International Journal of Engineering Innovation & Research
Volume 3, Issue 1, ISSN: 2277 – 5668

Overview of Emerging Trends in Network Security and Cryptography

Sri. T. Vinod Kumar
VBIT, Proddatur
Email: vinodoct30@gmail.com

Sri. O. S. Khanna
NITTTR, Chandigarh
Email: oskhanna@gmail.com

Sri. M. Purushotham Reddy
VBIT, Proddatur
Email: purushotham.mps@gmail.com

Sri. G. Sreenivasula Reddy
VBIT, Proddatur
Email: seenu.gurrampati@gmail.com

Sri. G. Rama Subba Reddy
VBIT, Proddatur
Email: subbareddy1227@gmail.com

***Abstract* – In this paper, we provide analysis of network security and cryptography technology topics, arranged groups that are either commonly found or emerging within the information security industry. These topics include: Access Control Management, Antivirus, Audit Data Reduction, Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Anomaly Detection Systems (ADS), Event Correlation Systems (ECS), Network Mapping, Password Cracking, Public Key Infrastructure, Virtual Private Network, and Vulnerability Scanning Systems. IDS, IPS, ADS and ECS are grouped together under one common heading (Intrusion Detection and Prevention Systems) due to their commonality and interdependence. This paper provides basic overview information about each technology within the modern information security.**

***Keywords* – Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Anomaly Detection Systems (ADS), Event Correlation Systems (ECS), Virtual Private Network(VPN), Access Control Management (ACM), Reset (RST), Local Area Network (LAN), etc.,**

I. Introduction and Overview of Approach

This paper introduces network security and cryptography technologies. Each of the following sections focuses on a specific technology.

The security technologies presented in this paper are:

- Access Control Management
- Antivirus
- Audit Data Reduction
- Firewalls
- Intrusion Detection and Prevention Systems
- Network Mapping
- Password Cracking
- Public Key Infrastructure
- Virtual Private Networks
- Vulnerability Scanning Systems

1.1 Access Control Management

Access control management (ACM) systems works on identity, authentication and authorization of the user A standard ACM provides an interface through which a user will self-identify, followed by a mechanism for challenging and confirming that identity, and then a method for granting rights, or access to information, based[12] on the non-repudiated authentication of the user. The primary role of an ACM solution is to protect the confidentiality of a resource by restricting access to the resource. ACM solution will control the attributes of the access, such as read, write and execute.

1.2 Antivirus

The first computer virus credited with being found "in the wild" is believed to be a program called "Elk Cloner" that targeted Apple DOS 3.3[16]. The term "virus" may actually have originated in the 1970s in science fiction literature6, though as a concept it has likely been around since the 1960s. Traditionally, "a virus is simply a computer program that is intentionally written to attach itself to other programs or disk boot sectors and replicate whenever those programs are executed or those infected disks are accessed[18]." In the modern context, this traditional form of malicious code, or malware, is less common. Instead, it is far more common to see variations on this original theme in the form of "worms" and "Trojan horses" that infect a computer system either through direct execution or through some form of network-based replication method.

Antivirus (AV) software has been around for at least the past 20-25 years, though no references were found that indicated a specific date when such programs were first made available. Antivirus software was developed to detect the presence, and eventually the attempted infection, of a system by malware. There are generally two types of antivirus scanning software: signature-based and heuristic. Signature-based scanning relies on a database of known malware signatures. Whereas businesses are expected to install and maintain antivirus software on most, if not all, systems as a matter of limiting legal liability, the effectiveness of AV software diminishes each day. The AV industry has generally reached a plateau in the last fifteen years and has not made any major advances in the ability to detect and prevent malware infection. The purpose of AV is to detect, protect and correct the malware.

1.3 Audit Data Reduction[2]

Audit Data Reduction is an emerging field of study in information security. The problem being addressed relates to the amount of audit data created, out of necessity, by critical systems. These critical systems often generate plentiful amounts of audit logs, which are often difficult to pour through for signs of malfeasance. The goals of audit data reduction systems are to contribute to misuse and

anomaly detection. Audit data reduction (ADR) will increasingly become a useful and necessary part of the information security solution toolset. The purpose of an audit data reduction system is to reduce the overall cost and complexity associated with combining audit logs into one location and interface.

