JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-8, Aug 2019 E-ISSN: 2347-2693

SD-IOT: Security and Privacy

Vishal S. Patil[1*], Suraj S. Bhute[2], Gauri J. Chauhan[3], Aparna P. Morey[4], Tejaswini S. Borkar[5]

[1,2,3,4,5]Computer Science and Engineering, Anuradha Engineering College, Sant Gadgebaba Amravati, Chikhli, India

Corresponding Author: vpatil1180@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i8.202207 | Available online at: www.ijcseonline.org

Accepted: 16/Aug/2019, Published: 31/Aug/2019

***Abstract*—** The Internet of things (IoT) is becoming apparent of the Internet which can connect nearly all environment devices, embedded with Internet Protocol (IP) and they are remotely monitored and controlled. Due to the huge growth of IoT devices, IoT networks are vulnerable to various security attacks. The implementation of efficient privacy and security protocols in IoT networks is extremely needed to ensure authentication, confidentiality, integrity and access control, among others. In this paper, I firstly present an in-depth meaning of the Internet of Things (IoT) and then propose a general framework for software-defined Internet of Things (SD-IoT) based on the SDx paradigm, software-defined everything (SDx) paradigm provides a way to strengthen the security of the IoT devices, as well as determines the impact of those new security and privacy issue and possible solutions. The proposed framework is implemented to strengthen the security of the IoT with heterogeneous and vulnerable devices. IoT**,** Software-defined Internet of Things (SDIoT)**,** Security, Privacy.

***Keywords*—**IoT**,** Software-defined Internet of Things (SDIoT)**,** Security, Privacy.

I.INTRODUCTION

Nowadays, The Internet has become a part of human's fundamental needs. most people complete their work, needs, or even transactions, sharing a large amount of data, playing games through the Internet. Such kind of interaction between humans and objects (things) requires connecting the objects around us with the Internet. Internet of Things (IoT) is becoming more popular, and it can be seen in the home, vehicles and wearable devices. IoT involves a large number of interconnected devices, including household appliances, wearable equipment, public facilities, medical equipment, unmanned aerial vehicles, and interconnected vehicles as well as other applications that require networking. These networking devices have no user interface, no security protocol, and no computing and storage capacity to enable firewalls and diagnostic tools; moreover, they cannot directly connect to the Internet via Wi-Fi. [1]

There are about 7 billion internet-connected devices according to Analytical sources. Due to the huge growth of IoT devices, IoT networks are vulnerable to various security attacks. The implementation of efficient privacy and security protocols in IoT networks is extremely needed to ensure authentication, confidentiality, integrity and access control, among others. protocols and Firewalls can manage the data traffic but are less effective in embedded protection of endpoints where the security usually depends on the characteristics of each node. Due to the huge growth of IoT device's implementation of privacy and security protocols is quite difficult so instead of changing security protocols in the device it is applied to the network, I proposed a general framework for software-defined Internet of Things (SD-IoT) based on the SD paradigm. The proposed framework consists of a controller pool containing SD-IoT switches, SD-IoT controllers integrated with an IoT gateway, and IoT devices. software-defined everything (SDx) paradigm provides a way to strengthen the security of the IoT devices. The software- defined Everything (SDx) paradigm includes software- defined radio (SDR), software-defined networking (SDN), defined radio (SDR), software-defined infrastructure (SDI), software-defined data centers (SDDC), and the software- defined world (SDW). [2]

Security must be protected by IoT systems for sensitive data and critical physical infrastructures. Users cannot use many IoT systems and applications without a good level of protection. Security in traditional networked systems remains challenging, while IoT systems present researchers with many more challenges due to the different special features of IoT systems. For the development of new security solutions, a thorough understanding of these challenges is essential. This study focuses on security threats and vulnerabilities in the context of the IoT and state-of-the-art IoT security. We survey a wide range of existing works in the area of IoT security that use different techniques. We present an IoT security taxonomy based on the current security threats in the contexts of application, architecture, and communication. Possible security threats and vulnerabilities of the IoT are also compared. We propose a new security scenario for the IoT structure and provide an analysis of the possible threats and attacks to the IoT environment. However, this shift from desktop PC to mobile, and now to IoT devices poses huge security risks of all sorts. Consider, for instance, the most recent and massive distributed denial of service (DDoS) attack in October 2016 targeting the Dyn server, which knocked offline major websites including Twitter, Spotify, Amazon, Reddit, Netflix, and The New York Times. [3][4]

II. RELATED WORK

The first Internet appliance was a Coke machine at Carnegie Melon University in the early 1980s. Programmers working several floors above the vending machine wrote a server program that chased how long it had been since a storage column in the machine had been unfilled. The programmers could connect to the machine over the Internet, check the status of the machine and determine whether or not there would be a cold drink awaiting them, should they decide to make the trip down to the machine.

