
- -DATA PLANE
- -CONTROL PLANE
- . It consists of a centralized controller and controlled by protocolS
- CONTROL PLANE- Recieves requirements from application layer manages flow control.
- APPLICATION PLANE-the plane where applications that rely on the networkto provide
- services for end users.
- DATA PLANE-receives instruction from the control plane and forward the data packets through switches.
- Nbi are used for application plane and contol plane communication.
- Sbi are used for data plane and contol plane communication.
- Timely dealing with vulnerabilities.
- Effective monitoring of abnormal traffic

CYBER-PHYSICAL SYSTEM:

- Cyber-physical systems are the interconnection of the physical world,information exchange and controlling the physical systems with a loop back mechanism.
- Evaluate and save recorded data.
- Directly record physical using sensors and affect physical processes using actuators.
- Dynamically reconfigurable
- Intelligent
- Scalable
- Automated

SOFTWARE DEFINED CYBER PHYSICAL SYSTEMS:

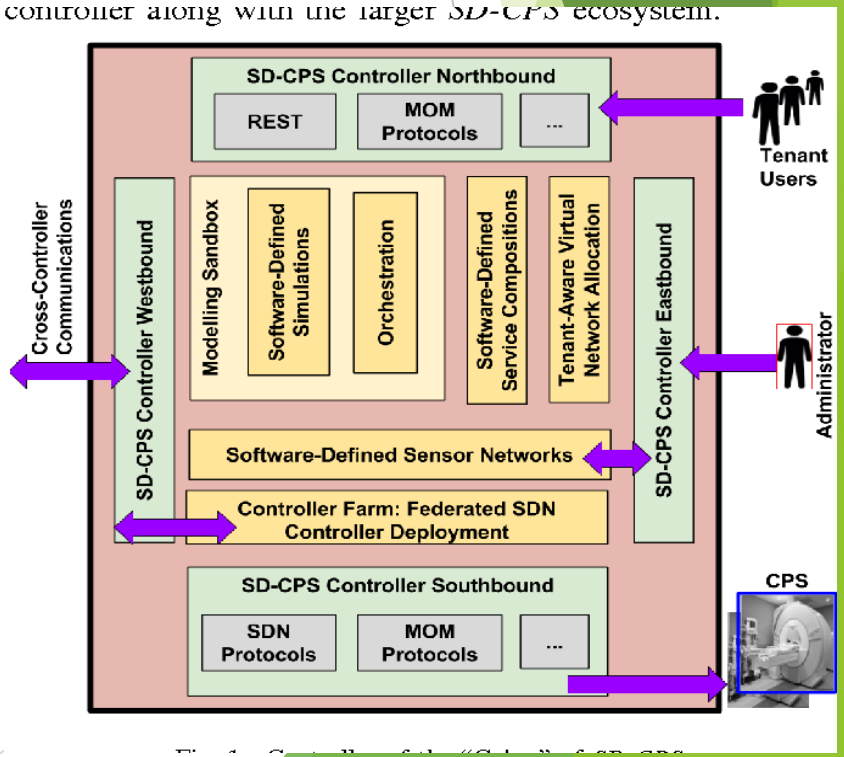
- The fusion of Software-defined networksin the communication layer transforms Cyber–Physical System

  into Software-defined Cyber–Physical System (SD-CPS) and has apotential considerable influence on the digital society.

- Sdn is used to defend against ddos attacks by centralized traffic monitoring ,dynamic updating of flow rules and network programability

VULNERABLE POINTS IN SDCPS:

- -Network layer
- -Physical devices
- -Sdn-forged traffic flows,manipulation of flow table,access to NB apis



DDOS:

Distributed Denial of Service (DDoS) attacks are the cyberattacks in which perpetrator makes the machine or network unavailable to legitimate users by disrupting the services of thevictim server by sending network traffic flood from geographically distributed devices AND PREVENTING IT FROM RECEIVING ANY DATA.

DDOS ATTACKS ARE LAUNCHED BY AN ARMY OF INFECTED COMPUTERS.

