INTRUSION DETECTION SYSTEM INSIDE GRID COMPUTING ENVIRONMENT (IDS-IGCE)

Basappa B. Kodada, Ramesh Nayak, Raghavendra Prabhu, Suresha D.

Dept. of Computer Science and Engineering
Canara Engineering College
basappabk@gmail.com, ramesh.nayak.spi@gmail.com, rghprabhu7@gmail.com, sureshasss@gmail.com

Abstract

Grid Computing is a kind of important information technology which enables resource sharing globally to solve the large scale problem. It is based on networks and able to enable large scale aggregation and sharing of computational, data, sensors and other resources across institutional boundaries. Integrated Globus Tool Kit with Web services is to present OGSA (Open Grid Services Architecture) as the standard service grid architecture. In OGSA, everything is abstracted as a service, including computers, applications, data as well as instruments. The services and resources in Grid are heterogeneous and dynamic, and they also belong to different domains. Grid Services are still new to business system & as more systems are being attached to it, any threat to it could bring collapse and huge harm. May be intruder come with a new form of attack. Grid Computing is a Global Infrastructure on the internet has led to a security attacks on the Computing Infrastructure. The wide varieties of IDS (Intrusion Detection System) are available which are designed to handle the specific types of attacks. The technique of [27] will protect future attacks in Service Grid Computing Environment at the Grid Infrastructure but there is no technique can protect these types of attacks inside the grid at the node level. So this paper proposes the Architecture of IDS-IGCE (Intrusion Detection System – Inside Grid Computing Environment) which can provide the protection against the complete threats inside the Grid Environment.

Key words:

Service Gird, Intrusion Detection System, IDS-IGCE, OGSA

1. INTRODUCTION

Grid [1] is a kind of Distributed Computing Environment, which allows large scale resource sharing and system integration. It is based on the networks and able to enable large scale aggregation and sharing of computational, data, sensors and other resources across institutional boundaries. In 2002, GGF (Global Grid Forum), which is now renamed as OGF (Open Grid

DOI: 10.5121/ijgca.2011.2403

Forum), integrated Globus [15] with the web services to present the OGSA (Open Grid Service Architecture) as the standard grid architecture which includes everything like computers, applications, data as well as instruments and facilities. With the growing use of internet, attackers have become more and more active in identifying the flaw of the application or Operating system connected to the network protocols are able to make the attacks on the network resources to make the damage on the network system or Application running in the system. Grid Computing is collection or heterogeneous resources or nodes from different organization globally. The need to support the integration and management of resources within VOs (Virtual Organization) introduces challenging security issues [28].

For a variety of issues relating to certification, group membership, authorization, and the like, the relationships among participants in VOs represent an overlay with respect to the relationships existing between those participants and their parent organizations. This overlay exists both in terms of trust and with respect to the security mechanisms and policies in place at those parent organizations. Grid system must detect the all type of attacks either it may be known or unknown or future attacks. In this paper we discuss about the Intrusion Detection System (IDS) and propose the IDS-IGCE to detect the all types of threats in the service grid.

Intrusion Detection Systems [16] have a very important role in the Grid Security Management. For the execution of large scale application or in service grid there is clearly need to detect the known or unknown intrusion and any other kind of dangerous events. Although, some traditional IDS's detection accuracies are high in the offline tests, when facing the more traffic some of them crashes since tremendous amount of packets often markedly slow down detection speed and detection speed power will come down. So this paper is proposing the Intrusion Detection System (IDS) inside the Service Grid which detects future attacks because no single technique can guarantee protection against the future attack.

Rest of the paper is organized as follows. Section 2 of this paper contains the security issues in the Grid Computing Environment. Section 3 gives the related work of IDS in the Grid Computing Environment. Section 4 explains about the Intrusion Detection System (IDS). Section 5 of this paper proposes the Security Architecture of IDS – Inside Grid Computing Environment and finally Section 6 concludes this paper and presents the future work.

