A Study of Different Intrusion Detection and Prevension System

Mitali Mittal, Alisha Khan, Chetan Agrawal

Abstract— a network is formed by grouping up of devices to communicate with each other through internet. During last few years, internet is providing the best technologies to communicate. Now-a-days public is so dependent on internet for numerous activities that it seems almost impossible to picture life and communication without internet. On the other hand, Internet is suffering through curse of security threats; because where information stands its security must be taken care of. Various technologies have come across to deal with the security of network. Earliest method: Intrusion (threat) detection systems (IDS) and the latest techniques: Intrusion (threat) prevention systems (IPS) are the important ones where security is concern. A system which detects illegal action to move into a computer and helps to notify the presence of some unauthorized means is IDS. A system which assists preventing the intrusion attack to maintain the security is IPS. This study of: Intrusion Detection & Prevention System (IDPS) has moved us through matters like intrusion, various technique & systems to detect and prevent them which are discussed as under.

Index Terms— Intrusion, Attacks, Detection, Prevention, System, Threats, Misuse, Network, IDPS

1 Introduction

From last some years, people from almost every society whether they are technocrats, students, bankers, corporate etc are getting dependent on I.T. rapidly. Social networking, stock prices, news, e-mail, online shopping, reservations, online education, etc are commonly used facilities of computer network. Where these facilities are present, on the other hand to destroy systems availability and integrity, threats also exist in network. These intrusion attacks on various security aspects of network system like

Confidentiality: Confidentiality specifies that only sender & the intended recipient(s) should be able to access the contents of message**.** Confidentiality gets compromised if an unauthorized person is able to access a message. The attack on confidentiality is called Interception.

Authentication: This mechanism helps in establishing proofs of identities**.** The authentication process ensures that the origin of an electronic message or document is correctly identified. The attack on authentication is called Fabrication.

Integrity: When the contents of a message are changed after sender sends it, but before it reaches the intended recipient, we say the Integrity of the message is lost. The attack on the integrity is called Modification.

Availability: The principle of availability states that resources (i.e. Information) should be available to authorized parties at all times. Such an attack is called as interruption. Interruption puts availability of resources in danger.

Earlier security was maintained by the use of antivirus and firewalls. Both helps in opposing viruses and worms. But this doesn't seem to be strong enough to overcome huge malicious attacks and intrusions like Trojan horse, zombie, viruses, masquerades etc. In today's world, systems like IDPS are in huge demand to oppose these intrusions by monitoring & blocking them and maintaining security.

2 Intrude, Intruder & Intrusion

2.1 Intrude

Intrude means to get involved into some process or task(s) uninvited. Else it could be simply defined as to "disturb" a situation, part or position of something already running with stability or settled.

2.2 Intruder

The intruder is something that enters a system with nonspecific recognition; to attack systems integrity. Prevention and detection here in this discussion is all to stop the activity of the intruder. The role of an 'intruder' is often confused with a 'hacker' [*]. To clear this: Intruder is someone who breaches a perfectly stable system with a criminal mindset. But a hacker is skilled, qualified with sound technical knowledge. In fact, the ethical hacker helps to trace invasion made by the intruders.

There are two types of intruder:

- **Internal Intruder:** The internal intruders are insiders who have been entrusted with authorized access to the machine or network. [10] The intruder requires access in order to fulfill obligations to the victim network. Internal intruder consist of two types including masquerade and clandestine.
- **External Intruder:** The external intruders are outsiders who have unauthorized remote access to machine or network and usually contain limited number of entry to attack the network from outside. [10]

- *Mitali Mittal is currently pursuing masters degree program in computer science engineering in Sagar Institute Of Research And Technology,Bhopal,M.P., India, PH- +90-8889200945. E-mail: mitali13mittal@gmail.com*
- *Alisha Khan is Asst Prof in IT Department at Radharaman Engineering College, Bhopal M.P., India, PH- +91-9407278989. E-mail: alishakhan.16@gmail.com*
- *Chetan Agrawal is Asst. Prof. CSE Department at Radharaman Institute of Technology & Science., Bhopal, M.P, India, PH- +91-9754502691. E-mail: Chetan.agrawal12@gmail.com*

2.3 Intrusion

Intrusion is an act of trespassing without any permission and hence resulting in loss and destruction. There are various ways to perform intrusion, some of which are listed below:

Classification of Intrusion:

