International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 6, November - December 2015 ISSN 2278-6856

ANALYTICAL STUDY ON INTRUSION DETECTION AND PREVENTION SYSTEM

***Sonal Paliwal[1], Rajesh Shyam Singh[2] , H.L.Mandoria[3]**

[1]Department of Information Technology
G. B. Pant University of Agriculture & Technology, Pantnagar, India

[2]Department of Information Technology Assistant Professor
G. B. Pant University of Agriculture & Technology, Pantnagar, India

[3]Professor and Head of Information Technology
G. B. Pant University of Agriculture & Technology, Pantnagar, India

ABSTRACT

This paper presents a review of intrusion detection and prevention system. With the day by day increasing amount of network throughput and security threats, the study of intrusion detection and prevention system (IDPs) has received a lot of attention all through the Information Technology field. Today viruses, worms, and several other invading malicious codes and programs proliferate widely on the Internet. With the environment becoming increasingly hostile, networks are easy targets because the infection can spread across the network rapidly.The current IDPs posture, challenges are on not only the intrusion detection and prevention from the fake intruders, but also the throughput of the system and to monitor the huge network traffic. Through there are number of existing literatures to IDPs, we attempt to give a more elaborate image for a comprehensive review. In addition, with some tables and figures we brief in the content.

Keywords: Intrusion, IDPs, Misuse Detection ,Anomaly, Hybrid system, Stateful Protocol Analysis ,Network Behaviour Analysis

1.INTRODUCTION

Intrusions are the activities that violate the security policy of system. Intrusion Detection and prevention is the process used to identify intrusions and prevent them from occurring.Intrusion detection and prevention system are contraption that monitor network and system activities for malicious activity. The main function of these systems is to identify the malicious activity maintain a log about this activity and stop or block it. They simply aims to detect and stop attacks.

Most IPS products strongly resemble firewalls. However, they usually include algorithms to perform more sophisticated traffic inspection and to operate at the application layer in addition to performing classic network and transport processing. James Aderson paper (1980) ‘Computer Security Threat Monitoring and Surveillance’ a study outlining ways to improve computer security auditing and surveillance at customer sites. The original idea behind automated ID is often credited to him for his paper on “How to use accounting audit files to detect unauthorized access”. This ID study paved the way as a form of misuse detection for mainframe systems the concept of detecting misuse and specific user events merged and Dr. Dorothy Denning and SRI(1984) develop first model for intrusion detection, Intrusion Detection Expert System developed. HayStack Project (1988) at University Of California lab released intrusion detection system for US Air Forceand again commercial company HayStack (1989) release Stalker and UC’s Todd Herberlein (1990) introduced the idea of Network Detection System and developed Network Security Monitor i.e the commercial development of IDS. Sornt was released in 1998 and in the same year the commercial development of IPS was also completed and released.

1.1 IDPS (IDS & IPS)

Intrusion Detection Systems (IDS) passively monitor traffic on a network and perform more advanced checks, including protocol and content inspection, to determine indications of possible attacks [2,4-6].

Intrusion Prevention Systems (IPS) combine the functionality of IDS and firewalls, performing in-depth inspection and using this information to block possible attacks. Thus together known as Intrusion Detection and Prevention Systems (IDPs) which is a passive system that scans the traffic and block reports on threats, actively analyzing and taking an automated action on all traffic flows that enter the network. These actions specifically include:

- Sending an alarm to the administrator.
- Dropping the malicious packets.
- Blocking traffic from the source address.
- Resetting the connections.

2.METHODOLOGY FOR INTRUSION DETECTION PREVENTION SYSTEMS

The IDPS has a number of detection methods, but prominent among all the methods are signature-based detection and statistical anomaly-based detection [25-27].

- Signature-based detection is based on dictionary of uniquely identifiable patterns in the code of each exploit and as the exploit is discovered its, signature is recorded and stored in the dictionary [36,40].
- Statistical anomaly-based detection takes the samples of the network traffic at random and compares them to the pre-calculated baseline performance level and when the sample is outside the parameters of the

baseline performance, the IDPS takes action to handle the situation [55-60].

- Stateful Protocol Analysis in this the protocol analyzers can natively decode application-layer network protocols, like HTTP or FTP. Once the protocols are fully decoded, the IPS analysis engine can evaluate different parts of the protocol for anomalous behavior or exploits against predetermined profiles[43-45].
- Hybrid based the most current IDPS systems use the hybrid methodology which is nothing but the combination of other methodologies to offer better detection and prevention capabilities. Hybrid system detect more intrusion then a regular one[6-8].

