International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-2, July 2020

Diverse Methods for Signature based Intrusion Detection Schemes Adopted

Jyoti Snehi, Abhinav Bhandari, Vidhu Baggan, Manish Snehi, Ritu

Abstract: Intrusion Detection Systems (IDS) is used as a tool to detect intrusions on IT networks, providing support in network monitoring to identify and avoid possible attacks. Most such approaches adopt Signature-based methods for detecting attacks which include matching the input event to predefined database signatures. Signature based intrusion detection acts as an adaptable device security safeguard technology. This paper discusses various Signature-based Intrusion Detection Systems and their advantages; given a set of signatures and basic patterns that estimate the relative importance of each intrusion detection system feature, system administrators may help identify cyber-attacks and threats to the network and Computer system. Eighty percent of incidents can be easily and promptly detected using signature-based detection methods if used as a precautionary phase for vulnerability detection and twenty percent rest by anomaly-based intrusion detection system that involves comparing definitions of normal activity or event behavior with observed events in identifying the significant deviations and deciding the traffic to flag.

Keywords: Intrusion detection system (IDS), Signature Based IDS, Anomaly Based IDS.

I. INTRODUCTION

IDS (Intrusion Detection System) is a hardware and software system that automatically detects and reacts to attacks on computer systems and maintains security, availability and confidentiality. Cyber criminals across the globe are taking advantage of insecurity and stealing information in unsecured networks.Because firewalls and anti-malware software alone are not sufficient to prevent internal threats, and multiple methods of intrusion detection are used to protect a whole network from any attack. Intrusion detection attacks may occur in the form of Denial-of-Service (DOS) attacks, i.e. attacks such as flooding and fault manipulation, eavesdropping, spoofing or root user (U2R), misuse of logons and applications.

Manuscript received on May 25, 2020.
Revised Manuscript received on June 29, 2020.
Manuscript published on July 30, 2020.
* Correspondence Author
Jyoti Snehi, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India
Abhinav Bhandari, Department of Computer Science and Engineering, Panjabi University, Patiala, India
Vidhu Baggan, Engineering Department, Infosys Limited, Chandigarh, India
Manish Snehi, Engineering Department, Infosys Limited, Chandigarh, India
Ritu, Engineering Department, Infosys Limited, Chandigarh, India

An intrusion detection system (IDS) functions as a computer network protection system, a central component for safeguarding and protected applications designed to automatically alert computer administrators when someone attempts to access the information system by malicious activities.

A Passive Intrusion Detection System detects incoming threats, notifies them and helps detect external and internal threats. IDS support by monitoring changes in network behavior, inspecting system operation, distinguishing between normal and abnormal activities with a restriction that often gives false alarms, takes time and is not 100% safe from attacks. DS feature includes device running without human interference, fault tolerance, self-recovery in case of system crash. Subversion resilience, performance, identification of deviations from normal behavior, scalability, adaptability, power and ease in attack detection and reusability.[1][2][3]

Types of intrusion detection systems are classified according to different factors depending on the deployment platform for detecting attacks and the input data obtained from various resources such as system calls, application phase, network traffic, audit logs, device and user activities.[2]

A. IDS Methods based on Deployment:

Based on deployment platform used, an IDS method can be divided into following categories:

a) HIDS: Host-based Intrusion Detection Systems are used for protecting the integrity of the device by gathering information from the server and processing the information in the form of operating system logs to identify unwanted activities and reporting it immediately to the network manager about the possibility of altering system behavior. [7]
b) NIDS: Network-based IDS detects intrusions such as Denial of Service attacks, port scanning attacks, etc. by capturing network traffic and analyzing data by collecting network packets, defining their relationship with all known threat signatures and comparing user activity in real time with already identified attacks. [7]
c) Hybrid Detection: Combines Host based and Network based IDS.[7]

B. IDS Methods based on Detection

There are different types of Intrusion Detection systems based on type of detection employed or the techniques applied which are listed below:

1. Knowledge/Signature/ Misuse detection techniques:

Misuse detection strategies classify all identified threats by evaluating their patterns of attack, matching them to a signature list and comparing them to identified signatures. Based on the comparison of system operation to a predefined sequence of events representing a known attack and therefore signature can be interpreted as a given set of rules/patterns relevant to known attacks.

