Detecting Network Anomalies using IP Gray Space Analysis and Preventing from it by using Machine Identification Code

Sandip S. Patil
Assistant professor
Department of Computer Engineering
SSBT's College of Engineering & Technology
Bambhori ,Jalgaon(M.S)

Nitin Y. Suryavanshi
Research Scholar
Department of Computer Engineering
SSBT's College of Engineering & Technology
Bambhori ,Jalgaon(M.S)

ABSTRACT
Security with the intranet and internet becomes the very important issue as the total business is going to migrate towards the e-business. Security is not just about keeping people out of your network but also provides access into your network in the way you want to provide it, allowing the people to work together. When we are going to give the access to the outside people there may be the risk of some mischief with the resources of the network. The most important thing is the information of the organization, and the external or the internal persons who are not having the permissions of accessing the information may access the organization information and may harm to the organization In Network Security concern network access control and security assurance is a major issue to secure the private or public network from abnormal user. In this paper we are presenting the design and implementation of HNADP model which is used to detect the anomalies using IP Gray Space analysis and preventing the network from such anomalies using MAC address filtering.

General Terms: Anomalies Detection System, Anomalies Prevention System, MAC Filtering, Processor ID, IP Gray Space

Keywords: Anomaly Detection and Prevention, IP Gray Space, MAC Address

1. INTRODUCTION
As network is having a very big and heterogeneous environment, many large and important applications are running at side by side on the network. To handle all these issues, the network security must consider the behavior of the out-side users from the internet which may cause the harm to the network and becomes anomalous users. The challenge of detection and prevention from anomalous host is accepted by anomaly detection and prevention system. [1]. we present a HNADP model which is used to detect and prevent the network anomalies using IP Gray Space analysis and MAC address filtering. This methodology is working in two phases first phase is identification phase and second phase is prevention phase. In identification phase it is detecting the abnormal behaviors using the concept of unassigned IP addresses viz Gray IP and in second phase it is preventing the network by using the concept of MAC address filtering.

1.1 Background and Motivations
Intrusion Detection technique is classified in to two categories one is signature based misuse detection and second is anomaly detection [2] [3]. In signature based misuse detection, attacks are signature based misuse detection approaches are strictly limited to the known abnormal users only. How to detect newly identified abnormal users by using specific tech is one of biggest challenged faced by signature or misuse detection [4]. To overcome this limitation of signature based misuse detection the concept of anomaly detection was introduced in the work of Denning [5]. According to Denning security violations could be detected by inspecting abnormal system usage patterns from the audit data. As reality most Anomaly Detection Techniques attempts to set up normal activity profiles by computing various metrics and an intrusion is detected when the actual system behavior davits from the normal profiles [3].Anomaly detection systems can observe activities that deviate significantly from the established normal usage profiles as anomalies. The main advantage of anomaly detection is that it does not require prior knowledge of intrusion and can thus detect new intrusions. But detecting any attack regardless of whether they are known or unknown with their potential behavior is the major challenge, which is not experienced in early IDS and ADS research. So to overcome these problems in signature based misuse detection and conventional anomaly detection system we are designing and implementing new network anomaly detection system which uses both IP gray space analysis and dominant scanning port identification heuristics (DSPI). Our HNADP system detects three categories of anomaly with their potential behaviors for the campus network and preventing the network which under consideration. In this paper we apply the novel notion of IP gray space analysis [1] to monitoring, identifying and tracking suspicious activities of anomalous host in a large area campus network and MAC address filtering for the prevention purpose.

1.2 Introduction to Network Anomaly
Anomaly is a behavior based system which detects normal and abnormal users in system anomaly detection system establishes baseline for all users and depends on it decides anomaly [9] .Network anomaly is an abstraction of existing intrusion detection techniques to the network level allowing us to simultaneously monitor the security of multiple nodes as well as the network infrastructure. Network anomalies typically refer to circumstances when network operations deviate from normal network behavior. The anomalies can arise due to various causes such as malfunctioning network devices, bad configuration in network services and operating systems, Network overload, malicious denial of service attacks, ill advised applications installed by users, high level users' effort to discover network and gather information about it and its devices These anomalous events will disrupt the normal behavior of some network data [6] [7].