Though the buzzword "Internet of Things" evolution was set out a way back in 1980's with coffee vending machine, the original term is coined by **Kevin Auston**, the Executive Director of Auto-ID Labs in MIT in 1999. The concept of IoT first became very popular through the Auto-ID centre in 2003 and in related market analyst's publications. Right from the beginning the Internet of Things evolution started, there were many things or objects connected to the internet for the different applications through diverse technologies depending on the type of object for the comfort ability of Human.

Yaser Jararweh, Mahmoud Al-Ayyoub,Ala' Darabseh, Elhadj Benkhelifa, Mladen Vouk , Andy Rindos published the paper on SD-IoT named as " SDIoT: a software defined based internet of things framework" on 20 February 2015. In this paper, a software defined based framework for the Internet of Things (SDIoT) is proposed. how the software defined system handles the challenges of traditional system architecture . [5]

Seongho Choi and JinKwak published a paper "ResearchArticle Enhanced SDIoT Security Framework Models" on 17 April 2016. In this paper, A security framework for the IoT environment that uses SDN technology has been studied. SDN has attracted attention as a means to improve efficiency and solve the limitations of the existing network environment. It uses software to organize the services provided by the existing network device through the improvement of the existing security control environment. [6]

Krushang Sonar, Hardik Upadhyay published a paper "A Survey: DDOS Attack on the Internet of Things". In this paper, the Internet of Thing is rapidly developing and become necessary and useful update in the near future. With this popularity of IoT security concerned with it is play a vital role. Prevent IoT from DoS/DDoS attacks is not an easy task, it faces so many challenges due to low power, low processing, and low memory.

Da Yin, Lianming Zhang, and Kun Yang, (Senior Member, IEEE), published paper named as "A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework" on April 30, 2018. In this paper, he describes a general framework for SD-IoT composed of an SD-IoT controller pool with controllers, SD-IoT switches integrated with the IoT gateway, and terminal IoT devices. [2]

III. METHODOLOGY

Working of IoT Technology

When talking about how does the Internet of Everything works, the process begins with devices that have built-in sensors, that are programmed to act in a certain way, are connected to achieve a certain result. The important data is then used to perform tasks that fulfill the needs of people.

1. Sensors/ Devices The almost component to consider in the Internet of Things technology is sensor/devices. A sensor picks up all the minute details from an environment, consists of many complexities. These sensors are built in the devices which collect all the data to be used later.
2. Connectivity*:* Once the data is collected it is transferred to the cloud infrastructure (also known as IoT platforms). But to transfer the data, the devices will need a medium. That's when connections like Bluetooth, Wi-Fi, WAN, cellular networks, etc come into play.
3. Data Processing After reaching the cloud infrastructure the data has to be analyzed so that the right action can be taken. The Analysis may be as straightforward as checking the temperature of the AC or a fancy one like a scenario wherever an unwelcome person comes in and therefore the device has to identify it through cameras. The IoT application is formed such it will method all the information at a quick rate to require immediate actions.
4. User Interface The last step is when the user is notified about the action with the help of a notification or an alert sound sent to the IoT mobile apps. the systems.

DESCRIPTION OF IOT SYSTEM ARCHITECTURE

In this paper, IoT system architecture has a seven-layer structure, as shown in Figure.1, from bottom to top, the bottom is IoT hardware devices and they are divided into two layers, sensing and act device layer and intelligent device layer; the above layer is related to information of things, they are physical information layer and logical information layer; then the above is the service layer, dividing into the IoT basic service layer and service middle layer; the top is the application layer. The devices in sensing and executing the device layer are divided into sensing devices and executing devices. Sensing device can be a sensor that directly accesses the intelligent device and transform the external physical signal into the signal that can be recognized by intelligent device; it can also be a sensing instrument, transforms the physical information into digit information and then transmits them to intelligent devices by bus; sensing device can also be a sensor network, it not only can collect information, but also transfer information along some paths, and finally send them to intelligent devices; executing device can receive control signals that intelligent devices send and control things' behaviors based on control signals.