2. Anomaly or Behavior detection techniques:

Anomaly based detection is intended to catch any behavior based on the assumption that misuse or intrusive behavior deviate from usual pattern and will be considered as intrusion. Anomaly detection has the capability to detect unknown attacks and it has ability to produce high amount of false alarms.[4]Our research paper is organized as Section I. presenting introduction about IDS and its types. Section II. consists of Signature based IDS methods, their types, description and advantages. It further explains limitations of Signature based methods and Section III. presents the conclusion of the research paper.

II. SIGNATURE BASED IDS METHODS

Signature-based/Profile-based/Misuse-basedIDS consists of four components as depicted in Figure 1.The first step involves performing intrusion detection by collecting the network packets and then analyzing them. The second component immediately drops those packets and checks whether or not theycorrespond to the block table rules. Packets that have no autonomous element manager and have autonomous coordinator to those rules are forwarded to warning clustering module and it generates warning for suspicious packets. The third part blocks the packets that are suspicious and sends warnings to other IDSs. The fourth step gathers warnings and makes packet decisions. By deploying the numerous Signatures based IDS as defined in Table 1we can protect all the devices from asingle point of failure attack.

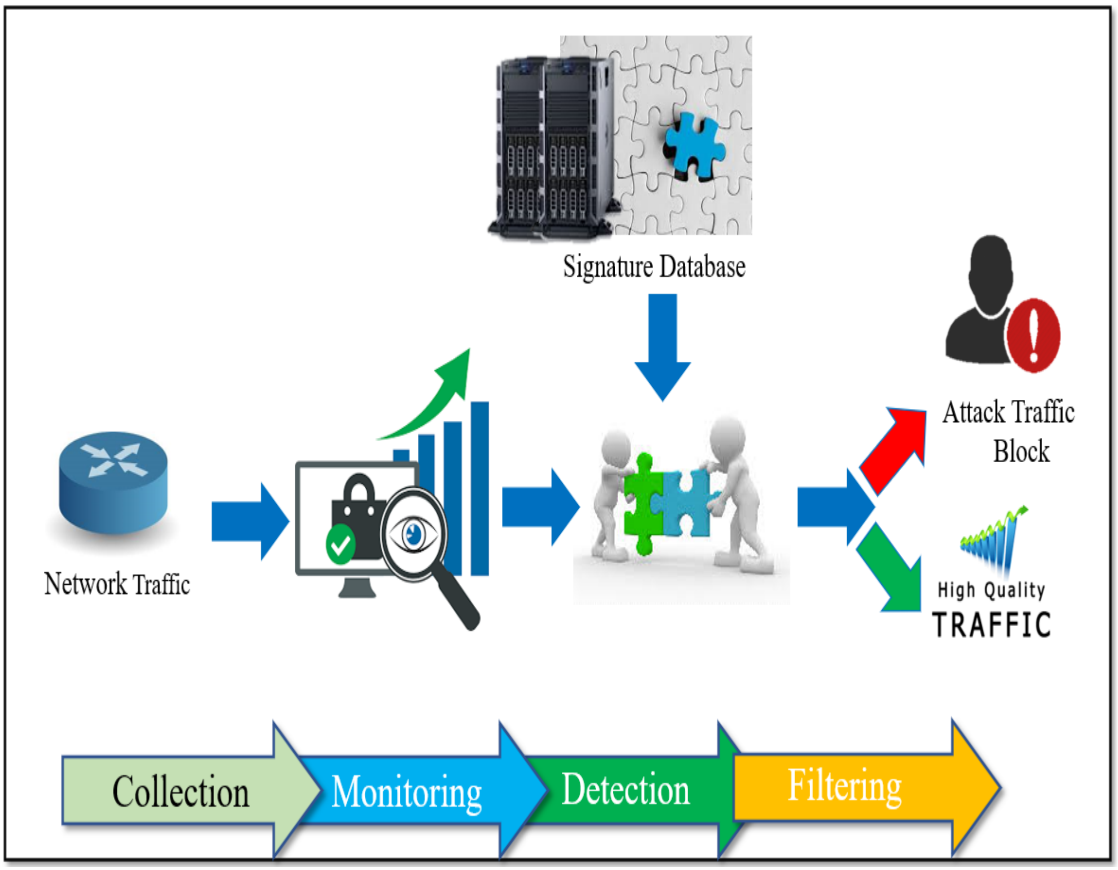

Figure 1: Methodology used in Signature based IDS

Table 1: Signature-based IDS Methods

S. No	Methods	References	Types	Detail	Significance
1.	Network Behavior based IDS Approach	[5] [6]	• NBA (Network Behavior Analysis) • DM (Detection method)	NBA tracks and manages network traffic to identify network-related inbound and outbound traffic to ensure all the vulnerabilities that result in unusual traffic flows, such as DDOS attacks, malware, and policy violations. DM detects intrusion into individual networks, components consisting of Sensor, Administration Server and Storage Server.	• Hard to track by attackers. • Stressing overall network interface behavior. • Respond effectively to unknown or recognized threats which do not have a signature. • Good on zero-day attack detection. • Better screening of identification detections. • Restore DDoS and malware infections.