2. GRID COMPUTING SECURITY ISSUES

Grid is collection of heterogeneous computers and resources spread across multiple administrative domains with the intent of providing users easy access to the resources. There may be many way to access the resources of computational grid, each with security requirements for both resource user and resource provider. There are many security issues in the Grid Computing Environment shown below[30]:

- Protect applications and data from system where computation executes
- Stronger authentication needed (for users and code)
- Protect local execution from remote systems
- Different admin domains/security policies
- Assurance (Performance and Reliability)
- Accounting (Tracking, limiting, Charging, Allocation of Resources).
- Audit (What went wrong, Intrusion Detection).
- Behavioral issues (Intrusion Detection System).

Computational grid services may be required to be availed anonymously within the grid framework to keep the personal sensitive information about the service requester protected. This paper focuses on the protection of privacy and anonymity of grid stakeholders inside the service oriented computational grid framework.

In a Virtual Enterprise (VE), a service provider as well as service requester or consumer must be allowed to define and enforce privacy policies [Foster (2004)] to protect sensitive information like personal information, credit history of a customer or some confidential data etc. While collating responses from multiple service providers, the master service provider or broker has to open individual sections of the form. But, the individual service provider is supposed to open the portion of the form designated for its own filling up and not to intervene with anyone else's area. This requires that the XML document be multi-parted and have some means to protect portions to undesired service provider. One level of concern is that the XML content, which may contain information of multiple heterogeneous service providers, may get exposed to one service provider, a node on the grid. This may have a breach of privacy between multiple service providers.

Many a times, privacy is closely resembled with anonymity that demands the need of being unidentified or unobserved while transacting over public domain such as web or other public realm. Adequate level of privacy needs to be achieved through controlled disclosure of identity and associated information. Anonymity can ensure achievement of privacy needs. In general, anonymous message transmission requires that the transacting message would not carry any information about the original sender and intended receiver

3. RELETED WORK

Grid Computing has many security mechanisms by integrating into Grid Security Infrastructure (GSI) which offers basic authentication and secure communication based on the X.509 certificates for authentication. [2][3][4] Provides an agent method to IDS respectively, but they could not resolve the problems caused by the heterogeneity and dynamic of the Grid; [5] provides a distributed IDS based on data fusion method, but it lack the ability of automatic reorganization.

Leu et al. [6] developed a performance-based grid intrusion detection system (PGIDS) which exploited grid's abundant computing resources to detect logical, DoS and DDoS attacks real-time so that the drawbacks that traditional IDSs suffer were then eliminated. However, PGIDS is performed on a static environment. Its detection flexibility is limited. Park and Lee in 2002 [7] raised a route-based packet filtering (RPF) approach checking whether each packet comes from a correct link and source. Moreover, many IDS prototypes have been developed in recent years, such as distributed attack detection (DAD) [8], Multicast Intrusion Detection and Alerting System (MIDAS) [9] and Distribution Intrusion Detection System (DIDS) [10].

In [14] a Grid level intrusion detection system is presented but it offers a very complicated system, without an emphasis on performance or the reduction of the number of sent messages. It describes the problem and the need for a higher level of intrusion detection but doesn't express the importance of having a real-time image of the applications running on the Grid to be able to detect the more advanced types of attack. Another important related work is the one presented in [12] which offers a good solution for Denial-of-Service [13] and Distributed Denial-of-Service attacks. Also, it presents a type of Grid Intrusion Detection System but it does not provide a solution to other types of attack. Hence this paper proposes the security architecture to prevent the all type of known attacks and future attacks as well.