As illustrated in Figure.1 The layered architecture of the IoT system The intelligent device layer contains the intelligent devices that can collect information about things and directly access the Internet. The intelligent devices are classified into IoT terminal, computer, and LAN. IoT terminal is an embedded system containing an intelligent chip, the computer can be a general-purpose computer, industrial computer or personal mobile devices, LAN must be connected to the monitoring and control equipment to provide information on things. The device layer of IoT provides the physical information of things to the upper layer, which constitutes the physical information layer of things. It is better to use data that are more easy to understand to represent, which is just like what programmers do when establishing an application database in general. So the information about things established in this way constitutes the logical information layer of things, the logical information of things describes virtual things. The basic service layer is the most critical layer of connecting things and the Internet. The basic services provided by things access to the Internet are divided into three types:

(1) Things identification: things identification is the simplest service that things can provide. To identify the things, first of all, it is required to set unique identifiers for things. There is not a unified standard for IoT things identifier at present. The common things identifier contains bar code, two-dimensional code, and RFID, and it was also suggested to regard IPv6 addresses as an identifier.

(2) Data collection of things: this is one of the earliest ways to be used, and the fields contain industrial control, environmental monitoring, automatic meter reading and so on. All of these data don't need to be extended to the Internet due to data specificity and security. The data collected from such services is highly relevant to the application, and many involve industry standards.

(3) Things behavior control: as well as (2), things behavior control is also one of the earliest ways to be used. This kind of control is an active behavior, mainly for industrial control, water, and other fields. If they are extended to the Internet, it is often related to higher security issues. There is a new area, which is an intelligent home, and it is a good way to control the behavior of home appliances through the IoT system. With the basic services based on things, there can be organic combination with the Internet service, then building the service middle layer, and making use of middle layer services to form service hierarchy that application layer needs. A middle layer service can be decomposed into sub-services and can integrate sub-services to finish the service. It shows the planning and resulting synthesis capability of the middle layer service. At the same time, planning capability also determines the interaction between services, and this kind of interaction can be constrained, and the constraints are distributed inside the service. [5]

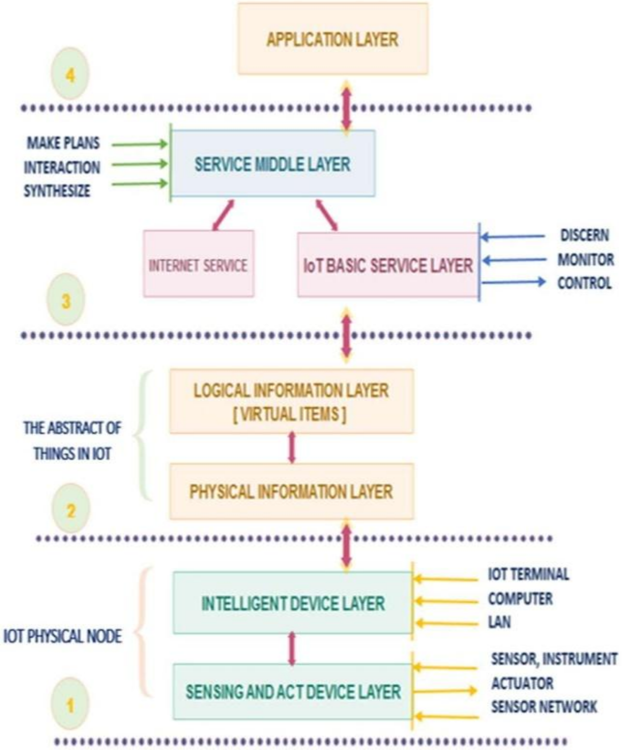

Figure.1 Layered Architecture of IoT System

Integrating SDN into IoT Networks

This section summarizes introduces the point of software-defined networking (SDN) and discusses it's the quality of being relevant to both acting as a gateway for IoT devices and as a security controller mechanism. Background About SDN, SDN is an open network architecture proposed in recent years to address some of the key shortcomings of traditional networks. The proponents of SDN state that the control logic of the network and network functions are two separate concepts, and should, therefore, be separated in different layers. To this end, SDN hence introduced the concepts of control plane and data plane: The centralized control plane (controller) manages the network logic, control traffic engineering functions from the data plane (switches) that just take care of forwarding the packets between the networks. So, the SDN can be considered as a physically distributed switching framework with a logically as illustrated Figure2. centralized control. SDN is designed for provisioning highly dynamic balance and quality of service/security policies. [3]