1) Insider Attack: An insider attack is an intentional misuse of machine or networks by authorized user, such as a disgruntled employee attacking the network.[12] Insider attacks can be malicious insiders who intentionally eavesdrop or damage information in a fraudulent manner or can deny access to other authorized user. Insider attack can also be no malicious attacks which typically result from carelessness, lack of knowledge, or intentional circumvention of security. Insider attacks result in more financial and other loss than another other type of attack

2) Denial of Service: Denial of service attack: Unlike a password-based attack, the denial-of-service attacker makes some network or memory resource engaged to handle legitimate requests, or Block traffic, which results in a loss of access to network resources by authorized users to bring the network to its knees by flooding it with useless traffic.[12] It causes a disruption to the network by making network connectivity available through more than one service. [10] There are many varieties of DoS attacks including mail bomb, Neptune, smurf attack, Ping flood, Ping of death, teardrop attack, etc

DoS attack may be performed at the network and application layer by sending carefully crafted and malicious datagram's that cause network connections to fail and become extremely busy or unavailable or stop functioning. Preventing apprehensive network traffic from reaching your hosts and preventing apprehensive program commands and requests are the best ways of minimizing the risk of a denial of service attack

3) Port Scanning: Port Scanning is process of systematically scanning a computer's port. A port is a section of a system where information goes in and out. Port Scanning is understood as open doors to a computer. [12]It has valid usage in managing network which can make it malicious in nature.

If someone is looking for a weaker access point to attack into a system while accessing internet, it could be work out easily because there is no way to stop port scanning during internet access as internet server is accessed through open ports (door).

4) User to Root Attack: Here, an attacker starts access to a normal user account on the system by sniffing password or dictionary attack. This makes him able to misuse some vulnerability for gaining root level access to system. There are different types of User to root attack where the most common is the buffer overflow attack which are used to generate root shells from a process running as root. It happens when a program copies too much data into a static buffer without the surety that the data will fit. [10]The mechanisms used to secure the authentication process are frequent target since there are no universal mechanisms that can be used to prevent security risks like weak password attacks, phishing attacks, key loggers, etc. [11]

5) Flooding Attack: Attack means any method used to try to go against the security and integrity of a network/system. Attack that tends to fail the pacing between the sender and receiver within the network/system is known as Flooding attack.

***6) Backdoor Channel Attack*:** Backdoor channel attack is an undocumented way of gaining access to a program, online services or an entire system. This is also known as Trapdoor Attack. [12] This attack is a potential security for whoever found a possible Net way to use backdoor channel to gain an unauthorized access.

3 APPROACHES OF IDS

IDS is a device or software application that monitors network and/or information system for malicious activities or policy violations and responds to that suspicious activity by warning the system administrator by one of several ways, including displaying an alert, logging the event or even paging the administrator.

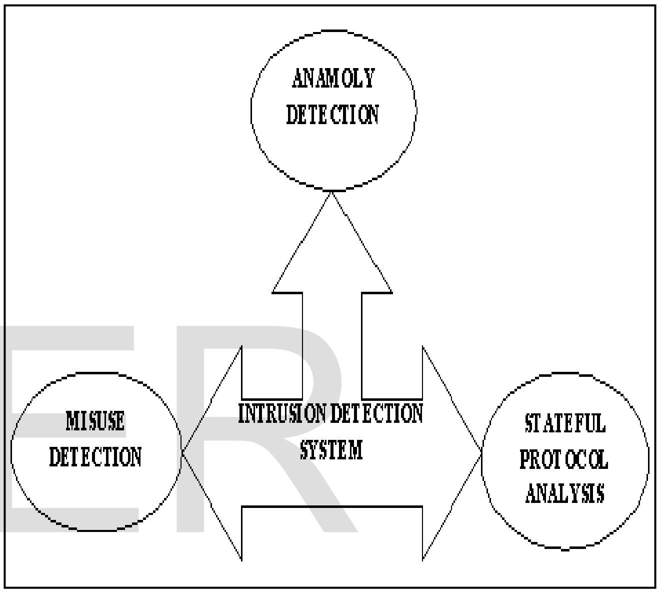

Fig 1 Approaches of IDS

3.1 Anomaly Detection:

Misuse is bounded but Anomaly is adaptive. Anomaly detection technique finds "normal activity profile" for the system logs event, network packet, kernel, software running, operating system information, etc into the database. If any abnormal activity or intrusive activity occurs in the system which deviates massively from system normal behavior then an alarm is raised against the event, which indicates it is a fabricated event. Anomalous activities that are not intrusive are flagged as intrusive. This results in false positive, i.e. false alarm. Intrusive activities that are not anomalous result in false negative [15].