In [29], a novel architecture for a streaming intrusion detection system for Grid Computing Environments is presented. Detection mechanisms based on traditional log-files or single host databases are replaced by a streaming database approach. The streaming architecture allows processing of temporal attack data across multiple sites and offers the potential for performance benefits in large scale systems, since data is processed during its natural flow and only stored as long as necessary for analysis. Two cross-site example attacks in a Grid environment and the streaming detection logic for these attacks are presented to illustrate the approach. Experimental results of a prototypical implementation are presented. The wide varieties of IDS (Intrusion Detection System) are available which are designed to handle the specific types of attacks. But this paper proposes the IDS to handle the known and unknown types of attacks.

4. INTRUSION DETECTION

Intrusion Detection is a process of identifying intrusion activities. IDS can function both at host level or Network level as well based on the three types of technique like anomaly detection, signature detection and denial of service [17]. A signature-based (or misuse-based) IDS has a database of attack signatures and works similarly to anti-virus software, by raising an alert when it matches one of the signatures. Those signatures typically address widely used systems or applications for which security vulnerabilities are known. Nevertheless, similarly to anti-virus software that fails to identify viruses when there is no signature available or the virus database is out of date, a signature-based IDS also fails to detect unknown attacks.

To overcome limitation of signature-based IDSs, researchers have sought out the other ways to detect intrusions. An anomaly-based IDS works by building a statistical model of usage patterns describing the normal behavior of the monitored resource. After this initial training phase, the system uses a similarity metric to compare new input requests with the model, and generates alerts for those deviating significantly, considering them anomalous. Basically, attacks are detected because they produce a different, i.e., anomalous, behavior than what was observed when creating the model. The main advantage of an anomaly-based system is its ability to detect previously unknown (or variants of known) attacks when they appear. Nevertheless, these systems typically suffer from high rates of false positives and can be evaded using mimicry attacks, i.e., attempts to pass as normal behavior, for example by using byte substitution or padding techniques.

The popularity of web applications, now often designated as software as a service (SaaS) when offered by a provider to a set of users, has caught the attention of attackers try to exploit their vulnerabilities. For example, in a recent survey, 95% of the respondent organizations reported having experienced more than 10 incidents related to their web sites [19]. Therefore, using intrusion detection and specifically anomaly-based intrusion detection is important in such systems. Several anomaly-based IDSs for web applications have already been proposed in the literature [18], [22], [23], [26], [24], [25], [21], [20]. Most of the IDS are focusing on only one type of detection either on anomaly detection or signature detection or denial of service detection. So the network or system administrators buy the solutions from the different vendors and integrate them to detect all type threats or malicious attacks.

Many Intrusion Detection System (IDS) detects the threats or attacks but there is a strong need of preventing the attacks also. The IDS uses so many mechanisms to alerting the new threats but some time it gives wrong or false alert. The current IDS in the Grid Computing are designed to support one or two security policies for Computational Grid and Data Grid but there is no technique detects or prevents the all types of threats in Computational Grid or Data Grid or

Service Grid. Hence we propose a Security Architecture for Service Grid which detects and prevents the future attacks inside the Grid Computing Environment.

5. IDS - IGCE ARCHITECTURE

Grid Computing is about several processors distributed globally and sharing the computational resources to solve various problems. The major issues associated with Grid Computing is coordinating resource sharing as well as problem solving in dynamic, multi-institutional virtual organizations (VOs). In 2002, GGF (Global Grid Forum), which is now renamed OGF (Open Grid Forum), integrated Globus [15] with Web services to present OGSA (Open Grid Services Architecture) as the standard grid architecture. In OGSA, everything is abstracted as a service, including computers, applications, data as well as instruments and facilities, etc. the services and resources in Grid are heterogeneous and dynamic, and they also belong to different domains.

So the intrusion detection system (IDS) for Service Grid should be a system which could rapidly and dynamically integrate the related node detection resources of a Grid Computing application according to the dynamic detection demand and ensure the security inside the Grid Computing. So in this paper we propose the Security architecture for inside the Service Grid Computing as shown in the figure 1, i.e. IDS - IGCE which detect the all types of attacks which could be known attack or it could be unknown attack. Figure 2 shows that all nodes inside the grid are communicated through the IDS - IGCE which monitor the all packet and detects anonymous and known attacks. Because trusted node inside the grid could be intruder. Hence this paper presents the Intrusion Detection System at the node level inside the Grid Computing Environment while providing any services.