3.REVIEW ON TYPES AND TECHNIQUES OF IDPS

3.1 TYPES OF IDPS

(i).Network-based: Perform packet sniffing and analyze network traffic to identify and stop suspicious activities. Deployed inline like a network firewalls behind remote access server. They receives the packets, analyze them, and decide whether they should be permitted, and allow acceptable packets to pass through. Allow some attacks ,such as network service worms, e-mail borne worms and viruses with easily recognizable, to be detected on networks before they reach their intended targets. Network-based products might be able to detect and stop some unknown threats through application protocol analysis. However, network-based products are generally not capable of stopping malicious mobile code or Trojan horses.

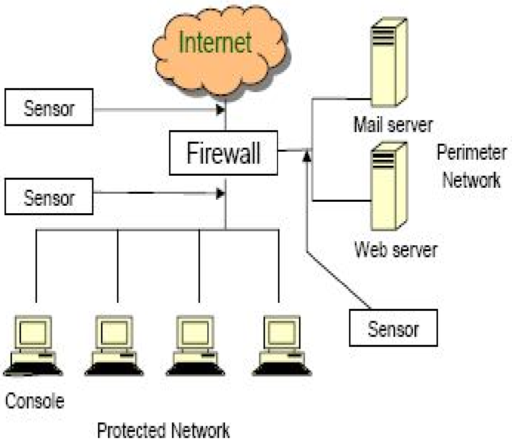

Fig.1: Network-based Architecture

(ii).Host-based: Are similar in principle and purpose to network-based , except that a host-based product monitors the characteristics of a single host and the events occurring within that host, such as monitoring network traffic, system logs, running processes, file access and modification, and system and application configuration changes. Host-based IDPSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information [2,3]

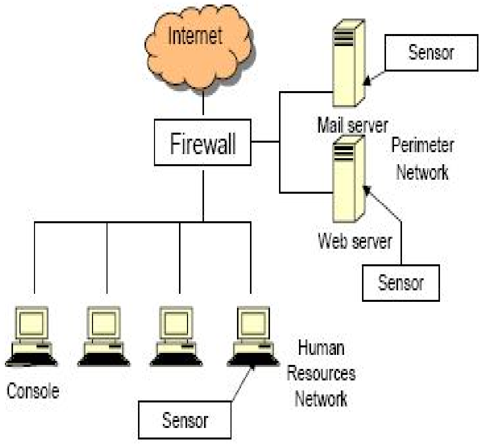

Fig.2: Host Based Architecture

(iii).Network Behavior Analysis (NBA): Examines network traffic to identify threats that generate unusual traffic flows, such as denial of service (DoS) and distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations. Most often deployed to monitor flows on an organization's internal networks, and are also sometimes deployed where they can monitor flows between an organization's networks and external networks [16,17].

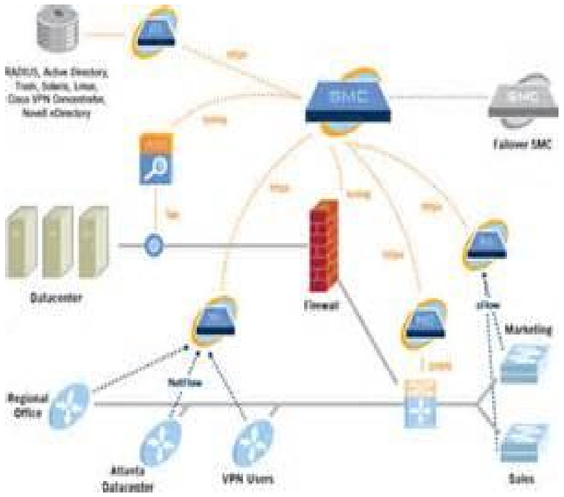

Fig.3: Network Behaviour Analysis Architecture

(iv).Wireless: Monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity involving the protocols themselves. Cannot identify suspicious activity in application. It is most commonly deployed within range of an organization's wireless network to monitor it [15]. Thus Joseph G. Tront and Randy C. Marchany [63] in 2007 introduce listed some intrusion detection and prevention in mobile
system.