Anomaly based detection can be static or dynamic. Once raised, a dynamic profile is adjusted perpetually as additional events are observed. Because systems and networks change over time, the corresponding measures of normal behavior also change. A static profile is stable unless the IDS are specifically directed to generate a new profile. [12] Anomaly detection can be used in variety of applications such as military surveillance for enemy activities, intrusion detection for cyber-security, etc

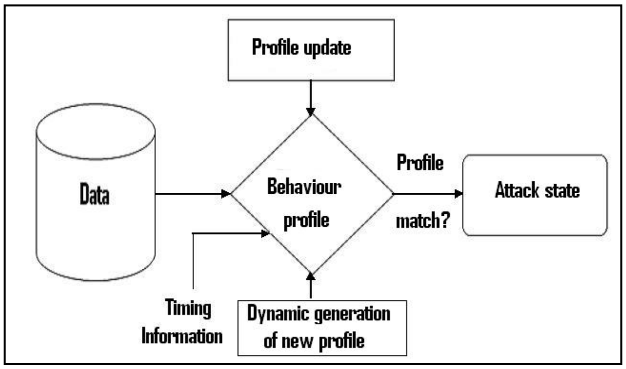

Fig 2 Anomaly Detection

3.2. Misuse / Signature Based Detection:

The concept behind signature detection or misuse detection scheme is that it stores the pattern, signature of the attacks and tries to detect abnormal behavior by analyzing the given traffic and matching several rules. As soon as the match found system generates alarm. Based on Analysis and comparison with the Rules the system can detect any attacks, such as matching signature pattern. [9].

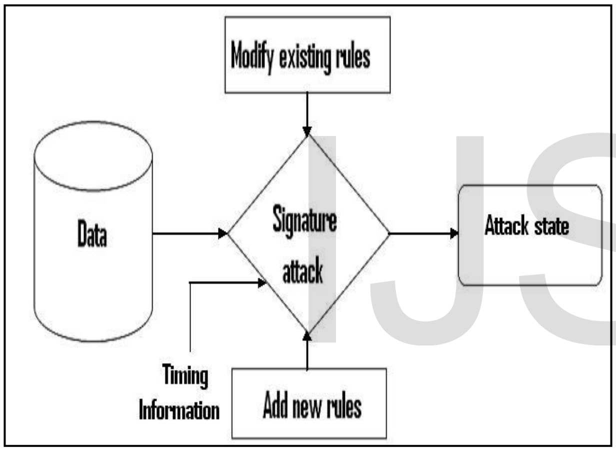

Fig 3 Misuse Detection

Little variation in known attacks may also affect the analysis if a detection system is not properly configured [9, 10].It cannot detect an unknown event (signature not known). Therefore, signature based detection is an efficient solution for detecting known attacks but fails to detect unknown attacks or variation of known attacks[11]

3.3. Stateful Protocol Analysis:

In Stateful protocol analysis user profile is not developed by network history for a particular organization. It is an alternation of the anomaly detection approach, IDS vendor provide universal profiles for how particular protocols should be used from the network of many organizations where information is collected to create these profiles. Using this approach, the IDS keep an eye on the "state" of a network, transport or protocols and then compare it with the behavior of user to check for violations. For example when the user starts access to the File Transfer Protocol the state is initially unauthenticated where the user can access few commands such as it can view help information or can request user name and password. When a FTP authentication attempt occurs, the IDS can determine if it was successful by finding the status code in the corresponding response. Once the user has authenticated successfully, the session is in the authenticated state, and users are expected to perform any of several dozen commands. The main advantage of this approach is that the user profiles are maintained and updated by the vendor. This type of IDS cannot detect Denial of Service attack because it does not violate acceptable behavior. [14].

4. Approaches of IPS

IPS has the ability to prevent known intrusion detected signatures, besides the unknown attacks originating from the database of generic attack behaviors. IPS can proactively block attacks.