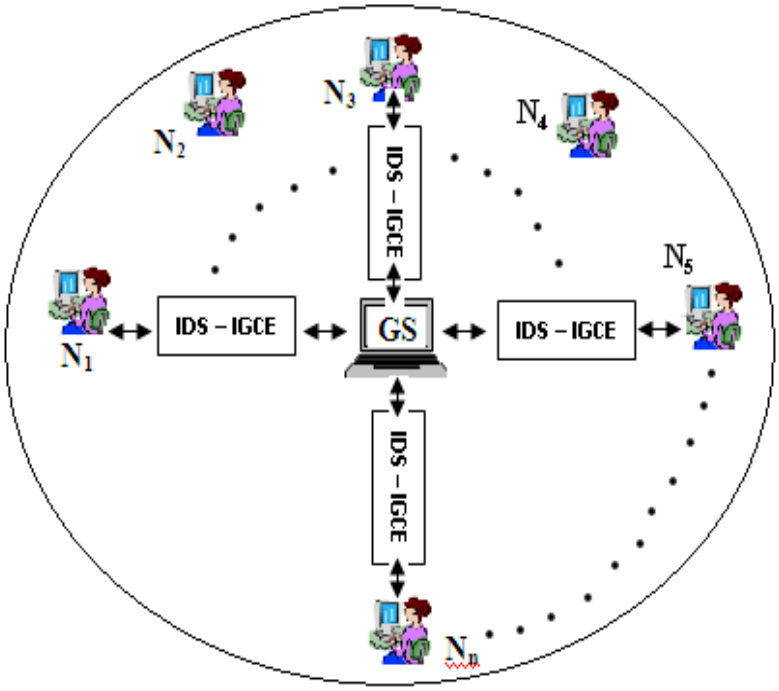


Figure 1: Security Architecture for Service Grid Computing

Figure 2 summarizes the architecture of the Intrusion Detection System – Inside Grid Computing Environment (IDS – IGCE). The proposed solution contains a Cache component that collects network packets based on a heuristic. The Sampler randomly/heuristically picks up sample packet windows (series of contiguous packets) and sends them to the Network Packet Analyzer component. The Analyzer and the preprocessing engine analyze the packets and convert them into a standard XML (Extension Markup Language) format by stripping the network and DLL headers. This metadata is sent for processing to the next component i.e. the "Rules Engine" which can be an OGSA (Open Grid service Architecture) component. The Rules engine is a OGSA enabled component of the application that facilitates the XML packet to be checked for anomalies against suspicious activities and predefined business rules. This component should be able to detect packets from invalid/entrusted IPs and domains. DoS attacks, Filtering, Screening, Authentication, Trust, etc. related issues can be addressed at this component. The Rules engine should be enabled to allow the organization to implement and customize the rules based on the location of the IDS on the network. Rules must be classified as preemptive/non-preemptive.

The rules engine upon detecting anomaly will automatically forward to alert agent component or manual intervention component. If directed to alert agent component then the alerts are audited, logged, and mailed to concerned authorities. If all packets in a sample packet window are cleared by Rules Engine, then the packets go for a check of known attack signatures to the verifier. The Verifier component checks the packets against attacks picked from a local signature known attack database. This DB is pre-populated from external and publicly known signatures and other IDS instance detected signatures. If the verifier detects the known attack signature then it directed to alert agent component then the alerts are audited, logged, and mailed to concerned authorities otherwise the packet will be accepted to continue. If the rule engine detects the anonymous attack, then Gen-sig (Generate Signature) will generate the signature and the updater then picks up these XMLs and their packet payloads and digests them using fast and compressive hashing algorithms that compact this information and store it in the local signature K. A. DB (Know Attack Data Base) for the known attacks.