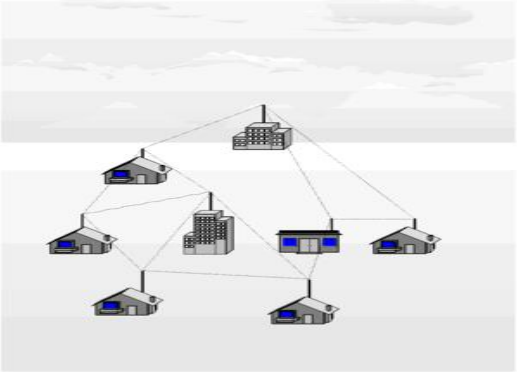

Fig.4: Wireless System Architecture

3.2 TECHNIQUIES

Intrusions are the activities that breaks the security policy of the system, and intrusion detection is the process used to identify intrusions. Intrusion detection techniques have been traditionally classified into one of two methodologies: anomaly detection or misuse detection. Theuns Verwoerd and Ray Hunt [1] observe some recent security threats and explains these techniques [17].

- **Misuse detection**

➢ Catch the intrusions in terms of the characteristics of known attacks or system vulnerabilities.

➢ Integrate the human knowledge and the rules are predefined.

➢ Cannot detect unknown attacks.

- **Anomaly detection**

➢ Detect any action that significantly deviates from the normal behavior.

➢ Any action that significantly deviates from the normal behavior is considered intrusion.

4. PURPOSE

Now the question arises why Intrusion Detection System should be used?

It’s a dire fact that while every enterprise has a firewall, most still suffer from network security problems. IT professionals are markedly aware of the need for additional protective technologies, and network equipment vendors are very eagerto fill in the gap [20-23]. Intrusion Detection and Prevention Systems have been promoted as cost-effective ways to block malicious traffic, to detect and contain worm and virus threats, to serve as a network monitoring point, to assist in compliance requirements, and to act as a network sanitizing agent. PengNing and SushilJajodi[62] in 2002 focuses on the use of IDPs, Jian Pei [61] tell the purpose too.

4.1 IDPSs are primarily focused on:

Identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

Identifying problems with security policies.

Documenting existing threats.

Deterring individuals from violating security policies.

IDPs performs the following as stated below:

- **Recording information related to observed events.** Information is usually recorded locally, and might also be sent to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems.

- **Notifying security administrators of important observed events.** This notification, known as an alert, may take the form of audible signals, e-mails, pager notifications, or log entries. A notification message typically includes only basic information regarding an event; administrators need to access the IDPS for additional information.

- **Producing reports.** Reports summarize the monitored events or provide details on particular events of interest. An IDPS might also alter the settings for when certain alerts are triggered or what priority should be assigned to subsequent alerts after a particular threat is detected. IPSs respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques:

- **The IPS stops the attack itself.** Terminate the network connection or user session that is being used for the attack. Block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute. Block all access to the targeted host, service, application, or other resource.

- **The IPS changes the security environment.** The IPS could change the configuration of other security controls to disrupt an attack. Such as reconfiguring a network device (e.g., firewall, router, switch) to block access from the attacker or to the target, and altering a host-based firewall on a target to block incoming attacks. Some IPSs can even cause patches to be applied to a host if the IPS detects that the host has vulnerabilities.

- **The IPS changes the attack’s content.** Some IPS technologies can remove or replace malicious portions of an attack to make it benign. An example is an IPS removing an infected file attachment from an e-mail and then permitting the cleaned email to reach its recipient.

- **Most IDPSs also offer features that compensate for the use of common evasion techniques. Evasion** is modifying the format or timing of malicious activity so that its appearance changes but its effect is the same. Attackers use evasion techniques to try to prevent IDPSs from detecting their attacks [39-40].

5.CONCLUSION

This paper aims to give a brief comprehensive review about Intrusion Detection and Prevention System which is an important aspect in the computer science because networks today are becoming increasingly vulnerable to hostile attacks and infections such as viruses and worms that spread rapidly, crippling the entire network. With this growing threat, networks need to be designed and equipped with the sophisticated intelligence to diagnose and mitigate these threats in real-time.