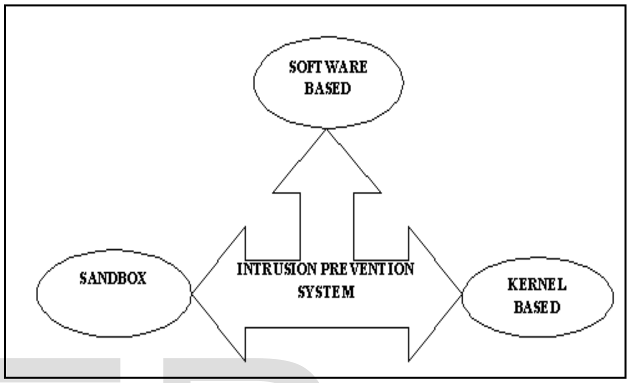

Fig 4 Approaches of IPS

4.1. Software Based Approach:

This approach is found with resemblance to IDS's anomaly detection which is based on comparison of recent activity with the log files containing normal activity profile of network and its: users, connection & hosts & application with the log files containing normal activity profile of network and its: users, connection & hosts & application, etc.., But in addition to it, this approach has the ability to oppose intrusions and obstruct them. [17]

4.2. Sandbox Approach:

Sandbox is a particular portion which has restriction to access to rest of resources in a system. For example; for security purpose mobile code is used which uses Active X, Java applets & other scripting languages. These valuable stuffs are isolated from rest of the system within sandbox. System runs the code in this sandbox and examines its behavior. If the code deviates from a predefined policy then it will stop processing & executing.

4.3. Kernel Based Protection Approach:

Kernel controls access to system resources like memory, CPU & peripherals to prevent user's direct access by sending user's application request to Kernel to take access permission. Execution of any code will use at least one system call to get access to privilege resources.

Kernel Based Intrusion Prevention System (KBIPS) helps prevent execution of malicious system calls. Using this approach threats could be avoided by protecting system resources, stopping privilege escalation exploits, preventing buffer overflow, stopping access to email contact list, etc.

4.4. Recognition Attack:

This approach aims at something very important for a system's security. Many methods for attack recognition had come across the year. Most of them focus mainly on the alarms of intrusion detection system and using low efficiency algorithms that can extract attack without rebuilding attack paths [16].

5. Detection & prevention system

From the above matter a question what is an Intrusion is very much clear. Now the next question could be what the Intrusion detection & prevention system is? For this, Detection implies: 'to Monitor' & Prevention implies: 'to Block'.

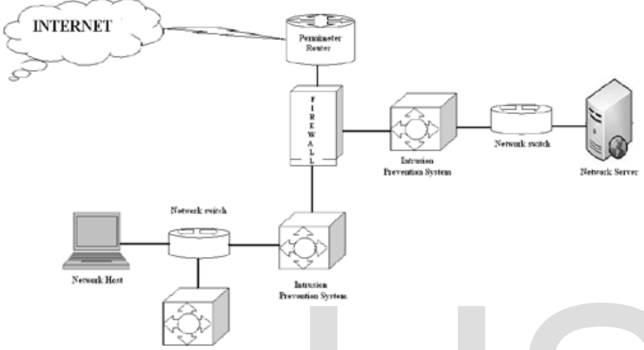

Fig.5: Intrusion detection & prevention system

A system which facilitates computer system (s) and a network in which it is connected to monitor the threats like viruses, malware, malicious attacks, etc and stop them from bringing in any unapproved action, such system is known as Intrusion Detection & Prevention System. In this system the process of Intrusion Detection is considered as a basic process which must be initialized first and Intrusion Prevention is next step to it.

5.1. Host Based Idps:

IDPS includes both detection and prevention process let us discuss them one by one with respect to host. HBIDS (Host Based Intrusion Detection System) uses software on a system through which it keeps an eye on suspicious processes. Initially this software is set on the system to supervise it by making use of log files/auditing agents as a source of data to be monitored. Like, NIDS (Network Intrusion Detection System) it provides protection on LANs but is more versatile than NIDS
Moving towards HIPS (Host Intrusion Prevention System) or HBIPS (Host Based Intrusion Prevention System) is a system rather program developed to protect single computer system called Host to resist viruses and internetwork malware. This system does not make use of patterns /virus signature to detect threats rather it keeps a track of trusted programs [8]. A program that exceeds its permission is obstructed from carrying out any unapproved act.