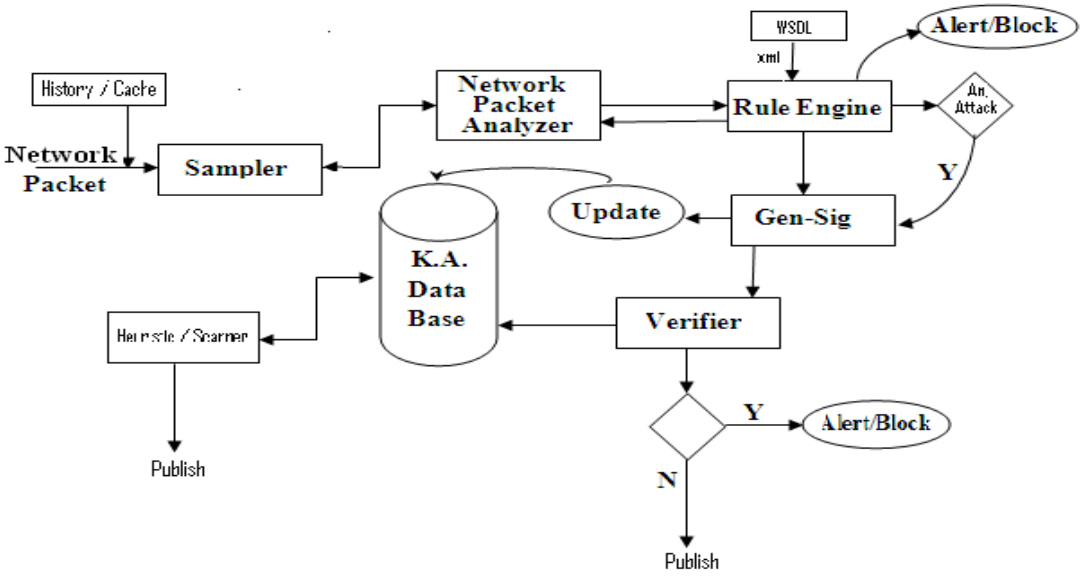


Figure 2: Architecture of IDS – IGCE

Since the signatures are hashed, comparing them in the verifier against new XMLs and network packet payloads becomes easy and quick to achieve the "fast Ethernet" speeds that this architecture claims. For packets that have matched a possible known attack, the packets and the payload can be sent into the heuristic and acute scanner that can perform further analysis to detect newer form of attacks or decisively declare a packet/source as safe. This can over period of time detect new attacks and recover from false alarms. All the period, the Database is kept updated through updater ensures that over a period of time the IDS learns to detect unknown attacks and thus can prevent them as well making it a true IDS. Whenever the verifier component detects a known signature match, it immediately discards the packet. As already mentioned the verifier checks the hash of the XML and the payload from the DB against the incoming XML packet and payload of the sample window, which enables to detect a match for components about attacks detected.

6. CONCLUSION

The proposed architecture can detect all types of attacks inside the Grid Computing which could be known attacks or unknown attacks efficiently. It allows new computing resources and services to be added dynamically and also previous unknown attacks will become known attacks by updating the new attack signature to known attack database inside the Grid Computing Environment. Our future work is to implement the SG-IDS & IDS – IGCE and simulate the results for the performance evaluation.

REFERENCES

[1] I. Foster and C. Kesselman, ***"The Grid: Blueprint for a New Computing Infrastructure"***, 1st ed. Morgan Kaufmann Publishers, November 1998.

[2] Jian Li, Guo-yin Zhang, Guo-chang Gu . ***"A Multi-agent Based Architecture for Network Attack Resistant System"***, LNCS 3032, 980-983, 2004.