1.3 Introduction to IP gray space and IP active space analysis

Campus or enterprise networks often have many unassigned IP addresses that collectively form IP gray space within the address blocks of such networks [1][8]. In network there are number of IP Addresses all these addresses are called as IP space that IP space is divided into two address blocks one is IP gray space and other is IP active space. All IP addresses are not likely to be assigned to "active" hosts (i.e., actual machines such as servers, desktops, lap- tops, etc.) at any give time period. We refer to these IP addresses within the campus network that are not assigned to any host throughout a given time period, say, an hour or a day, as "inactive" or gray IP addresses. In contrast, the IP addresses within the same address blocks that are assigned to hosts at any point within the time period are referred to as active IP addresses. The inactive IP addresses collectively forms IP gray space [1] within the address blocks, while active addresses the active space. By definition, IP gray and active space within a campus or any network are time dependent in other words, they are not fixed and vary over time.

In IP Gray space analysis we will identify IP gray space if any outside host if try to access that gray IP address we will trap him/her and after trapping he/she will be the anomalous host in our campus network.

1.4 IP Gray Space Identification

Let I denote the collection of all IP addresses of a network under consideration, and t0 the starting time of a time period of interest, and T the length of the period. We say an (inside) IP address $g \in I$ is a gray (or inactive) address over the time period [t0, t0+T] if and only if no traffic originating from g is observed , during [t0-Ť, t0 +T + Ť] for some fixed Ť. We use G to denote the collection of all gray IP addresses within the time period, or IP gray space. The Complementary set, A = I -G, is referred to the active space. In other words, for any $a \in A$, there is traffic originating from a at some time during [t0-Ť, t0 +T + Ť] thus a is likely assigned to an active host during the time period. In this study, we set to be 24 hours, t0 the 0^{th} hour of a day, and Ť one hour.

1.5 IP Gray Space Characteristics

We apply the above heuristic to the PRTG Network Traffic Graphic at the router of our ADS client server network in our campus network.

Table 1: Gray IP and Active IP Database

	Source IP	Source Port	Destination IP	Destination Port	Protocol	Volume
1	SSPComputer (192.168.13.59)	137 (NETBIOS)	[192.168.255.255]	137 (NETBIOS)	UDP	8648 bytes
2	192.168.1.7	137 (NETBIOS)	[192.168.1.255]	137 (NETBIOS)	UDP	3036 bytes
3	[192.168.13.1]	137 (NETBIOS)	[192.168.255.255]	137 (NETBIOS)	UDP	2484 bytes
4	N/A	68	Broadcast (255.255.255.255)	67	UDP	2360 bytes
5	[192.168.111.17]	137 (NETBIOS)	[192.168.255.255]	137 (NETBIOS)	UDP	1320 bytes
6	[192.168.1.1]	67	Broadcast (255.255.255.255)	68	UDP	1264 bytes
7	192.168.255.21	138 (NETBIOS)	[192.168.255.255]	138 (NETBIOS)	UDP	1159 bytes
8	COMPUTER (192.168.55.15)	137 (NETBIOS)	[192.168.255.255]	137 (NETBIOS)	UDP	1104 bytes
9	[192.168.111.10]	138 (NETBIOS)	[192.168.255.255]	138 (NETBIOS)	UDP	675 bytes
10	192.168.13.29	137 (NETBIOS)	[192.168.255.255]	137 (NETBIOS)	UDP	644 bytes
11	[192.168.13.105]	138 (NETBIOS)	[192.168.255.255]	138 (NETBIOS)	UDP	450 bytes
12	192.168.13.29	138 (NETBIOS)	[192.168.255.255]	138 (NETBIOS)	UDP	432 bytes
13	CC15 (192.168.111.15)	137 (NETBIOS)	[192.168.255.255]	137 (NETBIOS)	UDP	368 bytes
14	[192.168.111.10]	137 (NETBIOS)	[192.168.255.255]	137 (NETBIOS)	UDP	368 bytes
15	[192.168.111.21]	137 (NETBIOS)	[192.168.255.255]	137 (NETBIOS)	UDP	330 bytes
16	[77.242.193.141]	443 (HTTPS)	SSPComputer (192.168.13.59)	2007	TCP	302 bytes

Since no traffic is observed to originate from a gray IP address to any outside host (in the rest of the Internet) for an entire day, it is likely that the address is not assigned to any live host during that day. Ideally one would expect no traffic from any outside host either. This is in general not true at all because external anomalous host doesn't know the active and gray IP space.

1.6 MAC Address Filtering and Processor Id Identification

It is a unique address assigned to almost all-networking hardware such as Ethernet cards, router etc. The MAC address is a unique value associated with a network adapter. MAC addresses are also known as hardware addresses or physical addresses. They uniquely identify an adapter on a LAN. MAC addresses are 12-digit hexadecimal numbers (48 bits in length).