5.2. Network Based Idps:

Network based Intrusion Detection and Prevention Systems: Network based Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network and tries to detect malicious activity such as DoS attacks, port scans by controlling network traffic. [11]Ideally all inbound and outbound traffic would be scanned; however doing so might create a bottleneck that would impair the overall speed of the network. NIDS capture the network traffic from the wire as it travels to a host. Number of sensors are used to sniff the packet on t he network which are designed to monitor the traffic of the network. If any suspicious or anomaly activity occurs then the alarm is triggered and the message is sent to the administrator which generate an automatic response. [8].
Network-based systems are designed to work in a distributed environment and uses signature based and anomaly based intrusion detection techniques. IPSs is considered to be the evolution of intrusion detection system but the difference is IPS are placed in-line at the time intrusions detected and can block or prevent the traffic from the trespassed IP address or can reset the connection.

5.3. Wireless Idps:

A wireless IDPS checks on the wireless network traffic and calculate its network's protocols to detect the problematic activity and protocols. Wireless IDS, initially tests IEEE 802.11 a, b, g and I protocol communication and detects attacks, misconfiguration & policy violation at WLAN protocol level. Corporation and Institutions systems should use WIDP product having combination of various detection (mentioned above) to achieve correct detection. Detection criteria can be: Types of events detected, Detection accuracy, Timing & customization, Technology limitation. [SP800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)]
Wireless IPS's prevention is done through sensor which provides two prevention capabilities for: Wireless & Wired network. As we are discussion Wireless IDPS, Let's move on with it. In these networks, some sensors in wireless network can end connection link between rogue STA and an authorized node or vice versa. It takes place by directly informing the end users to disconnect the present session. Also, sensor can deny establishing new connection

5.4. Network Behavior Analysis(NBA):

NBA continually monitors the traffic from an unusual event. NBA has capability to detect several types of malicious activities and generate an alarm to an activity. To analyze the flow of the network some stateful protocol analysis technique are used with network behavior analysis. Signature based detection is usually used by the administrator manually for essential signature to detect or prevent specific thread, most of the Network behavior analysis technologies do not make use of the signature based detection .Some sensors are used to monitor network traffic directly similar to network-based IDPS sensors who sniff the packet on the network to monitor the traffic of the network directly , some sensors do not monitor the traffic directly instead they relay on the information provided by the router and other networking devices. Most of the inline NBA sensors offer firewall capability that is used to drop or reject doubtful network activity.

6 Important analysis

Table 1: Analysis of various intrusion detection & prevention methods

Lit. ref.	Schem e	Type	Method	Approach	Anomaly Detection / Prevention	Signature Detection / Prevention	Disadvantages	Advantages
[1]	IDPS	HIDPS and NIDPS	Signature based and anomaly based	Peer to peer	Yes	Yes	Memory and Implementation issue	Reliable trusted and efficient
[2]	IDPS	HIDPS and NIDPS	Signature based	Sequence matching, malicious matching	No	Yes	Unable to detect and respond to anomaly behavior	Automated response to malicious attacks
[3]	IDPS	HIDPS and NIDPS	Signature based and anomaly based	In-source and out-source	Yes	Yes	Well trained analysts are required	Secured infrastructure
[4]	IDPS	HIDPS and NIDPS	Signature based and anomaly based	Operating system and Application level approach	Yes	Yes	Cost ineffective, implementation, updating, monitoring issues	Automatic response, reduce human effort
[5]	IDPS	HIDPS and NIDPS	Signature based and anomaly based	Network layer to application layer level	Yes	Yes	High rate of false positive, well trained analysts are required	Flexibility of customize, Cost effective
[6]	IDPS	HIDPS	Signature based and anomaly based	Secure mobile agent	Yes	Yes	Security of mobile agent, needs to adopt some other techniques	Real time response, reduce human effort
[7]	IDPS	HIDPS	Signature based and anomaly based	OS and Application level approach	Yes	Yes	A large amount of memory is requires	Strong detection and protection mechanism

7. Conclusion

As one and all are familiar with; IT Companies develop more and more each day. Along with these developments, attackers find new traditions to hazard. To follow the attackers, more ways are invented to prevent this intrusion. The paper presented is a strong on the subject of how to make intrusion detection system preserve attack against itself. It is the paper in which we discussed the nature of attacks that the system could be subjected to, what techniques have to be made about these attacks and how the system counteracts them. In this study of Intrusion Detection & Prevention System (IDPS), we Describes the main features of several IDPs systems/platforms that are currently available in a concise manner. The presented information constitutes an important point to start for addressing Research & Development in the field of IDS.