2.	Knowledge based IDS Approach	[7] [8]	• Finite State Machines • Description Languages • Expert Systems	This approach test network and host events against predefined rules/attack patterns. E.g. rule-based systems, ontology-based systems of analysis, Expert systems, logic-based systems, and State transfer systems are knowledge-based approaches.	• Safe and versatile. • High speed detection.
3.	Survey based IDS Approach	[6] [9] [10] [11]	• Pattern matching • Stateful pattern matching • Protocol decode based analysis • Fuzzy clustering	IDS can use a matching pattern algorithm to search the attack and malware signatures machine files. Creation of signature system and complete pattern matching-based analysis algorithm tests the existence of a signature in the incoming packet sequence and outputs the string position within the packet.	• Effectively process the great number of signatures
4.	Hierarchically Structured IDS Approach	[12]		This approach learns classes as a series of independent classification problems and integrates predictions through the use of class associations that define the hierarchy. The network is divided into cluster-headed clusters that detect attacks and can cooperate to form a global IDS with the central base station.	• Ensure greater precision compared to other approaches
5.	Virtual Switch based IDS Approach	[13]		By processing the network packets, it gathers records of incoming and outgoing traffic. If a large number of packets with the same IP addresses are detected, then the virtual server blocks those IP addresses.	• Secures VMs against DDoS attacks
6.	Clustering based Approach	[14] [7]	• Single link clustering algorithms • Squared error clustering • Hierarchical clustering algorithms	Clustering techniques work by grouping the observed data and assigning a collection of relevant dataobjects to classes called clusters. Theobjects in the same cluster are similar to each other and differ from the objects inother clusters. Clustering is used in extraction ofthe explorative data.	• Efficient for generating rapid response • Reduces computational complexity
7.	Feature Selection based Approach	[15] [16]	• Filter approach • Wrapper approach	Selection of features is an IDS preprocessing module and a method of selecting appropriate features and eliminating obsolete or redundant features from the original dataset, e.g. pattern recognition, machine learning, data mining and statistics.	• Reduce data input dimensions to a classifier or an IDS.