1.4 Firewalls

A firewall is defined as a "component or set of components that restricts access between a protected network and the Internet, or between other sets of networks." Firewalls are network security resources that are defined to control the flow of data between two or more networks. From a high-level perspective, they can serve as a choke-point, designed to restrict, or choke, the flow of network traffic, or as a gateway that performs further processing on the traffic beyond simple choking restrictions. The cost of a firewall today is minimal, and is greatly outweighed by the vast utility it serves. Firewalls need not be expensive solutions, but can be based on generic computer components that make use of free, open-source operating systems and software. "Firewalls are powerful tools, but they should never be used *instead* of other security measures. They should only be used *in addition* to such measures[11]." The primary role of a firewall, in the traditional sense, is to protect against unauthorized access of resources via the network as part of a “defence in depth” solution.

1.5 Intrusion Detection and Prevention Systems

The concept of **intrusion detection**[3] has been around since 1980. In its most essential form, intrusion detection is designed to detect misuse or abuse of network or system resources and report that occurrence. This detection occurs as a result of identifying behaviour based on anomalies or signatures. The most common form of intrusion detection system (IDS) today relies on signature-based detection.

The security industry has greatly expanded intrusion detection over the past years to incorporate several advanced concepts. Beyond basic detection and alerting, most systems today bill themselves as having "intrusion prevention" capabilities; otherwise known as active response. The concept of intrusion prevention is that an activity can be detected reliably and then stopped, either at the host or network level, by the detecting system. From the network perspective, this response could be as simple as detecting an abusive TCP-based network connection and issuing a TCP Reset (RST) packet to both the source and destination hosts, forging the IP header information to impersonate each side. Additionally, significant advances have been made in the areas of event correlation and anomaly detection. Event correlation is an approach wherein multiple alerts that may appear disparate are able to be linked together based on common criteria, such as time or method or target, and result in an escalated alert, if not a coordinated automatic response. Anomaly detection is similar to event correlation, though its primary role is to scientifically determine a baseline for performance, such as across a network or group of hosts, and then generate alerts when performance deviates significantly from that baseline.

Intrusion detection systems are typically classified according to their primary method of detection: network-based, host-based, hybrid, or network-node. Network-based detection captures packets directly off the network, while host-based detection resides on a host and captures data as it flows into and out of that host. Hybrid systems aggregate the capabilities of network-based and host-based systems whereas network-node systems try to function like a network-based system while residing on a host. Today, IDS has begun to mature to the point where most systems can be operated as a hybrid, if the business desires. The main approach used, such as through the open-source product Snort, is to conduct network- and/or host-based scanning using a signature set and then aggregate alerts to a single host for management of those alerts.

The original role of IDS was to detect threats on networks and hosts. This role has evolved to include active response capabilities that allow it to protect resources and correct misuse or abuse on networks or hosts. IDS can today serve in a role that impacts Confidentiality, Integrity and Availability, depending on the signature set deployed, the effectiveness of alert management, and whether or not an active response capability exists.

1.5.1 Intrusion prevention systems, or IPS, are often defined as "any device (hardware or software) that has the ability to detect attacks, both known and unknown, and prevent the attack from being successful." IPS have grown from a desire to combine the deep inspection capabilities of IDS with the blocking capabilities of firewalls. These blocking capabilities, often referred to as active response, allows the detection of a policy violation to be translated in real-time into a policy-based action designed to impede or stop the violation.

There are a few variations on IPS, but the most common is the inline network-based system. Another variation of IPS are the so-called "Layer 7 switches" that have matured to include DoS and DDoS detection and mitigation based on an awareness of traffic at the application layer of the OSI model. Also, host-based application firewalls have been integrated with IDS capabilities to allow for application-specific active response capabilities based on a general policy instead of a signature set. Hybrid switch solutions are network-based, but operate similar to the application firewalls.

All of these types of IPS have two things in common: they generate an alert, based either on a signature or a policy, and they initiate a response, as has been programmed into the system. These alerts may occur as the result of a signature match or a violation of a security policy setup specific for an application, and the response may range from choking the flow of traffic to terminating or blocking the offending traffic altogether. There are a couple key limitations to IPS, as exist for IDS. Those limitations include accurate detection, the ability to handle the full throughput of a network, and the ability to generate the response correctly and in a timely manner.