REFRENECES

[1]. Intrusion Detection Techniques and Approaches Theuns Verwoerd and Ray Hunt, Department of Computer Science University of Canterbury, New Zealand

[2]. Short Paper Froc. of Int. Conf on Advances in Recent Technologies in Communication and Computing 20 I I A STUDY ON NETWORK INTRUSION DETECTION AND PREVENTION SYSTEM CURRENT STATUS AND CHALLENGING ISSUES
S.Vasanthi 1 and Dr.S.Chandrasekar 2

[3]. Mika Ilvesm"aki, JouniKarvo : "On the behavior of the candidate table of the per-flow packet count flow classifier", June 27, 2000.

[4]. Design of Intrusion Detection and Prevention System (IDPS) using DGSOTFCin Collaborative Protection Networks.

[5]. Axelsson, S. (1999). Research in intrusion-detection systems: A survey. Technical report TR 98-17.Göteborg, Sweden: Department of Computer Engineering, Chalmers University of Technology.

[6]. Barbara, D., Couto, J., Jajodia, S., & Wu, N. (2001). ADAM: A testbed for exploring the use of data mining in intrusion detection. ACM SIGMOD Record, 30 (4), 15--24.

[7]. Intrusion Detection Techniques PengNing, North Carolina State University SushilJajodia, George Mason University.

[8]. Lee, W., & Xiang, D. (2001). Information-theoretic measures for anomaly detection. In R. Needham & M. Abadi (Eds), Proceedings of 2001 IEEE symposium on security and privacy (pp. 130--143), IEEE Computer Society, Los Alamitos, CA.

[9]. Mannila, H., Toivonen, H., &Verkamo, A.I. (1995). Discovering frequent episodes in sequences.In U. Fayyad & R. Uthurusamy (Eds.), Proceedings of the 1st conference on knowledge discovery and data mining (pp. 210--215), AAAI Press, Menlo Park, CA.

[10]. A study of Methodologies used in Intrusion Detection and Prevention Systems (IDPS) David MudzingwaDepartment of ECIT North Carolina A&T State University Greensboro, NC 27411 Email: dmudzing@ncat.edu Rajeev AgrawalDepartment of ECIT North Carolina A&T State University Greensboro, NC 27411

[11]. AnimeshPatcha, Jung-Min Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends, Computer Networks," The International Journal of Computer and Telecommunications Networking, Vol.51, No.12, August, 2007, pp.3448-3470.

[12]. Rebecca Bace, "An introduction to intrusion detection and assessment for system and network security management." ICSA Intrusion Detection Systems Consortium Technical Report, 1999.

[13]. A Comprehensive Approach to Intrusion Detection Alert CorrelationFredrik Valeur, Giovanni Vigna, Member, IEEE, Christopher Kruegel, Member, IEEE, andRichard A. Kemmerer, Fellow, IEEE.

[14]. S.M. Bellovin, "Packets Found on an Internet," technical report, AT&T Bell Laboratories, May 1992.

[15]. L.T. Heberlein, G.V. Dias, K.N. Levitt, B. Mukherjee, J. Wood, and D. Wolber, "A Network Security Monitor," Proc. IEEE Symp. Research in Security and Privacy, pp. 296-304, May 1990.

[16]. Beigh, Bilal Maqbool, and M. A. Peer. "Intrusion Detection and Prevention System: Classification and Quick." (2011).

[17]. Intrusion Detection and Prevention System: Challenges & Opportunities Uzair Bashir Department of Computer Sciences Mewar University Chittorgarh, Rajasthan, India ManzoorChachoo Research Supervisor Mewar University Chittorgarh, Rajasthan,

[18]. Practical Intrusion Prevention Juan M. Estevez-Tapiador• Carlos III University of Madrid IEEE DISTRIBUTED SYSTEMS ONLINE 1541-4922 © 2006 Published by the IEEE Computer Society June 2006 (vol. 7, no. 6), art. no. 0606-o6005.

[19]. MartinRoesch, ―SNORT – Light weightIntrustion detection for networks‖,Proceedings of LISA '99: 13th Systems Administration Conference Seattle, Washington, USA, November 7–12, 1999.

[20]. © 2014 IJEDR | Volume 2, Issue 3 | ISSN: 2321-9939 IJEDR1403077 International Journal of Engineering Development and Research (www.ijedr.org) 3290 Intrusion Detection Techniques and Open Source Intrusion Detection (IDS) Tools Rana M PirLecturer Leading university, sylhet Bangladesh.

[21]. H. Debar, M. Becker, D.Siboni "A Neural Network Component for an Intrusion Detection System",

[22]. Proc. IEEE Symposium on Research in Computer Security and Privacy, 1992.