The Medium Access Control (MAC) layer will encounter different protocols that are already deployed in the access points (AP) of the networks. The various types of MAC protocols can be classified in terms of their multiple access schemes. A MAC first provides procedures for detecting and accessing the available networks that the terminal can access, i.e., access. Then, the available resources in these various types of networks are modeled. MAC is based on a unified resource model. Each flow that is sent to the MAC layer is then served through the network that is most suitable for the QoS requirements of the flow, i.e., decision. Moreover, A-MAC provides QoS-based scheduling for multiple flows assigned to the same network, i.e., scheduling. As a result, the two-layer A-MAC exploits the available resources in the networks by providing procedures for serving multiple flows through multiple network architectures available to the terminal simultaneously[10][11]. Processor Serial Number (PSN): The CPUID Also called as processor id opcode is a processor supplementary instruction (its name derived from CPU Identification) for the x86 architecture. It was introduced by Intel in 1993 when it introduced the Pentium and SL-Enhanced 486 processors. MIC is unique Identification computer. PSN used for by application to identify processor & by extension, its system.[11]

Figure 1: Structure of MIC

2 PROPSED METHODOLY

In proposed methodology we are designing and implementing a HNADP model used to detect and prevent the network from anomalies this model will work in two phase

2.1 Phase-I Detection of Anomalies using IP Gray Space Analysis

This work involves the development of two step methodology naming as H-NADS Model for identifying and tracking anomalous hosts by correlating traffic towards both IP gray and active spaces of a campus network.

Step1. Identification of anomalous external host using IP gray space and relative uncertainty: In the first step we set an IP active threshold range that range is called as IP active space. Such a threshold setting is called as association rule generation [5] for supervised learning .If source IP Address of communication host is comes from IP Active Space then the respective communicating host is a normal user. In contrast if communicating host uses gray IP (not active IP) for communicating then he/she is an anomalous host. To implement this step we set up thresholds for IP Active Space (192.168.55.1 to 192.168.55.254) and IP gray space if any host crosses that threshold of IP active space the n he/she is an anomalous host. For that purpose we are calculating relative uncertainty (RU). Relative Uncertainty is standardized entropy which detects observational variety of any anomalous host.

Let Os be the set of outside hosts that we have to characterize for checking anomaly. For any h ∈ Os, let GF (h) denote the collection of gray flows generated by h. The destination ports (dstPrt in short) used by gray flows in GF (h) induce an empirical distribution, for each dstPrt i, pi: = mi=m where mi is the number of gray flows in GF (h) with dstPrt i, and m is the total number of gray flows in GF (h), m = | GF (h)|. Entropy is the measurement of the observational variety in the observed values of any variable X [9]. It is denoted by H(X). Which is Entropy (empirical) of X. Uncertainty is a empirical probability p(xi) of any

variable x on a given time variably**.** To understand it, consider a random variable X that may take N_x discrete values. Suppose we randomly sample or observe X for m times, which induces an empirical probability distribution on X, Which is denoted as p (xi) = mi/m, xi ∈ X

Where mi is the frequency or number of times we observe X taking the value xi.

The (empirical) entropy of X is then defined as

$$H(X) = -\sum_{xi\in X} p(xi)\log p(xi) \qquad (1)$$

Standardized entropy below referred to as relative uncertainty (RU) which provides an index of variety or uniformity regardless of the support or sample size:

$$RU(X) = \frac{H(X)}{H\max(X)} \qquad (2)$$

We apply information theoretical metric Relative Uncertainty (RU) or standardized entropy defined below to the destination port distribution of h to identify dominant scanning (destination) ports (if they exist). So from equations (1) and (2) we get RU for destination as well as server port

$$RU\,(dstPrt) := -\sum_{i\in dst\,Prt} pi \log pi \Big/ \log m \qquad (3)$$

Step2. Identification of category of Anomaly using dominant scanning port (DSPI)

In this step we identify five categories of anomalies using their dominant scanning port (DSP). DSP is the foreign port and port service used by scanning flaws SF(h) of anomalous host for communication with internal host. From equation (3) we can define RU (SrcPrt), for source port (srcPrt) distribution of GF (h). Hence RU (srcPrt) and RU (dstPrt) allows us to determine the existence of dominant scanning port in the gray flaws of an outside host of the campus network.