IPS expands the basic detection capabilities of IDS to include definite corrective capabilities. These corrective capabilities have the related benefit of protecting resources

based on security policies. These capabilities work together to protect the Confidentiality, Integrity and Availability of systems and data.

1.5.2 Event Correlation Systems build on the successes of Intrusion Detection Systems by providing a better mechanism for aggregating, managing and correlating IDS events, such as are generated through signature detections or policy violations. ECS goes beyond simply pulling together event logs from IDS, however. ECS allows for the aggregation of log data from multiple sources, including firewalls, hosts, applications, and of course IDS. Most ECS solutions serve a dual role as a data warehouse for logs and by providing a data mining interface (manual and automated) to make use of the data stored in the warehouse.

The primary benefit of the Event Correlation System is in its ability to correlate events from multiple systems and generate smart alerts, along with the capability to escalate alerts, based on that correlation. Event Correlation Systems are usually comprised of several key activities: Compression, Counting, Suppression, Generalization and Time based correlation.

1.5.3 Compression takes multiple occurrence of the same event, examines them for duplicate information, removes redundancies and reports them as a single event. So 1,000 "route failed" alerts become a single alert that says "route failed 1,000 times."

1.5.4 Counting reports a specified number of similar events as one. This differs from compression in that it doesn't just tally the same event and that there's a threshold to trigger a report.

1.5.5 Suppression associates priorities with alarms and lets the system suppress an alarm for a lower-priority event if a higher-priority event has occurred.

1.5.6 Generalization associates alarms with some higher-level events, which are what's reported. This can be useful for correlating events involving multiple ports on the same switch or router in the event that it fails. You don't need to see each specific failure if you can determine that the entire unit has problems.

1.5.7 Time-based correlation can be helpful establishing causality -- for instance, tracing a connectivity problem to a failed piece of hardware. Often more information can be gleaned by correlating events that have specific time-based relationships. Some problems can be determined only through such temporal correlation.

The primary function of ECS is to better detect events within the enterprise. Once reliable detection occurs, then other capabilities, such as active response, can be developed with it. Until that time, however, this solution is primarily aimed at protecting the Integrity of systems and data as a result of detecting active threats against them.

1.5.8 Anomaly Detection Systems are an extension of Intrusion Detection Systems (or Misuse Detection Systems, as defined by Chung). Per Maxion and Kymie, "[anomaly] detection is a key element of intrusion detection and other detection systems in which perturbations of normal behaviour suggest the presence of intentionally or unintentionally induced attacks, faults, defects, etc." This type of detection is based largely on the rules of probability and predictable, taking into consideration log data from multiple sources (much as is done in ECS), but applying theories of predictability to these logs and automatically generating a best guess as to whether or not a misuse, or abuse, is occurring. In its basest form, ADS generates a baseline for performance and then monitors for behaviour that deviates from that baseline. In its more advanced, optimized form, ADS dynamically calculates the current performance based on aggregate log data and determines whether or not the current level of performance is deviant from expected levels. Anomaly detection systems are an emerging solution related in part to intrusion (or misuse) detection systems and event correlation systems. This reality as an emerging technology limits the number of commercial solutions available and increases the cost of deployment.

ADS are primarily designed to detect threats to the organization. This detect capability may be expanded in the future to include protect and correct capabilities, but only after the product has matured further. The general goal of ADS, as is true with most intrusion detection related solutions, is to primarily ensure Integrity, with secondary goals of ensuring Availability and Confidentiality.

1.6 Network Mapping

Network mapping (Nmap) is defined as "the study of the physical connectivity of the Internet." In its most common form, network mapping is used to document the layout of a local area network (LAN) as part of an overall security assessment. This use is a form of intelligence gathering and oftentimes precedes the actual assessment of targeted systems. Network mapping has evolved over the years from the simple performance of "PING" or "CONNECT" attempts to more extensive and subversive (or "quiet") methods of detection. Today, the most popular tool for performing network mapping is the open source tool Nmap. Nmap is capable of testing for the presence of nodes on a network based on a variety of detection techniques, including the use of Internet Protocol (IP), Transmission Control Protocol (TCP) and Universal Datagram Protocol (UDP). Each of these protocols has a unique flavour, and thus can generate varying results.