[3] Grzegorz Kolaczek, Agnieszka Pieczynska Kuchtiak, Krzysztof Juszczyszyn, ***"A Mobile Agent Approach to Intrusion Detection in Network Systems***", LNCS 3682, 514, 2005.

[4] Andrew H. Sung, Srinivas Mukkamala, ***"The Feature Selection and Intrusion Detection Problems",*** LNCS 3321, 468, 2004.

[5] Yong Wang, HuihuaYang, Xingyu Wang, Ruixia Zhang, ***"Distributed Intrusion Detection System Basedon Data Fusion Method***", Proceedings of the 6 World Congress on Intelligent Control and Automation. 2004.

[6] F.Y. Leu, J.C. Lin, M.C. Li and C.T. Yang, ***"A Performance-Based Grid Intrusion Detection System",*** Proc. of IEEE Annual International Computer Software and Applications Conf., pp. 525-530, July 2005.

[7] K. Park and H. Lee, ***"On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets",*** Proc. ACM SIGCOMM, Aug.2001, pp.15-26.

[8] K. K. Wan and R. Chang, ***"Engineering of a Global Defense Infrastructure for DDoS Attacks",*** Proc. IEEE Int'l. Conf. Net., Aug. 2002.

[9] Sebring, Michael M., E. Shellhouse, M. E. Hanna, and R. A. Whitehurst, ***"Expert Systems in Intrusion Detection: A Case Study",*** Proceedings of the Eleventh National Computer Securtiy Conference, Washington, D.C., October 1988.

[10] Snapp, S. R. et al. ***"DIDS (Distributed Intrusion Detection System) – Motivation, Architecture, and An Early Prototype",*** Proceedings of the Fifteenth National Computer Security Conference, Baltimore, MD, October, 1992.

[11] M. Humphrey, M. Thompson, and K. R. Jackson, ***"Security for grids",*** in Proceedings of the IEEE (Special Issue on Grid Computing), March 2005.

[12] Fang-Yie Leu, Jia-Chun Lin, Ming-Chang Li, Chao-Tung Yang, Po-Chi Shih, ***"Integrating Grid with Intrusion Detection***", International Conference on Advanced Information Networking and Applications (AINA'05), 2005.

[13] D Moore, C Shannon, DJ Brown, GM Voelker, ***"Inferring Internet denial-of-service activity"***, ACM Transactions on Computer Systems (TOCS), 2006.

[14] A. Schulter, J.A. Reis, F. Koch, C.B. Westphall, "***A Grid-based Intrusion Detection System****"*, ICNICONSMCL 06: Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006.

[15] C. K. I. Foster, ***"Globus: A meta-computing infrastructure tookit",*** Intl J. Supercomputer Applications, vol. 11, no. 2, pp. 115–128, 1997.

[16] Yu, Zhenwei and Tsai, Jeffrey J. P. and Weigert, Thomas, ***"An adaptive automatically tuning intrusion detection system***", ACM Transactions on Autonomous and Adaptive Systems (TAAS), 2008.

[17] Rebecca Bace and Peter Mell, ***"Intrusion Detection Systems",*** NIST Special Publication on Intrusion Detection System.

[18] S. Cho and S. Cha. ***"SAD: web session anomaly detection based on parameter estimation",*** Computers & Security, 23(4):312–319, 2004.

[19] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson. ***"CSI/FBI computer crime and security survey",*** Computer Security Institute, 25, 2005.

[20] K. L. Ingham. "***Anomaly detection for HTTP intrusion detection: algorithm comparisons and the effect of generalization on accuracy",*** PhD thesis, University of New Mexico, 2007.

[21] K. L. Ingham, A. Somayaji, J. Burge, and S. Forrest. "***Learning DFA representations of HTTP for protecting web applications",*** Computer Networks, 51(5):1239–1255, 2007.

[22] C. Kruegel and G. Vigna. ***"Anomaly detection of webbased attacks",*** In Proceedings of the 10th ACM Conference on Computer and Communications Security, pages 251–261, 2003.