[23]. AleksandarLazarevic, Vipin Kumar, JaideepSrivastava, "INTRUSION DETECTION: A SURVEY", Managing Cyber
Threats: Issues, Approaches and Challenges, Vol. 5, 2005, Springer Publisher.

[24]. AirTight Networks, "Airtight Enhances Wireless Intrusion Prevention
Through API Integration With Cisco Wireless Products",http://www.airtightnetworks.com/home/ne

ws/pressreleases/pr/browse/l/select_category/26/articleI123/airtightenhanceswireless-intrusion-prevention-through-api-integration-with-ciscowireless-products.html, 20 I O.

[25]. K N Gopinath, P. Bhagwat, "Method and a system for regulating, disrupting and preventing access to the wireless medium", US PatentApplication 20060165073, August 2004.

[26]. The Method of Detecting Malware-Infected Hosts Analyzing Firewall and Proxy Logs Kazunori Kamiya, Kazufumi Aoki, Kensuke Nakata, Toru Sato, Hiroshi Kurakami, Masaki Tanikawa in 2015.

[27]. R. Lippmann, D. Fried, I. Graf, J. Haines, K. Kendall, D. McClung,D. Weber, S. Webster, D. Wyschogrod, R. Cunningham, and M.Zissman, “Evaluating Intrusion Detection Systems: The 1998DARPA Off-Line Intrusion Detection Evaluation,” Proc. DARPA Information Survivability Conf. and Exposition, vol. 2, Jan. 2000.

[28]. BugTraq Mailing List, Vulnerabilities by BugtraqID,http://www.securityfocus.com/bid/bugtraqid/, 2004.

[29]. J. McHugh, “Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evalautions as Performed by Lincoln Laboratory,” ACM Trans. Information and System Security, vol. 3, no. 4, Nov. 2000.

[30]. D.L. Mills Network Time Protocol (Version 3), RFC 1305, 1992.

[31]. B. Morin and H. Debar, “Correlation of Intrusion Symptoms: An Application of Chronicles,” Proc. Int’l Symp. Recent Advances in Intrusion Detection, Sept. 2003.

[32]. B. Morin, L. Me, H. Debar, and M. Ducasse, “M2D2: A Formal Data Model for IDS Alert Correlation,” Proc. Recent Advances in

[33]. SAMI 2015 • IEEE 13th International Symposium on Applied Machine Intelligence and Informatics • January 22-24, 2015 • Herl’any, Slovakia Distributed Firewall in Mobile Ad Hoc Networks Jozef Filipek, Ladislav Hudec Faculty of Informatics and Information Technologies Slovak University of Technology in Bratislava Ilkovičova 2, 842 16 Bratislava, Slovakia xfilipekj1@stuba.sk, ladislav.hudec@stuba.sk

[34]. Nessus Vulnerabilty Scanner, http://www.nessus.org/, 2004.

[35]. Beigh, Bilal Maqbool, and M. A. Peer. "Intrusion Detection and Prevention System: Classification and Quick." (2011).

[36]. Mir, SuhailQadir, S. M. K. Mehraj-ud-din Dar, and Bilal MaqboolBeig. "INFORMATION AVAILABILITY: COMPONENTS, THREATS AND PROTECTION MECHANISMS." Journal of Global Research inComputer Science Journal of Global Research in Computer Science 2.3 (2011).

[37]. Williamson, Matthew M. "Resilient infrastructure for network security." Complexity 9.2 (2003): 34-40.

[38]. Karlzén, Henrik. "An Analysis of Security Information and Event Management Systems-The Use or SIEMs for Log Collection, Management and Analysis." (2009).

[39]. Haystack Labs, Inc.Stalker, available from the company’s website at http://www.haystack.com/stalk.htm, 1997.

[40]. Internet Security Systems, Inc.RealSecure, Internethttp://www.iss.net/prod/rsds.html, 1997.

[41]. A Survey of Intrusion Detection systemsy. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, ―Electron spectroscopy studies on magneto-optical media and plastic substrate interface,‖ IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[42]. SURYA BHAGAVAN AMBATI, DEEPTI VIDYARTHI, ―A BRIEF STUDY AND COMPARISON OF, OPEN SOURCE INTRUSION DETECTION SYSTEM TOOLS‖ International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-1, Issue-10, Dec-2013

[43]. Karen Scarfone and Peter Mell, “Guide to Intrusion Detection and PreventionSystems(IDPS),”http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf, 2007.