8.	Rule based Approach	[14] [10]		Rule-based structures are made up of conditional program statements known as rules with behavior performed if the conditions stated are met.	• Easy • Intuitive• • Less rigid and unstructured.
9.	Application based Approach	[17] [18]	• Application layers (Saas) • Physical layer Software Environment layer (Paas)	Application-based IDS monitor a particular framework designed specifically for the applications it protects to track and reliably detect malicious behavior.	• Has the ability to access encrypted data • Attribute unwanted user-specific behaviors.
10.	Classification-based Approach	[7]	• One-class classifiers • Semi-supervised classification • Decision trees	A classification can be defined as the problem of determining a new observation that belongs to a specific category set based on training data containing all observations, and whose membership categories are identified.	• Perform better. • Approaches Teaching and learning more flexibly. • Known assaults have a high detection rate.
11.	Data mining Techniques based Approach	[19] [20]	• Data Classification • Clustering • Association Rules	Data mining is the ability to take information as input, to arrange data sets, to classify patterns, to create relationships and to extract patterns using data analysis to gain information on that pattern. And variations with simple strategies which might not be possible.	• Data mining aims at removing the manual and ad hoc components used to build IDS
12.	Expert System based Approach	[21] [22] [23] [24] [25]	• framework-based expert systems • reasoning-based expert systems • the rule-based expert systems	Expert system is a programming language which uses a rule base to define activities and combines the data acquired with expert expertise and successful reasoning representing all documented breaches. They render integrated audit, logic, identification and control system to form a closed loop control system.	• Expert program uses a rule base that identifies behaviors that reflect documented breaches of security • Recognizes new attack instances and work speed
13.	Decision Tree-based Approach	[26] [27]		A Decision Tree is a hierarchical graph consisting of internal nodes that reflect a check on an attribute and branches because the check and the outcome of the leaf nodes imply a class mark. It analyzes the data and identifies characteristics that indicate malicious activities within the network. The classification algorithm is inductively learnt to build a model from the reclassified data set. For each element the values of the attributes are defined and classification can be interpreted as mapping from a collection of attributes to a particular class. The classification rules are generated by the path from the selected root node to the leaf. The tree is created by defining the attributes and their associated values.	• Assists in deciding on incoming and non-malevolent traffic. • Offers reasonable precision within acceptable time.

III. OBSERVATIONS

Most intrusion detection systems are based on signature and rely on using a preconfigured signature database to detect attacks and generate alarms. The intrusion event whose pattern / signature already exists in the network can be easily identified but it cannot recognize unknown and emerging threats. Signature-based detection is a process where a unique identifier about a known threat is created for future identification of the danger. IDS based on a signature is very effective in sniffing out documented attacks.

Limitations of Signature Based IDS are that sometimes Signature based detection cannot detect new intrusion or previously unknown attacks. If a form of attack doesn't suit a signature then the new attack will go undetected. Hence it is required to keep signature database wellupdated.Hackers can easily trick signature-based solutions by modifying the way an attack is made and having network access.The Processor load paid for the device that analyzes each signature depends on the database of the signature. The increasing the number of signatures that are searched for, the increasing the probability that more false positives will be found.

To address the limitation of anomaly-based signature detection IDS are implemented to detect the unknown malware attacks as new malware arrives daily. Unlike signature-based identification, behavioral analysis does not look for particular features of the individual hazard, instead it looks at the outcomes. This uses machine learning to build a model of trustful behavior, and everything that comes is compared with that model and is considered suspicious unless it is found in model. Anomaly based systems use IDS or Security Administrator generated profiles. These profiles helps in detecting the attack and generating alarms for traffic trends or device behavior that do not conform to a given profile Anomaly-based systems have a comparatively high rate of false positives as they produce warnings if there is a deviation from standard. It can be sometimes a difficult task to defining unusual traffic and operation.

IV. CONCLUSION

Considering the Pareto principle ("80/20 rule") Eighty percent of events can be easily detected by signature-based detection, and remains a technique of fundamental importance. Twenty per cent of the problems trigger eighty per cent of the problems. If any organizationundergoes focused behavioral research, the remaining twenty percent of the intrusion will be carried out.

