



SAT: A Security Architecture in Wireless Mesh Networks

K.G.S. VenkatesanAssociate Professor, Dept. of CSE
Bharath University, Chennai, INDIA**K.P. Shyamraj**Department of C.S.E.
Bharath University, Chennai-600073**S. Anand**Department of C.S.E.
Bharath University, Tamil Nadu

Abstract - *Anonymity has received increasing attention among the literature as a result of the users' awareness of their privacy of late. Anonymity provides protection for users to relish network services whereas not being derived. whereas anonymity-related issues are extensively studied in payment-based systems like e-cash and Peer-to-Peer (P2P) systems, little or no effort has been dedicated to Wireless Mesh Networks (WMNs). On the selection hand, the network authority desires conditional obscurity specified misbehaving entities among the network keep traceable. throughout this paper, we have got a bent to tend to propose a security vogue to confirmed conditional obscurity for honest users and traceability of misbehaving users for network authorities in WMNs. The planned vogue strives to resolve the conflicts between the obscurity and traceability objectives, in addition to guaranteeing basic security desires in conjunction with authentication, confidentiality, information integrity, and non repudiation. Thorough analysis on security and potency is in demonstrating the utility and effectiveness of the planned vogue.*

Key Words : *Wireless Mesh Network (WMN), misbehaviour, revocation.*

I. INTRODUCTION

Wireless Mesh Network (WMN) may even be a promising technology and is anticipated to be widespread as a result of its low investment feature that the wireless broadband services it supports, taking part to every service suppliers and users. However, security issues inherent in WMNs or any wireless networks would really like be thought of before the preparation and proliferation of these networks, since it's unappealing to subscribers to induce services whereas not security and privacy guarantees. Wireless security has been the recent topic among the literature for various network technologies like cellular networks [1], wireless native area networks (WLANs) [2], wireless detector networks [3], [4], mobile spontaneous networks (MANETs) [5], [6], and conveyance spontaneous networks (VANETs)[7]. Recently, new proposals on WMN security [8], [9] have emerged. In [8], the authors describe the specifics of WMNs and establish three basic network operations that need to be secured. we have a bent to tend to [9] propose degree attack-resilient security vogue (ARSA) for WMNs, addressing countermeasures to Associate in Nursing outsized vary of attacks in WMNs. Due to the fact that security in WMNs remains in its infancy as very little or no interest. Our system borrows the blind signature technique from payment systems [11], [12], [14] and hence, can achieve the obscurity of unlinking user identities from activities, still as a result of the traceability of misbehaving users. Furthermore, the projected nom Diamond State guerre technique renders user location info unexposed. Our work differs from previous add that WMNs have distinctive stratified topologies and swear heavily on wireless links, that ought to be compelled to be thought of among the obscurity vogue. As a result, the original obscurity theme for payment systems among bank, customer, and store cannot be directly applied. In addition to the obscurity theme, varied security issue such as authentication, key establishment, and revocation are important in WMNs to create certain the proper application of the anonymity theme. Moreover, although we have a bent to tend to use the widely used nom Diamond State guerre approach to create certain network access obscurity and computing machine privacy, our anonym generation does not believe a central authority, e.g., the broker in [9], the domain authority in [15], the transportation authority or the manufacturer in [7], so the sure authority in [18], world organization agency can derive the user's identity from his pseudonyms associate degree illicitly trace Associate in Nursing honest user. Note that our system is not supposed for achieving routing obscurity, which will be incorporated as associate degree sweetening. Specifically, our major contributions throughout this paper include **1)** form of a ticket-based obscurity system with traceability property; **2)** bind of the price tag and nom Diamond State guerre which guarantees anonymous access management (i.e., anonymously authenticating a user at the access point) and simplified revocation process; **3)** adoption of the stratified identity-based cryptography (HIBC) for inter domain authentication avoiding domain parameter certification. The rest of the paper is organized as follows: Section a combine of introduces some preliminaries. The system model at the aspect of the description and trust model is delineate in Section 3. Section four elaborates on the ticket-based obscurity theme, that's that the key an area of our security architecture. Security analysis, efficiency analysis, and possible enhancements pertinent to the projected vogue are given in Sections V, VI, and VII, severally. Finally, Section VIII concludes the paper.