[44]. Pedro Garcı´a-Teodoroa, Jesus E. Dı´az-Verdejoa, Gabriel .Macia-Ferna´ndeza, Enrique Va´zquezb, “Anomaly-based network intrusion detection: Techniques, systems and challenge,” Computers Security 28.1-2, 2009, pp. 18-28.

[45]. D. Goodin, “Duqu Spawned by ‘Well-Funded Team of Competent Coders’—World’s First Known Modular Rootkit Does Steganography, Too,” The Register, 9Nov. 2011; www.theregister.co.uk/2011/11/09/duqu _analysis.

[46]. Symantec Security Response, W32.Duqu—The Precursor to the Next Stuxnet (version 1.4), white paper, Symantec,23 Nov. 2011; www.symantec.com/content/en/us/ enterprise/media/security_response/whitepapers/-w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf.

[47]. P. Zhou, X. Luo, A. Chen, and R. K. C. Chang, STor: Social Networkbased Anonymous Communication in Tor, in The Computing ResearchRepository (CoRR), 2011.

[48]. S. T. Zargar, and J. B. D. Joshi, A Collaborative Approach to FacilitateIntrusion Detection and Response against DDoS Attacks, the 6th Int’lConference on Collaborative Computing: Networking, Applicationsand Worksharing (CollaborateCom 2010), Chicago, IL, October 9-12,2010.

[49]. A New Era In Information Security and Cyber Liability Risk Management: A Survey on Enterprise-wide Cyber Risk Management Practices, Sponsored by Zurich Financial Services Group and administered by New York-based Advisen Ltd, October 2011, [online]http://corner.advisen.com/pdf files/cyberliabilityriskmanagement.eps

[50]. J. Kesan, R. Majuca, and W. Yurcik, Cyberinsurance as a market-based solution to the problem of cybersecurity:a case study, SIFT Information Security Services, 2006

[51]. F. Yu, Z. Chen, Y. Diao, T. V. Lakshman, and R. H. Katz, "Fast and memory-efficient regular expression matching for deep packet inspection," in Proc. ACM/IEEE ANCS, 2006, pp. 93–102.

[52]. D. Ficara, S. Giordano, G. Procissi, F. Vitucci, G. Antichi, and A. Di Pietro, "An improved DFA for fast regular expression matching," Comput. Commun.Rev., vol. 38, no. 5, pp. 29–40, 2008.

[53]. M. Becchi and P. Crowley, "Extending finite automata to efficiently match Perl-compatible regular expressions," in Proc. ACM CoNEXT, 2008, Article no. 25.

[54]. L. Krishnamurthy, R. Adler, P. Buonadonna, J. Chhabra, M. Flanigan, N. Dushalnagar, L. Nachman, and M. Yarvis, "Design and deployment of industrial sensor networks: Experiences from a semiconductor plant and the north sea," in Proc. Sensys'05, 2005, pp. 64–75.

[55]. A. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H.Wong, "Decentralized intrusion detection in wireless sensor networks," in Proc. 1st ACMInt.Workshop on Quality of Service Security in Wireless and Mobile Networks, 2005, pp. 16–23.

[56]. B. Sinopoli, C. Sharp, S. Schaffert, and S. S. Sastry, "Distributed control applications within sensor networks," in Proc. IEEE, Aug. 2003 vol. 91, no. 8, pp. 1234–1246.

[57]. A. A. Strikos, "A full approach for intrusion detection in wireless sensor networks," School of Information and Communication Technology, Mar. 2007, KTH.

[58]. C.-C. Su, K.-M.Chang, Y.-H.Kuo, and M.-F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks," in Proc. IEEE WCNC'05: Broadband Wireless forthe Masses Ready for Takeoff, Mar. 13–17, 2005, pp. 1927–1932.

[59]. Lee, W., &Stolfo, S.J. (2000). A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information and System Security, 3 (4) (pp. 227-261).

[60]. JianPei, Data Mining for Intrusion Detection: Techniques ,Applications and Systems, Proceedings of the 20th International Conference on Data Engineering (ICDE 04)

Author

Sonal Paliwal received the B.tech degree in Computer Science and Engineering from S.C.R.I.E.T. CCS University Campus Meerut India in 2013. At present pursuing her M.tech Information Technology from G.P.U.A.T. Pantnagar India and has interest in network security and image processing.