[23] C. Kruegel, G. Vigna, and W. Robertson. "***A multi-model approach to the detection of web-based attacks",*** Computer Networks, 48(5):717–738, 2005.

[24] W. Robertson, G. Vigna, C. Kruegel, R.A. Kemmerer, et al. "***Using generalization and characterization techniques in the anomaly-based detection of web attacks",*** In Proceedings of the 13th Symposium on Network and Distributed System Security, February 2006.

[25] K. Wang, J. Parekh, and S. Stolfo. "***Anagram: A content anomaly detector resistant to mimicry attack***", In Proceedings of the 9th International Conference on Recent Advances in Intrusion Detection, pages 226–248. Springer, 2006.

[26] K. Wang and S.J. Stolfo. ***"Anomalous payload-based network intrusion detection",*** In Proceedings of the 7th International Conference on Recent Advances in Intrusion Detection, pages 203–222. Springer, 2004.

[27] Basappa B. Kodada, Manjunath Prasad, ***"Security Architecture for Building IDS in the Service Grid",*** IJCSIS August 2011 (Accepted).

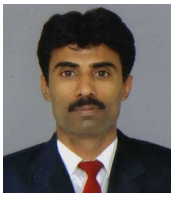
[28] Foster, I., Kesselman, C., Tsudik, G. and Tuecke, S, ***"A Security Architecture for Computational Grids",*** ACM Conference on Computers and Security, 1998, 83-91.

[29] M. Smith, et. Al, ***"A Streaming Intrusion Detection System for Grid Computing Environments",*** IEEE - ICHPCC 2009, 978-0-7695-3738-2/09.

[30] Clifford Neuman, ***"Security issues in Grid Computing",*** Reading: Grid Book, Chapter 16: Security, Accounting and Assurance.

AUTHOR PROFILE

Mr. Basappa B. Kodada, Asst. Professor, is a Faculty of Canara Engineering College, Mangalore at Vishweswaraya Technological University Belgaum, Karnataka. Prof. Basappa B. Kodada obtained his B.E (Computer Science and Engineering) from Vishweswara ya Technological University Belgaum, Karnataka and M.Tech (Computer Science & Engg – Information Security) from National Institute of Technology Karnataka in 2007 and 2010 respectively. His research areas include the Information and Network Security, Distributed Computing, Grid Computing, Cloud Computing and Mobile Computing. He has published 2 international journal and 3 international conference papers.



Mr. Ramesh S. Nayak, is currently working as Assistant Professor in department of Information Science & Engineering at Canara Engineering College, Bantwal, Mangalore. He obtained his B.E from Karnataka University, Dharwad and M.Tech in Computer Science & Technology from University Of Mysore in 2008. He has 13 years of teaching experience. His research areas include Communication Networks, Network Security, Could computing and Image processing. He has published 1 international journal and 2 international conference and 3 national conference papers.

Mr. Raghavendrab Prabhu is persuing M.Tech at Canara Engineering College, Mangalore at Vishweswaraya Technological University Belgaum, Karnataka. He has obtained hi s B.E (Computer Science and Engineering) from Vishweswaraya Technological University Belgaum, Karnataka in 2010. His research area of interest includes the Distributed Computing, Grid Computing, Cloud Computing, Information and Network Security and Mobile Computing.

Mr. Suresha D, Asst. Professor, is a Faculty of Canara Engineering College, Mangalore at Visvesvaraya Technological University Belgaum, Karnataka. Prof. Suresha D obtained his B.E (Computer Science and Engineering) from Kuvempu University, Jnanasahyadri, Shankaragatta and M.Tech (Computer Network Engineering) from Visvesvaraya Technological University Belgaum Karnataka. His research areas include Image processing, Information and Network Security, Grid Computing and Ad hoc Networks. He has published 1 national conference paper.