II EXISTING SYSTEM

In existing system the obscurity set up were implemented in P2P and payment system like e-cash system whereas not traceability. The obscurity is nothing however it provides the protection to the user real credentials. But the traceability

ideas weren't used here. the sole issue here traceability in P2P and payment system as a results of whereas not traceability couldn't found the misbehave users. In wireless communication systems, it's easier for a world observer to mount traffic analysis attacks by following the packet forwarding path than in wired networks. Thus, routing obscurity is indispensable, which conceals the confidential communication relationship of 2 parties by building associate anonymous path between them. Anonymity may incur corporate executive attacks since misbehaving users do not appear to be from now on traceable. Therefore, traceability is awfully fascinating like in e-cash systems where it's used for detection and tracing double-spenders.

III Proposed System

Our planned system is meant in wireless mesh networks exploitation the weekday style. This style builds the four ideas like:

A Tag Activity System

In this paper we'd prefer to sustain the protection against the aggressor, so as that every user at the beginning sends the request to the trustworthy authority to urge the worth tag from the trustworthy authority. anytime the trustworthy authority receives the request from the user thereafter the trustworthy authority authenticates the particular user, if the verification succeeds only it will make over the tickets to the particular user. the worth tags are basically contains the price tag vary, expire date and time and act details.

B Ticket Deposit System

In our paper next level is Associate in Nursing once acquire the tickets successfully from the reliable authority, the user send the request to the deposit approach for deposit the tickets. The request contains the data like ticket and name to the deposit approach, here before depositing the price tag price tag} the approach send the authenticates the user once verification succeed only the ticket are attending to be deposited.

C Fraud Detection System

In our system the fraud detection supported the user multiple {ticket|pricetag|price {ticket|pricetag|price pricetag {ticket|price tag|price {ticket|price tag|price price tag}}}} deposit to the gateway; this ticket is additionally deposited quite once valid ticket or already used ticket .This technique found by the reliable authority in deposit approach.

D Revocation System

Once the user used his/her all the worth price tags or invalid ticket ,thereafter user send the new request to the reliable authority once acquire the new ticket from the metal .The user send the new deposit request to the deposit approach if the verification successes only the worth price tag are attending to be deposited here.

IV. Modules

A Wireless mesh networks (WMNs)

The wireless mesh backbone consists of mesh routers (MRs) and gateways (GWs) interconnected by ordinary wireless links (shown as dotted curves). Mesh routers and gateways serve as the access points of the WMN and the last resorts to the Internet, respectively. Each WMN domain, or trust domain(to be used inter changeably) is managed by a domain administrator that serves as a trusted authority the central server of a campus WMN.

B Blind Signature

In general, a blind signature scheme allows a receiver to obtain a signature on a message such that both the message and the resulting signature remain unknown to the signer. We refer the readers for a formal definition of a blind signature scheme, which should bear the properties of verifiability, unlink ability, and unforged ability. Blind signature scheme, where the restrictiveness property is incorporated into the blind signature scheme such that the message being signed must contain encoded information. As the name suggests, this property restricts the user in the blind signature scheme to embed some account-related secret information into what is being signed by the bank (otherwise, the signing will be unsuccessful) such that this secret can be recovered by the bank to identify a user if and only if he double-spends. The restrictiveness property is essentially the guarantee for traceability in the restrictive blind signature systems.

C Ticket Issuance

In order to maintain security of the network against attacks and the fairness among clients, the home server manager may control the access of each client by issuing tickets based on the misbehavior history of the client, which reflects the server manager's confidence about the client to act properly. Ticket issuance occurs when the client initially attempts to access the network or when all previously issued tickets are depleted. The client needs to reveal his real ID to the server manager in order to obtain a ticket since the server manager has to ensure the authenticity of this client.

D Fraud Detection

Fraud is used interchangeably with misbehaviour in this paper, which is essentially an insider attack. Ticket reuse generally results from the client's inability to obtain tickets from the TA when network access is desired, primarily due to the client's past misbehaviour, which causes the server manager to constrain his ticket requests.

E Fundamental security objectives

It is trivial to show that our security architecture satisfies the security requirements for authentication, data integrity, and confidentiality, which follows directly from the employment of the standard cryptographic primitives, message authentication code, and encryption, in our system. We are only left with the proof of non repudiation in this category. A fraud can be repudiated only if the client can provide a different representation, he knows of message from what is derived by the server manager. If the client has misbehaved, the representation he knows will be the same as the one derived by the server Manager which ensures non repudiation..