Phase-I : HNADP Anomaly Detection Algorithm

Parameters GF (h), β=βo;
Initialization: DSP: =Ø;
Compute pro dist. Pprt and ϴ:= RU(prt) from GF(h);
While ϴ ≤ β and |GF (h)| >= 10 do
  Find prti with highest Pprti
  DSP: =DSP ∪ prti
 Remove flaws associated with prti from GF (h)
  Remove Pprti from Pprt;
  Compute ϴ: = RU (prt) from GF (h)
End While

Types of anomalies detected using DSPI algorithm

Bad Scanner-I, Bad Scanner-II, Bad Scanner-III , Focused Hitters and Mixed Intruders Anomaly

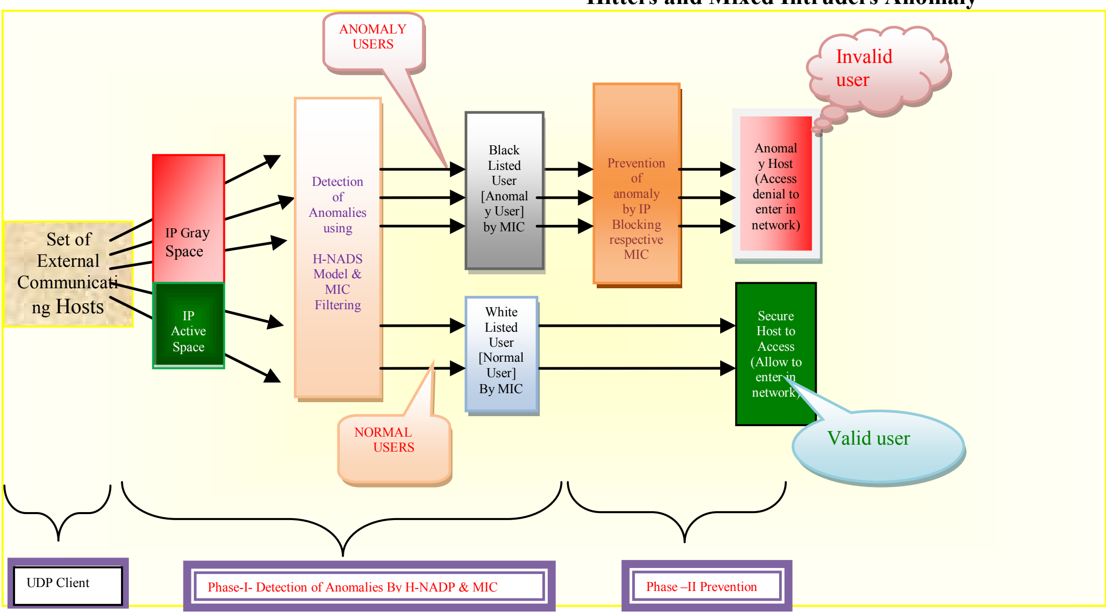

Figure 2 Conceptual views of H-NADPS

2.2 Phase-II-Prevention of Network from Anomalies using MIC

This phase processed the result of first phase. Once HNADP model detect network anomalies then the working of this phase starts. If any anomalous host interfaces out defended network then it becomes necessary to protect the network from such users. In this phase the model will captures the MAC address and Processor-ID of each outsider interfacing host and by using that knowledge this phase will deny all services of anomalous host by masking the source IP of given anomalous host .

Phase 2: HNADP Prevention Algorithm

1. Client type one code which shown on screen (i.e. Processor Serial number) used as CAPTCHA. Which indentified that user is human not a dummy program.
2. Send that code to the server.
3. Server accept that that packet in the form of UDP and analyze as existing work store in Input table.
4. In detection and prevention
   IP & its associate machine code Id are verified by using White table
   a. If communicated IP and Associated MIC in white table to allow the access.
   b. If IP is matched but its associated MIC not match with white List then give message as invalid user & IP snooper & Make entry in black list of MIC
   c. If IP is not in White List or not active IP but MIC in White List, it treated as masking user and denies access.
   d. If MIC & IP is not white list & its active IP Then It is new user Administrator decided the action
      Added to White List & allow the access
      Else add in Black List to deny the access.