The goal of network mapping is to determine would nodes are active on a network. This basic determination can be developed further to identify how far away the nodes are from the scanning host. Operating system identification may also be performed by tools like Nmap, though this functionality is an extension of network mapping and not core to its capabilities.

Network mapping is a form of detection, from the standpoint that it detects nodes on a network, which can in turn be used to determine whether or not a given node is authorized to be on the network. Network mapping may also be construed as a form of protection, since the actions that derive from comparing network mapping data sets could result in removal of unauthorized nodes from the network. From the standpoint of Confidentiality, Integrity and Availability, network mapping primarily serves the

goal of ensuring the Integrity of the network. It may also be used to verify that certain nodes remain available on a network. Network mapping does not have any impact on Confidentiality.

1.7 Password Cracking

According to Wikipedia, "[password] cracking is the process of recovering secret passwords stored in a computer system."30 Password cracking may serve to recover a lost password or to compromise an unknown password for the purposes of gaining unauthorized access to a system or data. Additionally, password cracking may be used as a preventative measure to ensure that strong passwords are being used by system users. Most passwords today are maintained as a hashed, rather than encrypted, value. Hashing means taking a password string and using it as an input for an algorithm that results in an output that does not resemble the original input. Unlike encryption, hashing only works one way and cannot be decrypted. Hashing passwords before storing them is far more efficient than encrypting and decrypting passwords on the fly. Thus, when a user attempts to login, their submitted password is hashed, and the hashed value is compared with the hashed value stored on the system. Given an exact hash match, the login is approved and the user is considered authenticated.

Passwords are typically subjected to a combination of two kinds of attacks: brute-force and dictionary (or word-list). Brute-force attacks attempt to iterate through every possible password option available, either directly attempting to the test password against the system, or in the case of a captured password file, comparing the hashed or encrypted test password against the hashed or encrypted value in the file. In a dictionary attack, a list of common passwords, oftentimes consisting of regular words, is quickly run through and applied in a similar manner as with the brute-force attack.

Dictionary attacks are oftentimes very effective unless systems require users to choose strong passwords. For example, the maintainers of the popular open-source password cracking tool John the Ripper sell collections of word lists on CD. The CDs include word lists for more than 20 human languages, plus common and default passwords and unique words for all combined languages. For around $50 an individual wanting to execute a massive dictionary-based attack could have access to over 600MB of word list data. The ready availability of such data sets for use in dictionary attacks means that, unless a strong password is selected, it is very likely that the password can be cracked in a reasonable amount of time. This is especially true of passwords that are based on human readable words.

A strong password is most often defined as a string of eight (8) or more characters that mix upper- and lower-case letters, numbers and special characters. Strong passwords do not resemble words, and are best when generated at random.33 One suggested approach is picking a passphrase and either using the passphrase in its entirety or picking the leading letters from each word in the phrase and substituting numbers and special characters for some of the letters. Certain password hashing algorithms produce stronger hash values with longer passwords while others produce stronger hash values based on increased complexity of the password. Password cracking is primarily a protective countermeasure. It is designed to ensure that passwords used in various authentication mechanisms are strong enough to prevent casual dictionary-based attacks. It is assumed, however, that a brute-force attack can be 100% successful given enough time. As such, it is vitally import to combine password cracking with strict systematic requirements for strong passwords and regular password rotation. Password cracking helps ensure the Confidentiality and Integrity of data and systems by propping-up the authentication system.

1.8 Public Key Infrastructure

Public Key Infrastructure was once thought to be the silver bullet for solving security and privacy on the Internet, as well as providing a framework for secure business transactions across shared network resources. The reality is that PKI is complex, expensive, and very difficult to implement well. Clarke has gone so far as to claim, with significant proof, that PKI will remain a failure and offers alternatives that seek to improve or supplant the current X.509 standard for PKI. "Its key deficiencies are its inherently hierarchical and authoritarian nature, its unreasonable presumptions about the security of private keys, a range of other technical and implementation defects, confusions about what it is that a certificate actually provides assurance about, and its inherent privacy-invasiveness."

The main role of PKI as a countermeasure is to protect against attack and compromise. Whether it be integrated into an authentication system or part of a code signing system, the overall goal is to ensure Integrity. Additionally, PKI can serve in a capacity of ensuring that Confidentiality of data through trusted encryption mechanisms that leverage trusted encryption materials. PKI may, however, have a negative affect on the Availability of data or systems. If the PKI fails, the associated materials or mechanisms may not function properly to decrypt data, or to allow for proper authentication to occur. Since a secure system will “fail safe,” failure of the PKI should fail to a closed state that disallows access, but in turn impacting Availability.