IOT-DDOS:

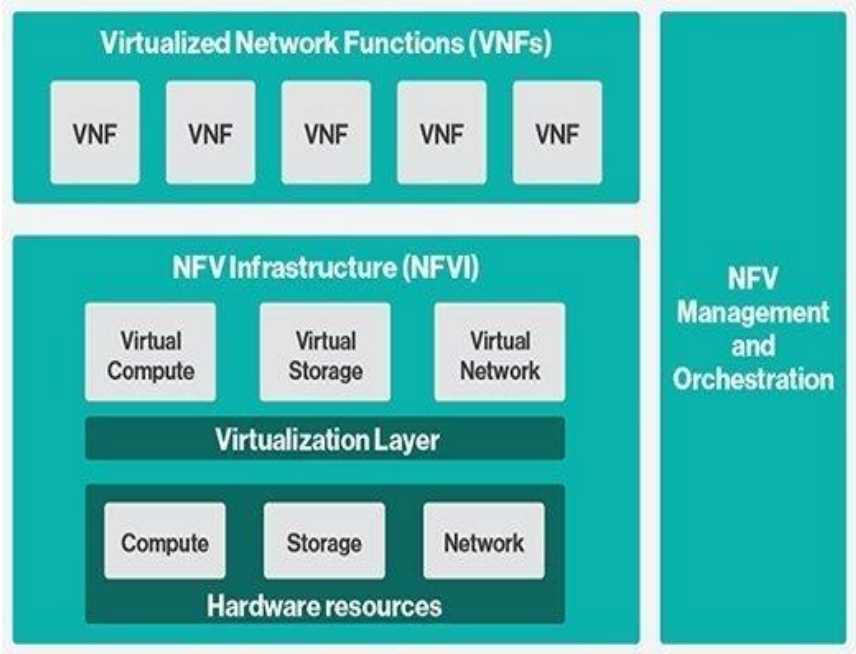
-- IoT-based DDoS attacks are into high attention which are launched by compromising the IoT devices. The results are devastating because the attack traffic is generated from millions of compromised heterogeneous IoT devices making the attack surface wider.

--The IoT-DDoS attacks are hard to handle because of very high traffic volume data, of the order of TB, generated by IoT devices.

-- DDoS attack detection methods implemented over Cloud will receive the legitimate as well as attack traffic, analyze traffic and send results back to the network enforcer to block the attack traffic will introduce latency in user operations.

NETWORK FUNCTION VIRTUALIZATION:

- Nfv is a new way to design,deploy and manage networking services.
- It is a complementary approach to sdn
- Nfv decouples the network functions,such as firewall,encryption form dedicated hardware and moves them to virtual functions.
- Reduces equipment and operational costs.



PROBLEM STATEMENT:

INCREASED DDOS ATTACKS DUE TO THE INCREASE IN THE ADOPTION OF CYBERPHYSICAL SYSTEMS USE OF BECAUSE OF THE INCREASED USE OF IOT,CLOUD COMPUTING IN INDUSTRY LEVEL.

LITERATURE REVIEW:

S.NO:	TITLE	PROPOSED METHOD	PROS	CONS	YEAR
1	A deep learning based intelligent framework to mitigate DDoS attack in fog environment	an intelligent framework with a blend of deep learning algorithms and fog computing paradigm to mitigate DDoS attacks. The authors have proposed a novel source-based defender.	▪ Decentralized data processing, storage. ▪ Increased system performance	▪ Power consumption increases ▪ Complexity ▪ Man in the middle attacks ▪ As there are millions of fog nodes they can be less secure	2019
2	Towards IoT-DDoS prevention using edge computing, in: USENIX Workshop on Hot Topics in Edge Computing	They have implemented the solution at the edge because the edge has the capability for IoT traffic packets processing. They have proposed an edge architecture to serve as an initial point of defense and named it ShadowNet.	▪ Fast detection of the attack	▪ As this occurs at edge level it can easily be flooded by heavy traffic and cant analyse The data.	2018

Flowtrapp: An SDN based architecture for ddos attack detection and mitigation in data centers	**proposal for DDoS attack detection and mitigation have come up with FlowTrApp design which can be used in SDN based data centers to address DDoS issues**	**The app detects and mitigates using the bound checks on flow rate and flow duration. These parameters are the decision-makers if traffic is being sent by legitimate users or not**	**Cant be accurate in case of high flow of data**	**2016**
Self-organizing map-based approaches in ddos flooding detection using SDN	They have implemented the proposed detection approach in SDN supported environment	monitoring, detecting, alerting for the attack, and offering the mitigation against DDoS attacks.	The traffic may be different for different types of devices which they are yet to automate in their future work.	2018

DDoS attack defense framework for cloud using fog computing	proposed a DDoS defense framework for Cloud which uses computation nodes at the Fog computing layer	▪ Immediate response ▪ Distributed storage	▪ Power consumption increases ▪ Complexity ▪ Man in the middle attacks	2018
Feature dynamic deep learning approach for DDoS mitigation within the ISP	They proposed the solution that can be implemented within the ISP domain	▪ They have used Apache Spark for distributed big data analysis to lessen the gravity of the high-volume attack ▪ As Netflow data volume produced by the ISP is too high, they have employed methods to boost system performance and data size reduction	▪ As authors have used dynamic feature selection technique which is expensive in terms of computationa l resources.	2020