3 IMPLEMENTATION

To implement our designed two step methodology we construct an HNADP Model (Hybrid Network Anomaly Detection and Prevention Model), which detects anomalies with their potential behaviors and prevent the network from such users

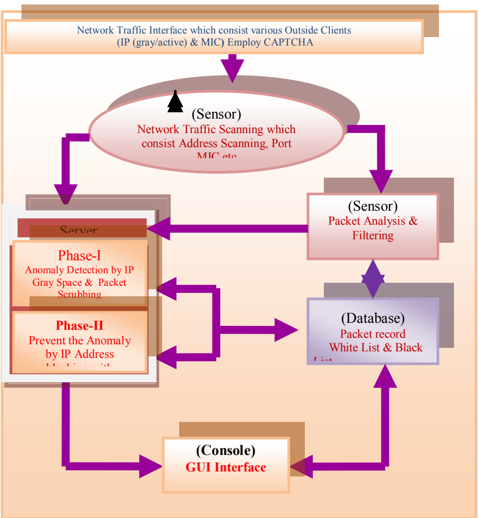

Figure 3: HNADP Model

Working of H-NADS Model**:** H-NADS Model interfaces with external host using ADS Client Interface. After this ADS Server will compare all the traffic with IP gray space and DSPI. Using this comparison this model detects various anomalies and Prevents using MAC address and Process Id.

4 RESULTS AND DISCUSSION

In result we identified various anomalies using IP Gray Space and prevent the network using MAC Address Filtering and Processor ID.
In External Host Interface we are using CAPTCHA Turing Test for the identification of human and machine

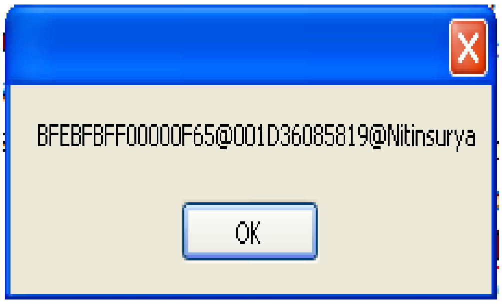

Figure 4: MIC send to server

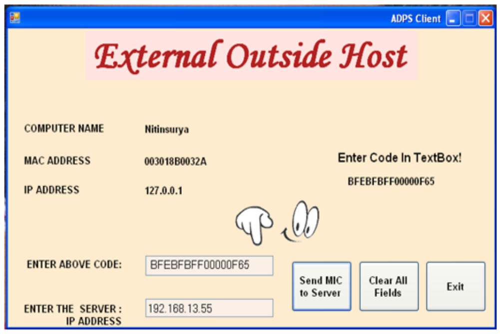

Figure 5: Snapshot of CAPTCHA based Host Interface

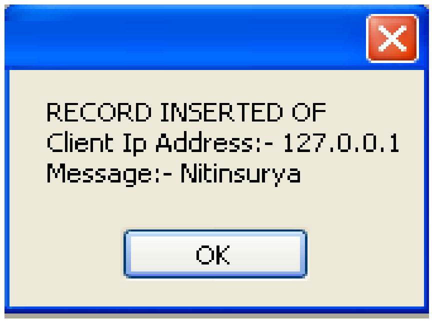

Figure 6: Record inserted in server database

Figure7: Detection & Prevention

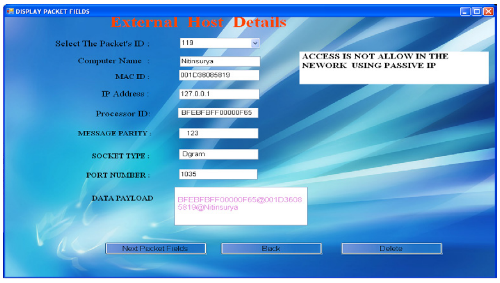

Figure 8: Prevention from Anomaly

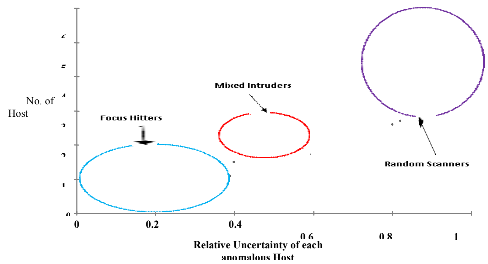

Figure 9: Graphical Analysis of all detected anomalies

Table : Sample Result

Packet ID and Source IP Address (Gray/Active IP)	**DSP**	Socket Service	**RU**	**Type of Anomaly Detected**	**Γ**	**Behavior**	**Prevention Status**
69 192.168.13.59	25	SMTP	0.85	Bad Scanner-I	0.9	Highly Potential	Prevented
62 192.168.13.59	23	Telnet	0.75	Bad Scanner-II	1	Highly Potential	Prevented
58 192.168.15.3	445	MS DS	0.65	Bad Scanner-III	1	Highly Potential	Prevented
72 192.168.22.66	53	DNS Lookup	0.14	Focus Hitter	0.2	Potential	Prevented
61 192.168.13.59	1086	Dgram	0.24	Mixed Intruder	0.5	Average	Warning Signal
91 192.168.55.3	2034	Dgram	00	Normal	00	Normal	no action