1.9 Virtual Private Networks

A Virtual Private Network (VPN) is a private communications network that makes use of public networks, oftentimes for communication between different organizations. A VPN is not inherently secure, though in its most common incarnation it does utilize encryption to ensure the confidentiality of data transmitted. The VPN is often seen as a cheaper solution for deploying a private network than private leased-lines. They often serve to protect and ensure the integrity of communications43 and may also protect the confidentiality of those communications when utilizing encryption. There are three types of VPNs available today: dedicated, SSL and opportunistic. Dedicated VPNs, either in a gateway-to-

gateway or client-to-gateway configuration, appear to currently be the most prominent deployment. However, SSL VPNs are increasing in popularity, serving as a lightweight, platform-independent client-to-gateway protection mechanism.

The basic goal of a Virtual Private Network is to ensure the integrity of the connection and communications. When encryption is added, the goal of preserving confidentiality may also be achieved. One downside to VPNs is that they tend to be built on complex systems and are prone to easy disruption, reducing the overall availability of data and communications.

1.10 Vulnerability Scanning Systems

Vulnerability scanning is the "automated process of proactively identifying vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened." Vulnerability scanning typically relies on a handful of tools that identify hosts and then proceed to test them for known weaknesses. The automated scanning process should include three high-level steps: receiving authority to scan, determining the scope of the program, and establishing a security baseline (based on the number of vulnerabilities found per number of hosts scanned).

Vulnerability scanning can contribute to countermeasures in all three areas of protect, detect and correct. The primary role of the scanning is to detect vulnerabilities in systems, but when used properly it will also contribute to protecting resources from being deployed insecurely and by providing adequate information to allow system administrators to correct vulnerabilities.

II. CONCLUSION

The above all emerging trends of information security such as Access Control Management, Antivirus, Audit Data Reduction, Firewalls, Intrusion Detection and Prevention Systems, Network Mapping, Password Cracking, Public Key Infrastructure, Virtual Private Networks, Vulnerability Scanning Systems are most important for information security industry to protect the data from intruders.

REFERENCES

[1] Kanish, Bob. *An Overview of Computer Viruses and Antivirus Software*. Unknown: Kanish, 1996, accessed 12 October 2004; available from http://www.hicom.net/~oedipus/virus32.html; Internet.

[2] Kay, Russell. *Event Correlation*. Unknown: COMPUTER WORLD, 2003, accessed 12 October 2004; available from http://www.computerworld.com/networkingtopics/networking/management/story/0,10801,83396,00.html; Internet.

[3] Manu. *Firewall Basics*. Unknown: SecurityDocs.com, 2004, accessed 06 November 2004; available from http://www.securitydocs.com/library/2413; Internet.

[4] Maxion, Roy A. and Kymie M.C. Tan. *Benchmarking Anomaly-Based Detection Systems*. Pittsburgh: Carnegie Mellon University, 2000, accessed 12 October 2004; available from http://www2.cs.cmu.edu/afs/cs.cmu.edu/user/maxion/www/pubs/maxiontan00.pdf; Internet.

[5] Moskowitz, Robert. *What Is A Virtual Private Network?*. Unknown: CMP, undated, accessed 12 October 2004; available from http://www.networkcomputing.com/905/905colmoskowitz.html; Internet.

[6] National Institute of Standards and Technology. *NIST PKI Program*. Washington: NIST, 2004, accessed 12 October 2004; available from http://csrc.nist.gov/pki/;Internet.

[7] National Institute of Standards and Technology. *NIST Planning Report 02-1: Economic Impact Assessment of NIST's Role-Based Access Control (RBAC) Program*. Washington: NIST, 2002, accessed 12 October 200 4; available from http://csrc.nist.gov/rbac/rbac-impact-summary.doc; Internet.

[8] @stake.@stake LC 5.Cambridge:@stake ,undated, accessed 12 October 2004; available fromhttp://www.atstake.com/products/lc/ ; Internet.