Smart home IoT traffic characteristics as a basis for DDoS traffic detection	proposed a novel approach for IoT-DDoS traffic detection by classifying the IoT devices	▪ The proposed four-phased model runs through a collection of network traffic, pre-processing the collected traffic data, feature selection, and determining the device class affiliation	▪ May not be feasible for a large group of iot network	2018

PROBLEM DESCRIPTION:

As the there immense demand for sdcps these days the more physical devices are involved in sdcps deployment through iot,

- As they are outside the network they are easily prone to attacks due to outdated firmware and making the attack surface wider.
- These attacks also pose a more serious threats to individuals whose devices used in botnets.From the access through physical devices they can even enter the cloud and steal a lot of data.
- As the number of connected devices increases and more information is shared between devices,the potential that a hacker could steal confidential information also increases
- Enterprises may eventually have to deal with massive numbers and collecting and managing the data from all those devices will be challenging.
- If there is a bug in the system,its likely that every connected device will become corrupted.
- This causes a serious security threat and demands for the need to develop methods to recognize and eliminate these attacks permnently.

CONCLUSION AND FUTURE SCOPE:

- --In this paper, we have studied and examined the state-of-theart Cyber–Physical System, components of modern-day Cyber– Physical System, architectural details, security issues with a focus on most devastating DDoS and IoT-DDoS attacks. Fog Computing has been proposed as a layer between perception and cloud for performance improvement and executing the delegated tasks on behalf of the cloud. We have studied the proposed solutions in the field of DDoS/IoT-DDoS detection and mitigation. Finally, we have carried out vulnerability and gap analysis of the available solutions and concluded to general gaps or vulnerabilities using the narrow down approach.
- -- The spring of supporting technologies and supplication areas in Cyber–Physical System requiring further research are, for example, Security as-aservice, application areas of CPS (Smart Cities, Smart Farming, etc.), Security Issues and Challenges in CPS (Smart Cities, Medical Cyber–Physical Systems, etc.), Intent-based networking in Software-defined Networks.

RESULTS AND DISCUSSIONS:

- In this article eventhough fog computing is helpful it also has its demerits
- Power consumption increases
- Complexity
- Man in the middle attacks
- As there are millions of fog nodes they can be less secure attacks
- Sdn is suggested to include in cps but sdn controller is itself most vulnerable.
- Doesn't taken high volume real-time traffic into consideration.
- Researchers are relying upon simulated environment. Hence there is a need to device real time experimentation testbed for effective evaluation.
- They should have provide measures for performance evaluation using confusion matrix.

- REVIEW ARTICLES:
- R. Priyadarshini, R.K. Barik, A deep learning based intelligent framework to mitigate DDoS attack in fog environment, J. King Saud Univ. - Comput. Inf. Sci. (2019) http://dx.doi.org/10.1016/j.jksuci.2019.04.010.
- K. Bhardwaj, J.C. Miranda, A. Gavrilovska, Towards IoT-DDoS prevention using edge computing, in: USENIX Workshop on Hot Topics in Edge Computing, HotEdge 18, 2018.
- C. Buragohain, N. Medhi, Flowtrapp: An SDN based architecture for ddos attack detection and mitigation in data centers, in: 3rd International Conference on Signal Processing and Integrated Networks, SPIN 2016, 2016, pp. 519–524, http://dx.doi.org/10.1109/SPIN.2016.7566750.
-] T.M. Nam, P.H. Phong, T.D. Khoa, T.T. Huong, P.N. Nam, N.H. Thanh, L.X. Thang, P.A. Tuan, L.Q. Dung, V.D. Loi, Self-organizing map-based approaches in ddos flooding detection using SDN, in: International Conference on Information Networking, Vol. 2018-Janua, 2018, pp. 249–254, http://dx.doi.org/10.1109/ICOIN.2018.8343119.
- Deepali, K. Bhushan, DDoS attack defense framework for cloud using fog computing, in: RTEICT 2017 - 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, Proceedings, Vol. 2018-Janua, 2018, pp. 534–538, http://dx.doi.org/ 10.1109/RTEICT.2017.8256654.
-] I. Ko, D. Chambers, E. Barrett, Feature dynamic deep learning approach for DDoS mitigation within the ISP domain, Int. J. Inf. Secur. 19 (1) (2020) 53–70, http://dx.doi.org/10.1007/s10207-019-00453-y.
-] I. Cvitić, D. Peraković, M. Periša, M. Botica, Smart home IoT traffic characteristics as a basis for DDoS traffic detection, 2018, http://dx.doi. org/10.4108/eai.6-11-2018.2279336.