5 CONCLUSIONS AND FUTURE WORK

Anomaly detection is a major issue in network security, so by considering this myth we develop and implement a two phase approach for

Identifying and preventing from anomalous host by considering IP Gray Space and MAC Address Filtering. Using this methodology we identify and prevent from five types of anomaly hosts with their three behaviors and obtained some sample results in the form of table and graph.

In future we will try to capture more number of anomalies with advanced prevention technique.

6 REFERENCES

[1] Yogendra Kumar JAIN, Sandip S. PATIL "Design of Hybrid Network Anomalies Detection System (H-NADS) Using IP Gray Space Analysis" International Journal of Informatica Economică vol. 13, no. 2/2009 110

[2] K. Jackson, Intrusion Detection Systems (IDS): Product Survey, Los Alamos National Laboratory,

[3] H. Debar, M. Dacier, and A. Wespi, Towards a Taxonomy of Intrusion Detection Systems, Computer Networks, 31(8):805-822, April 1999[4] Wei Lu, Mahbod T. and Ali A." Detecting Network Anomalies Using Different Wavelet Basis Functions", Communication Networks and Services Research Conference 978-0-7695-3135-9 IEEE August, 2008 .

[4] Wei Lu, Mahbod T. and Ali A." Detecting Network Anomalies Using Different Wavelet Basis Functions", Communication Networks and Services Research Conference 978-0-7695-3135-9 IEEE August, 2008

[5] D.E.Denning , "An Intrusion Detection Model." IEEE Transactions on software engineering , 2:222

[6] Y.Yasami,M.Farahmand,V.Zargari "An ARP-based Anomaly Detection Algorithm Using Hidden Markov Model in Enterprise Networks", (ICSNC 2007),IEEE 2007.

[7] Gaia Maselli , Luca Deri , Stefano Suin , "Design and Implementation of Anomaly Detection System"2007

[8] Y. Jin, G. Simon, K.Xu, Z.-L. Zhang and V. Kumar, "Gray's Anatomy: Dissecting Scanning Activities Using IP Gray Space Analysis". In Proc. of SysML'07, 2007

[9] Xiuyao Song, Mingxi Wu, Christopher Jermaine, and Sanjay Ranka" Conditional Anomaly Detection", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 19, NO. 5, MAY 2007

[10] Giulia Bruno, Paolo Garza, Elisa uintarelli, Rosalba Rossato," Anomaly Detection in XML databases by means , IEEE July 2007

[11] Ricardo C. Carrano, Luiz C. S. Magalhães, Débora C. Muchaluat Saade and Célio V. N. Albuquerque "IEEE

802.11s Multihop MAC: A Tutorial" , IEEE 802.11S MULTIHOP MAC: A TUTORIAL 53 IEEE 2011

7. AUTHORS PROFILE

Sandip S. Patil Working as Assistant Professor in Department of Computer Engineering SSBT's College of Engineering & Technology Bambhori, Jalgaon (India). Received the B.E. degree in Computer Engineering, in 2001 from SSBT's College of Engineering and Technology, Bambhori, Jalgaon affiliated to North Maharastra University Jalgaon(MH) , M.Tech. in Computer Science and Engineering from Samrat Ashok Technological Institute Vidisha affiliated to Rajiv Gandhi Technological University, Bhopal (M.P.), in 2009, & Pursuing PhD in Computer Sci & Engg. His research focus includes developing network security applications for the detection of suspicious abnormal behaviors.

Nitin Y. Suryavanshi received the B.E. degree in Computer Science & Engineering, in 2005 from MBES's College of Engineering ,Ambajogai, Dist: Beed affiliated to DR. Babasaheb Marathwada University Aurngabad , Pursuing M.E. In Computer Science and Engineering from from SSBT's College of Engineering and Technology, Bambhori, Jalgaon affiliated to North Maharastra University Jalgaon(MH) His research focus includes developing network security applications for the detection & Prevention of suspicious abnormal behaviors.