[9] Blanding, Steven F. "Secured Connections to External Networks," in Information Security Management Handbook, 4th Edition, ed. Harold F. Tipton and Micki Krause.Boca Raton: Auerbach, 2000.

[10] Chapple, Mike. Vulnerability scanning with Nessus. Unknown: TechTarget.com, 2003, accessed 12 October 2004; available from http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci938271,00.html?track=NL-20; Internet.

[11] Clarke, Roger. Conventional Public Key Infrastructure: An Artefact Ill-Fitted to the Needs of the Information Society. Canberra:Clarke, 2000, accessed 12 October 2004; available from http://www.anu.edu.au/people/Roger.Clarke/II/PKIMisFit.html; Internet.

[12] Cliff, A. Password Crackers - Ensuring the Security of Your Password. Unknown: SecurityFocus.com, 2001, accessed 12 October 2004; available from http://www.securityfocus.com/infocus/1192 ; Internet.

[13] Cook, Christopher. Managing Network Vulnerabilities in a DOE/NNSA Environment.Kansas City: DOE, undated, accessed 12 October 2004; available fromhttp://cio.doe.gov/Conferences/Security/Presentations/CookC.pps ; Internet.

[14] Desai, Neil. Intrusion Prevention Systems: the Next Step in the Evolution of IDS. Unknown: SecurityFocus.com, 2003, accessed 12 October 2004; available from http://www.securityfocus.com/infocus/1670 ; Internet.

[15] eBCVG IT Security. Heuristic Scanning - Where to Next?. Tel-Aviv: eBCVG, 2004,accessed 12 October 2004; available from http://www.ebcvg.com/articles.php?id=264 ; Internet.

[16] Fyodor. Nmap Security Scanner. Unknown: Insecure.org, undated, accessed 12 October 2004 available from http://www.insecure.org/nmap/index.html ; Internet.

[17] Garfinkel, Simson and Gene Spafford, Practical UNIX & Internet Security, 2nd Edition. Cambridge: O'Reilly, 1996.

[18] Innella, Paul. The Evolution of Intrusion Detection Systems. Unknown:SecurityFocus.com, 2001, accessed 12 October 2004; available from http://www.securityfocus.com/infocus/1514; Internet

AUTHOR'S PROFILE

Vinod Kumar Tummaluru

pursuing his M.E (Electronics & Communication Engineering) from NITTTR, Chandigarh. Presently he is working as Assistant Professor in Electronics & Communication Engineering, Vignana Bharathi Institute of Technology, Proddatur, Kadapa dist, A.P, India.

Sri. O. S. Khanna

working as Associate Professor, National Institute of Technical Teachers' Training and Research Chandīgarh, India since 1984. Research field: Electrical and Electronic Engineering-Wireless and Mobile Communication, Wireless Sensor Networks. Worked as R & D Engineer at Electronics Consortium Pvt Ltd. Delhi, India during Nov 1979-Jan 1981. Worked as Design and Development Engineer at Unitron Limited Farīdābad, India Oct 1978 - Nov 1979 Worked as Junior Scientific Officer at Defence Research & Development Organization, India Hyderabad, India during Jan 1976 - Oct 1978

Dr. G. Sreenivasula Reddy
has prosecuted his B.E(Mechanical Engineering) from Bangalore University in 1996 , M.C.A from Madurai Kamaraj University in 2002 and M.Tech degree in Computer Science Engineering in 2007 from RGMCET Nandyal [Affiliated to JNTU, Hyderabad]. Presently he is working as Associate Professor and Incharge Principal, Vignana Bharathi Institute of Technology, Proddatur, Y.S.R. Kadapa (Dist), Andhra Pradesh. He got a Ph.D in Computer Science & Engineering. His research area is Data Mining, Data Warehousing and Image Processing.

M. Purushotham Reddy
received his M.Tech (Computer Science & Engineering) from Jawaharlal Nehru Technology University, Anantapur. Presently he is working as Associate Professor in Computer Science & Engineering, Vignana Bharathi Institute of Technology, Proddatur, Kadapa dist, A. P., India.

G. Rama Subba Reddy
received his M.Tech (Computer Science & Engineering) from Satyabama University, Chennai. Presently he is working as Associate Professor and H.O.D in Computer Science & Engineering, Vignana Bharathi Institute of Technology, Proddatur, Kadapa dist, A.P, India.