In future, a scheme that works on the further comprehensive span may be capable of detecting scattered attack a complete commune. Explanation of such a system would be an important involvement to the study and implementation of intrusion detection

REFERENCES

[1.] Ramaprabhu Janakiraman, Marcel Waldvogel, Qi Zhang. Indra: A peer-to-peer approach to network intrusion detection and prevention, Enabling Technologies: Infrastructure for Collaborative Enterprises, WET ICE 2003.

[2.] Harley Kozushko. Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems, (2003).

[3.] Intrusion Detection and Prevention In-sourced or Out-sourced, SANS Institute (2008).

[4.] Ahmed Patel, Qais Qassim, Christopher Wills. A survey of intrusion detection and prevention systems, Information Management & Computer Security Journal (2010).

[5.] Host Intrusion Prevention Systems and Beyond, SANS Institute (2008).

[6.] Muhammad Awais Shibli, Sead Muftic. Intrusion Detection and Prevention System using Secure Mobile Agents,IEEE International Conference on Security & Cryptography (2008).

[7.] Oludele Awodele, Sunday Idowu, Omotola Anjorin, and Vincent J. Joshua, A Multi-Layered Approach to the

[8.] Design of Intelligent Intrusion Detection and Prevention System (IIDPS), Babcock University, (Volume 6, 2009).

[9.] Usman Asghar Sandhu [1+], Sajjad Haider [2], Salman Naseer [3], Obaid Ullah Ateeb [4], A Survey of Intrusion Detection & Prevention Techniques, [1,2]Shaheed Zulfiqar Ali Bhutto Institute of Science & Technology, Islamabad. (SZABIST) University of the Punjab Gujranwala Campus, vol.16 (2011).

[10.] Sheetal Thakare, Pankaj Ingle, Dr. B.B. Meshram, IDS: Intrusion Detection System the Survey of Information Security, VJTI, Matunga, Mumbai, Volume 2, 2012.

[11.] Vera Marinova-Bonchev, A Short Survey of Intrusion Detection Systems*, Institute of Information Technologies, 1113 Sofia (2007).

[12.] Chirag Modi, Dhiren Patel, Hiren Patel, Bhavesh Borisaniya, Avi Patel, Muttukrishnan Rajarajan, A survey of intrusion detection techniques in Cloud, Centre for Cyber Security Sciences, City University London EC1V 0HB, (2012).

[13.] Karen Scarfone, Peter Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), Recommendations of the National Institute of Standards and Technology (2007).

[14.] Varun Chandola, Arindam Banerjee and Vipin Kumar, University of Minnesota, Anomaly Detection: A Survey, University of Minnesota (2009).

[15.] Malik Datardina, Intrusion Detection Systems, ACC 621: IT Assurance & Computer Assisted Auditing,(2010).

[16.] Yeubin Bai, Hidetsune Kobayashi. Intrusion Detection Systems: technology and Development, 17th International Conference of Advanced Information Networking and Applications, (AINA 2003)

[17.] Hao Bai[1],Kunsheng Wang[2],Changzhen HU[1],Gang Zhang2,Xiaochuan Jing[2], Boosting performance in attack intention recognitation by integrating multiple techniques,[1]School of computer science and technology, Beijing Institute Of Technology,[2]China Aerospace Engineering Consultation Center, Beijing, China (2010).

[18.] Dinesh Sequeira,Intrusion Prevention System Security Silver Bullet, version 1.4B (2002)

Mitali Mittal: pursuing M.Tech from Sagar Institute of Research & Technology, Bhopal (M.P.). Studied B.E. IT at Sri Satya Sai Institute Of Science & Technology, Bhopal (M..P.). She is interested in Cloud Computing, Network Security, Green Computing and Data Mining.

Alisha Khan Alisha Khan, Studied B.E. IT at TRUBA Institute of Engineering & Information Technology, Bhopal (M.P.).Asst Prof in IT Department at Radharaman Engineering College, Bhopal (M.P.). She is interest in Network security, Computer Network, Human Interaction Computing and Artificial Intelligence.

Chetan Agrawal studied M.E: CSE at TRUBA Institute of Engineering & Information Technology, Bhopal and Studied B.E. CSE at BANSAL Institute of Science & Technology, Bhopal. He is Asst. Prof. in CSE Department at Radharaman Institute of Technology & Science., Bhopal, M.P. India. He is interested in Network Security, Cyber Security, Wireless Network and Data mining.