SD-IoT FRAMEWORK

In this section, we describe a general framework for SD-IoT using the SDx paradigm, as illustrated in Figure 3. The proposed SD-IoT framework can be seen as an extended version of the SDN architecture applied to IoT, as well as a general type of IoT architecture based on the SDN as proposed in [12]. The framework can be divided into three layers: the application layer, control layer, and infrastructure layer. The application layer consists of the IoT server in the cloud computing center, which is connected to controllers. in the SD-IoT controller pool, and the IoT server provides different applications and services via APIs.

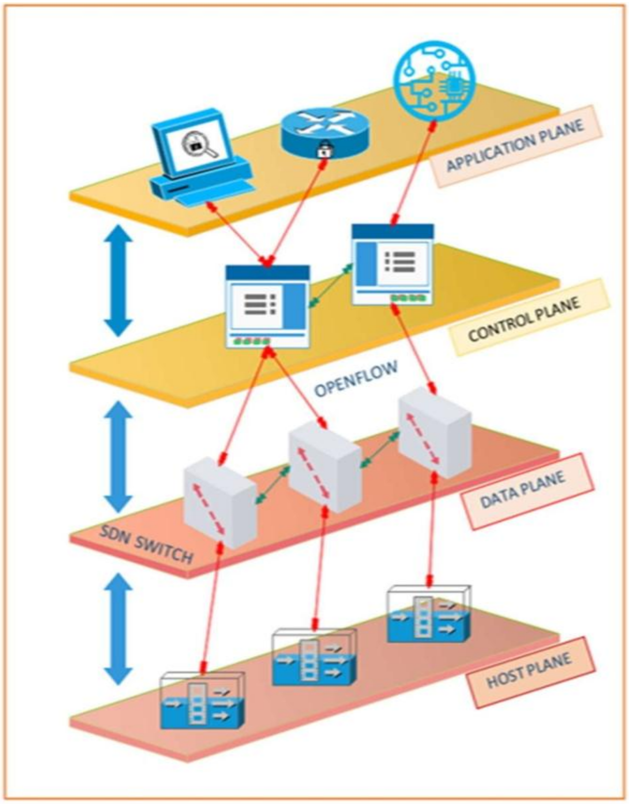

Figure.2 (a) SDN Architecture

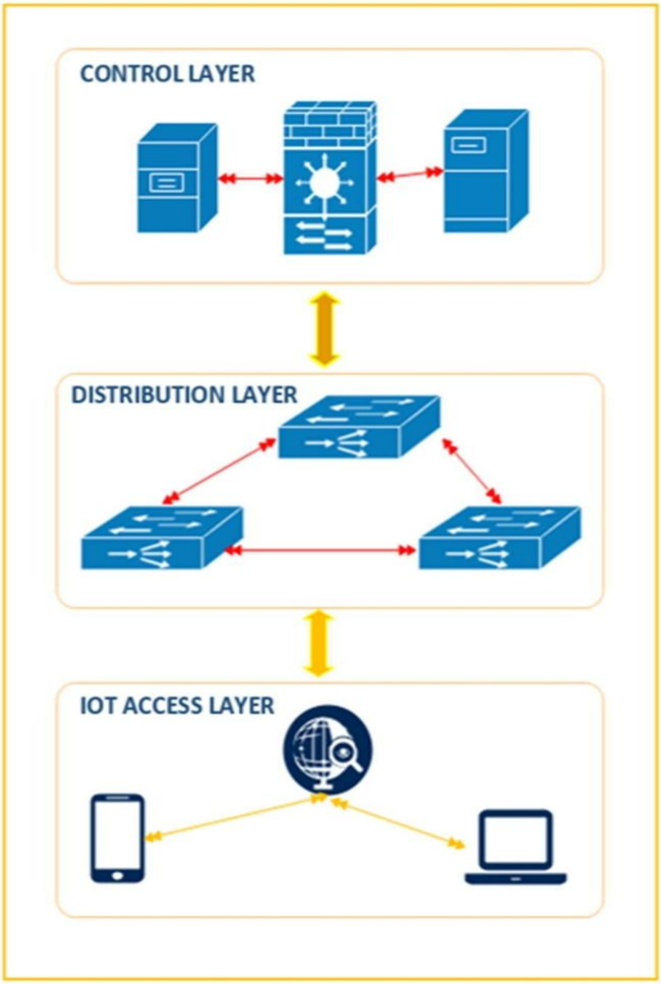

FIGURE.2 (B) SDN-IOT INTEGRATED ARCHITECTURE

The control layer consists of a controller pool with many SD-IoT controllers, which run a distributed operating system that provides logically centralized control and a topology view for IoT data forwarding in a distributed physical network environment which run a distributed operating system that provides logically centralized control and a topology view for IoT data forwarding in a distributed physical network environment