REFERENCES

1. A. K. Saxena, S. Sinha, and P. Shukla, "General study of intrusion detection system and survey of agent based intrusion detection system," *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2017*, vol. 2017-Janua, pp. 417–421, 2017, doi: 10.1109/CCAA.2017.8229866.
2. N. Agarwal and S. Z. Hussain, "A Closer Look at Intrusion Detection System for Web Applications," *Security and Communication Networks*, vol. 2018, 2018, doi: 10.1155/2018/9601357.
3. A. Bhandari, A. L. Sangal, and K. Kumar, "Characterizing flash events and DDoS attacks - An Empirical Investigation," *International Journal of Applied Engineering Research*, vol. 9, no. 22. pp. 5968–5974, 2014, doi: 10.1002/sec.
4. W. Yassin, N. I. Udzir, Z. Muda, A. Abdullah, and M. T. Abdullah, "A Cloud-based Intrusion Detection Service framework," *Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012*, pp. 213–218, 2012, doi: 10.1109/CyberSec.2012.6246098.
5. C. Day, "Intrusion prevention and detection systems," *Managing Information Security: Second Edition*, pp. 119–142, 2013, doi: 10.1016/B978-0-12-416688-2.00005-2.
6. S. M. Othman, N. T. Alsohybe, F. M. Ba-alwi, and A. T. Zahary, "Survey on Intrusion Detection System Types," no. December, 2018.
7. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 1, pp. 303–336, 2014, doi: 10.1109/SURV.2013.052213.00046.
8. A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, 2019, doi: 10.1186/s42400-019-0038-7.
9. M. Aldwairi, A. M. Abu-Dalo, and M. Jarrah, "Pattern matching of signature-based IDS using Myers algorithm under MapReduce framework," *EURASIP Journal on Information Security*, vol. 2017, no. 1, 2017, doi: 10.1186/s13635-017-0062-7.
10. V. B. Salve, V. Savalkar, and S. Mhatre, "Efficient pattern matching algorithms in IDS," *Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018*, no. Icisc, pp. 1083–1089, 2018, doi: 10.1109/ICISC.2018.8398971.
11. W. Lee, "An Overview of Intrusion Detection Techniques," 2004, doi: 10.1201/9780203507223.ch48.
12. M. S. Islam Mamun and S. K. A.F.M, "Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network," *International Journal of Network Security & Its Applications*, vol. 2, no. 3, pp. 102–117, 2010, doi: 10.5121/ijnsa.2010.2307.
13. S. G. Kene and D. P. Theng, "A review on intrusion detection techniques for cloud computing and security challenges," *2nd International Conference on Electronics and Communication Systems, ICECS 2015*, no. May 2016, pp. 227–232, 2015, doi: 10.1109/ECS.2015.7124898.
14. M. R. Deshmukh, M. R. Deshmukh, and P. M. Sharma, "Rule-Based and Cluster-Based Intrusion Detection Technique for Wireless Sensor Network," vol. 2, no. June, pp. 200–208, 2013.
15. F. Zhang and D. Wang, "An effective feature selection approach for network intrusion detection," *Proceedings - 2013 IEEE 8th International Conference on Networking, Architecture and Storage, NAS 2013*, pp. 307–311, 2013, doi: 10.1109/NAS.2013.49.
16. K. Kumar, G. Kumar, and Y. Kumar, "Feature Selection Approach for Intrusion Detection System," *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, vol. 2, no. 5, pp. 47–53, 2013, [Online]. Available: http://warse.org/pdfs/2013/icceitsp09.pdf.
17. A. Ids and A. Ids, "Application and Signature - Based Ids."
18. M. Tiwari, "Intrusion Detection System," no. April, pp. 39–57, 2011, doi: 10.1142/9781848164482_0004.
19. K. S. Desale, C. N. Kumathekar, and A. P. Chavan, "Efficient intrusion detection system using stream data mining classification technique," *Proceedings - 1st International Conference on Computing, Communication, Control and Automation, ICCUBEA 2015*, pp. 469–473, 2015, doi: 10.1109/ICCUBEA.2015.98.
20. J. Ng, D. Joshi, and S. M. Banik, "Applying data mining techniques to intrusion detection," *Proceedings - 12th International Conference on Information Technology: New Generations, ITNG 2015*, pp. 800–801, 2015, doi: 10.1109/ITNG.2015.146.
21. G. A. Isaza, A. G. Castillo, and N. D. Duque, "An intrusion detection and prevention model based on intelligent multi-agent systems, signatures and reaction rules ontologies," *Advances in Intelligent and Soft Computing*, vol. 55, pp. 237–245, 2009, doi: 10.1007/978-3-642-00487-2_25.
22. J. Yu, P. Tian, H. Feng, and Y. Xiao, "Research and Design of Subway BAS Intrusion Detection Expert System," *Proceedings of 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference, IAEAC 2018*, no. Iaeac, pp. 152–156, 2018, doi: 10.1109/IAEAC.2018.8577262.
23. H. Yong and Z. X. Feng, "Expert system based intrusion detection system," *Proceedings - 3rd International Conference on Information Management, Innovation Management and Industrial Engineering, ICIII 2010*, vol. 4, pp. 404–407, 2010, doi: 10.1109/ICIII.2010.578.