V Technologies Used

A JAVA

It is a Platform freelance. Java is associate object-oriented artificial language developed at the start by James goose and colleagues at Sun tiny systems. The language, at the start stated as Oak (named once the oak trees outside Gosling's office), was meant to interchange C++, although the feature set higher resembles that of Objective C.

INTRODUCTION TO JAVA

Java has been around since 1991, developed by atiny low team of Sun tiny systems developers in associate degree passing project originally stated because the inexperienced project. The intent of the project was to develop a platform-independent coding system technology that will be used within the purchaser trade. The language that the team created was originally stated as Oak. The first implementation of Oak was in associate degree passing PDA-type device stated as Star Seven (*7) that consisted of the Oak language, associate package stated as inexperienced OS, a programme, and hardware. The name *7 was derived from phonephone{thephonephone} sequence that was used within the team's geographical point that was dialled thus on answer any ringing phonephone from the opposite phone at intervals the geographical point.

OPERATIONAL OF JAVA

For those who unit unaccustomed object-oriented programming, the thought of a class area unit unaccustomed you. Simplistically, a class is that the definition for a section of code that will contain every information (called attributes) and functions (called methods). once the interpreter executes a class, it look for a particular technique by the name of main, which may sound acquainted with to C programmers. the foremost technique is passed as a parameter associate array of strings (similar to the argv[] of C), and is declared as a static technique. To output text from the program, we have a tendency to tend to execute the println technique of System.out, that's java's output stream. UNIX users will appreciate the speculation behind such a stream, as a result of it's extremely customary output. For those who unit instead used to the Wintel platform, it's going to write the string passed to that to the user's program.

Java consists of two things :

- 1.Programming language
- 2.Platform

The code and would possibly originate changes whenever felt necessary. variety of the standard needed to achieve the preceding objectives unit as follows:

Java is unusual in that each Java program is every co understood and understood. With a compiler, you translate a Java program into associate intermediate language referred to as Java store unit codes – the platform freelance codes understood by the Java interpreter. With associate interpreter, each Java store unit code instruction is parsed and run on the computer. Compilation happens merely once; interpretation happens on each occasion the program is dead. This figure 1 illustrates but it works : you will take into account Java store unit codes as a result of the pc code directions for the Java Virtual Machine (JVM). every Java interpreter, whether or not it's a Java development tool or an online browser that will run Java applets, is associate implementation of JVM. That JVM can also be enforced in hardware. Java store unit codes facilitate produce “write once, run anywhere” getable. you will compile your Java program into store unit codes on any platform that contains a Java compiler. the pc memory unit codes can then be run on any implementation of the JVM. as an example, that exact same Java program can e run on Windows organisation, Solaris and Macintos.

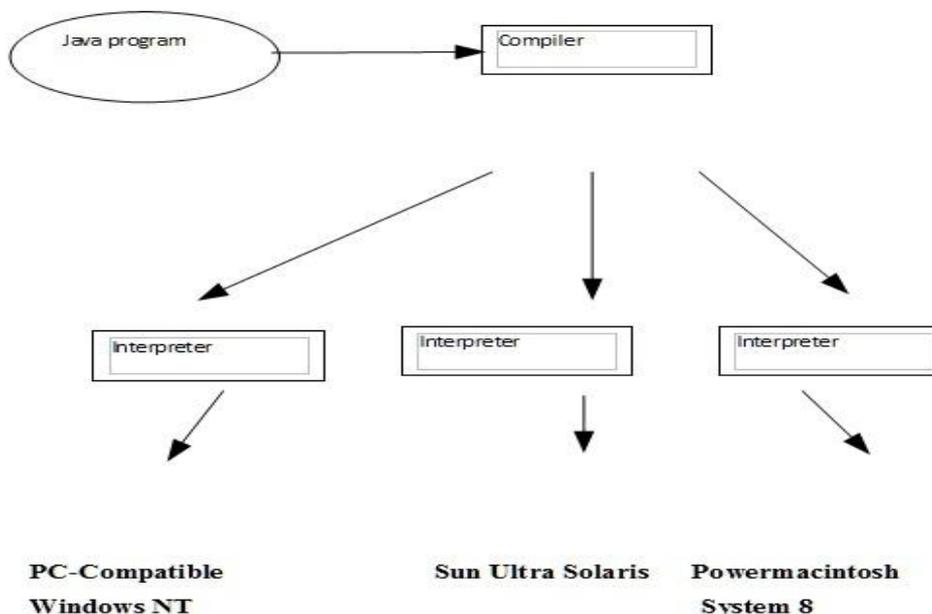


Fig 1 : Java Program with compiler & Interpreter.