The infrastructure layer is a collection of a mass of SD- IoT switches. Every SD-IoT switch integrates the function of an IoT gateway and an SDN switch, and each SD-IoT switch can access different IoT actuating devices and sensing devices, such as cameras, digital cameras, smartphones, and personal computers, by controlling the data plane interface. The IoT gateway in the proposed SD-IoT framework is integrated with the function of an SDN switch, whereas the IoT gateway in the framework mentioned, [12] is separate from the SDN switch. In addition, the proposed SD-IoT framework adopts the SD-IoT controller pool, and whereas the framework in [13] adopts a single controller.

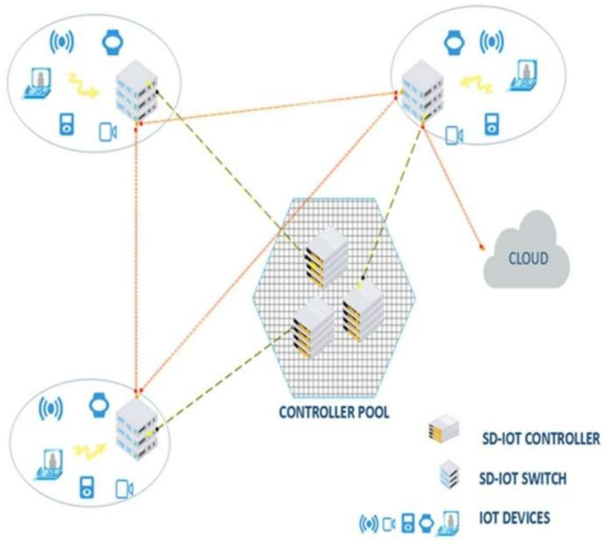

Figure.3 SD-IoT Framework

In the above-mentioned SD-IoT framework, the controller pool is designed as a vertical control structure, It is divided into two layers: the main control layer and the basic control layer. The main control layer interacts with the application layer upwards and interacts with the basic control layer downwards, and the basic control layer interacts with the infrastructure layer. Each controller of the main control layer, called the main controller, manages some base controllers, whereas the other basic controllers in the basic control layer are used as standby control objects. The main controllers are responsible for resource management, security, and coordination of the basic control layer and also offer a northbound interface for the application layer services. In the main controllers, a Leader is elected by using the Paxos algorithm to solve the consensus problem. The Leader can obtain the global network topology information, control the main controllers and coordinate the basic controllers. The basic controllers are responsible for resource management and security in a domain of IoT, as shown in Figure 3. IoT devices in the same domain can communicate through the basic controller of the domain. Each switch connects a master controller, and other controllers are known as slave controllers. Two IoT devices in different domains communicate through the main controller. The basic controllers communicate with the switches of the infrastructure layer, send packet-out messages to the switches at regular intervals, and obtain information on the switches through feedback packet-in messages. The basic controllers submit their own control information by interacting with the main controllers so that the main controllers can obtain the entire network global view. The load balance of the entire IoT can be improved through the coordination of messages in the main controllers and by using the dynamic load-balancing algorithm in the basic controllers [13]. The vertical structure of the controller pool is not only easy to manage but also solves a series of problems caused by the single point failure of the simple controller, e.g., incompatibility in the underlying controllers, load imbalance and message inconsistency between the main controllers. [2]

IV. CONCLUSION AND FUTURE SCOPE

In this paper, we have covered a brief overview of Internet of Things (IoT). Also we had focused on various points like Architecture of Internet of things as well as Integrating SDN into IoT Networks, how the software defined system handle the challenges of traditional system architecture as it provides a centralized, programmable, flexible, simple and scalable solution to control the systems, Then overview on how to Integrating SDN into IoT Networks The proposed model was built to provide a proof of concept, and we explained how the systems can be built to accommodate large data which produced from the widespread of the IoT.