24. I. Annals, “The March of IDES: The Advent and Early History of Intrusion Detection Expert Systems Jeffrey R. Yost, Charles Babbage Institute, University of Minnesota,” pp. 1–19, 2015.
25. Z. P. Jia, Z. L. Yao, and S. F. Liu, “An expert system for preventing and auditing intrusion,” *Proceedings of the 9th International Conference on Computer Supported Cooperative Work in Design*, vol. 2, pp. 852–855, 2005, doi: 10.1109/cscwd.2005.194297.
26. K. Rai, M. S. Devi, and A. Guleria, “Decision Tree Based Algorithm for Intrusion Detection,” *International Journal of Advanced Networking and Applications*, vol. 07, no. 04, pp. 2828–2834, 2016, [Online]. Available: https://www.researchgate.net/publication/298175900.
27. M. Kumar, M. Hanumanthappa, and T. V. S. Kumar, “Intrusion Detection System using decision tree algorithm,” *International Conference on Communication Technology Proceedings, ICCT*, pp. 629–634, 2012, doi: 10.1109/ICCT.2012.6511281.

AUTHORS PROFILE

Jyoti Snehi , received B. Tech degree in Computer Engineering from Kurukshetra University, India in 2002 and received her M. Tech degree in Computer science and Engineering from Dr. B.R. Ambedkar NIT, Jalandhar, India in 2013 She is perusing her Ph.D. degree in Computer Engineering from Punjabi University, Patiala, India. She is working as Asst. Professor in the Department of Computer Science & Engineering, Chitkara University Institute of Engineering & Technology, Chitkara University Punjab, India since 2009. She has strong background of teaching in PDM University and Lingayas University Faridabad in past. For more information, reach her at Jyoti.snehi@chitkara.edu.in

Dr. Abhinav Bhandari, has done B. Tech in Computer Science and Engineering from G.T.B.K.I.E.T., Malout in 2001. He completed his M. Tech in Computer Science and Engineering from D.A.V.I.E.T. Jalandhar in 2008 and Ph. D. from Dr. B.R. Ambedkar NIT Jalandhar in 2017.

He has worked as a Lecturer in Lala Lajpat Rai Institute of Engineering and Technology, Moga, Punjab from 2001 to 2008, as an Assistant Professor in Lala Lajpat Rai Institute of Engineering and Technology, Moga from 2008 to 2012. He is currently working as an Assistant Professor, Department of Computer Science and Engineering, Punjabi University, Patiala since 2012. For more information, reach him at bhandarinitj@gmail.com

Dr. Vidhu Baggan, graduated at Beant College of Engineering & Technology and completed her Master’s Degree at NITTTR, Chandigarh. She did her Ph.D. from Chitkara University, Punjab, India.She has a teaching experience of more than 18 years. At present, she is Associate Professor in the Department of Computer Science & Engineering, Chitkara University Institute of Engineering & Technology, Chitkara University Punjab. In addition, she is certified as a Microsoft Certified Professional (2004), Cisco Certified Network Associate (2005 & 2016), Huawei Certified Network Associate (2018) and Huawei Certified Instructor (2018). She has many research publications to her credit. Her core interest areas are domains of networking. Her areas of interest include Computer Networks, Software Defined Networking and Cloud computing.

For more information, reach her at vidhu.baggan@chitkara.edu.in.

Mr. Manish Snehi received his bachelor degree in Computer Engineering from Kurukshetra University, Kurukshetra, India in 2002 and received Master of Science (M.S.) degree in Software Systems from Birla Institute of Science and Technology (BITS), Pilani, Rajasthan, India in 2005. He is perusing his Ph.D. degree in Computer Engineering from Punjabi University, Patiala, India. He is working as Senior Technology Architect in Infosys Limited, Chandigarh, India and has an extensive experience in Information Security, Web-Security and Internet of Things domains. For more information, reach him at: snehi.manish@gmail.com

Ms. Ritu completed her B. Tech from Vaish College of Engineering and ME in Computer Science and Engineering. She is pursuing Ph.D. in Computer Science and Engineering from Punjab Technical University.

At present, she is working as an Assistant Professor in the Department of Computer Science & Engineering, Chitkara University Institute of Engineering & Technology, Chitkara University Punjab. For more information, reach her at ritu.rathee@chitkara.edu.in