REFERENCES

[1] Mosenia and N. K. Jha, "*A Comprehensive Study of Security of Internet-of-Things*," in *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586- 602,1Oct.-Dec.2017.doi: 10.1109/TETC.2016.2606384

[2] D. Yin, L. Zhang and K. Yang, "*A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework*," in *IEEE Access*, vol. 6, pp. 24694-24705,2018.doi: 10.1109/ACCESS.2018.2831284

[3] Krishnan, Prabhakar & S. Najeem, Jisha & Achuthan, Krishnashree. (2018)."*SDN Framework for Securing IoT Networks*" 10.1007/978-3-319-73423-1_11.

[4] Fadele, Alaba & Othman, Mazliza & Abaker Targio Hashema, Ibrahim & Alotaibi, Faiz. (2017). "Internet of things Security: A Survey. Journal of Network and Computer Applications". 88.10.1016/j.jnca.2017.04.002.

[5] Weigong LV, Fanchao MENG, "*AGeneral Architecture of IoT System*", International Conference on Computational Science and Engineering, Vol.1, No.5, pp.1-4, 2017.

[6] Jararweh, Yaser & Al-Ayyoub, Mahmoud & Darabseh, Ala & Benkhelifa, Elhadj & Vouk, Mladen & Rindos, A.ndrew. (2015). "*SDIoT: A Software Defined based Internet of Things framework*". Journal of Ambient Intelligence and Humanized Computing. 1. 453-461. 10.1007/s12652-015-0290-y.

[7] Choi, S., & Kwak, J. (2016). "Enhanced SDIoT Security Framework Models. *International Journal of Distributed Sensor Networks"*. https://doi.org/10.1155/2016/4807804

[8] Ullah, Rafi & ul Sami, Iftikhar & Ahmad, Maaz & Asif, Muhammad. (2018). "*DoS/DDoS detection for E- healthcare in Internet of Things*". International Journal of Advanced Computer Science and Applications. 9. 10.14569/IJACSA.2018.090140.

[9] Ma YW, Lai CF, Huang YM, Chen JL. "*Mobile RFID with IPv6 for phone services*." In: Proc. of the 13th IEEE Int'l Symp. On Consumer Electronics. Kyoto: IEEE Press, 2009. 169170. [doi: 10.1109/ISCE.2009.5156859]

[10] Yaser Jararweh1 ,Mahmoud Al-Ayyoub1, Ala' Darabseh1

"*SDIoT: a software defined based internet of things framework*", Springer-Verlag Berlin Heidelberg, pp.1-9, 2015.

[11] Krishnan, Prabhakar & S. Najeem, Jisha & Achuthan, Krishnashree. (2018)."*SDN Framework for Securing IoT Networks*" 10.1007/978-3-319-73423-1_11.

[12] A. Hakiri, P. Berthou, A. Gokhale, and S. Abdellatif, ''*software defined networking for efficient and scalable IoT communications,*'' IEEE Commun. Mag., vol. 53, no. 9, pp. 48–54, Sep. 2015.

[13] X. Zhong, *Research on Distributed Controller Deployment Algorithm Based on Software Defined Network. Changsha*, China: Hunan Normal Univ., 2017, pp. 29–33.

Authors Profile

Prof.Vishal S Patil pursued Bachelor of Engineering from SGBAU Amravati University of Maharatsra ,in 2012 and Master of Engineering from SGBAU Amravati University of Maharatsra Amravati University of Maharatsra ,in 2014. He is currently working as Assistant Professor in Department of Computer Science & Engineering, at Anuradha Engineering College Chikhli Since July 2014M.S. India.

Mr Suraj S. Bhute pursuing Bachelor of Engineering in Computer Science & Engineering Department from Anuradha Engineering College of SGBAU Amravati *University Maharashtra*

Ms Gauri J Chauhan pursuing Bachelor of Engineering in Computer Science & Engineering Department from Anuradha Engineering College of SGBAU Amravati *University Maharashtra*

Ms Aparna P Morey pursuing Bachelor of Engineering in Computer Science & Engineering Department from Anuradha Engineering College of SGBAU Amravati *University Maharashtra*

Ms Tejaswini S Borkar pursuing Bachelor of Engineering in Computer Science & Engineering Department from Anuradha Engineering College of SGBAU Amravati *University Maharashtra*