B INTRODUCTION TO JAVA FX

The JavaFX Script artificial language helps you to supply stylish wanting applications with refined graphical user interfaces. it completely was designed from all-time low up to form interface programming easy; its declarative syntax, info binding model, animation support, and integral visual effects enable you to accomplish plenty of labor with less code, resulting in shorter development cycles and exaggerated productivity. This tutorial is your house to start for learning the JavaFX Script artificial language. It focuses on the fundamentals only: that is, on the underlying, non-visual, core constructs that square measure common to any or all FX applications. once finished, you'll be ready for Building interface Applications with JavaFX, the second tutorial throughout this series. After that, the Media Browser tutorial will walk you through the total finish-to finish development of a real-world application. to boot, advanced developers area unit fascinated by the JavaFX Script artificial language Reference and Application Programming Interface (API) documentation. These reference documents provide a lower-level discussion of the syntax, semantics, and supported libraries of the JavaFX Script artificial language and SDK.

Introduction

Purpose

The foremost keep of this project to make academic degree convenience of obscurity and traceability in wireless mesh networks exploitation SAT style.

Paper Scope

The scope of this paper is security style to verify obscurity for honest users and traceability of misbehaving users for network authorities in WMNs [17]. The obscurity plan was implemented in P2P and payment system like e-cash system whereas not traceability. Here we've got a bent to unit of measurement reaching to implement the project in wireless mesh networks victimization Saturday style. This style is utilized tag provision and deposit system to create a network lots of security and maintain the obscurity and traceability [15]. Here the trustworthy authority is utilized to issue the worth tag} to the user and entrance is utilized to deposit the price tag from the user. therefore once the verification is maintained to create associate convenience security to the user credentials

VI Sat Design

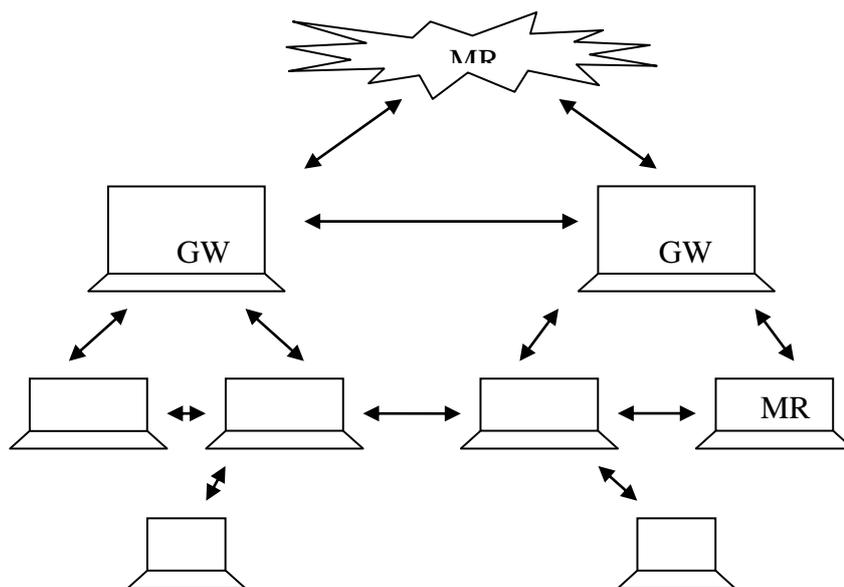


Fig 2 : SAT Design with positive authority, Mesh router.

- TA - positive Authority
- GW - approach
- MR - Mesh Router
- CL - shopper

A Ticket Request

In our paper the first module is to elect the node .The node is used to send the request to the trustworthy authority then get the worth tag from the trustworthy authority Before issue the value tag} the metal will contact the verification whether or not or not the node is real node or not there once entirely metal will issue the price ticket.

B Ticket Deposit

During this paper our second module is to elect the router. The router is used to connect to the entree, its act as a wireless access purpose it produce a association to the node like P2P system . This association may be multihop communication. This router jointly connect with the router [12]. So as that entire node is below the mesh router. whereas not router the node can't connect with the entree. If the node needs to communicate between the alternative node means the

communication happened through the router. Here the node is send the deposit request to the entree, it's going to happened through router.

C Data Communication Ticket: Activity and Deposit System

In our final module, the trustworthy authority system accustomed kind secure specification. once the nodes are request to the worth tag, the metal square measure authenticates the node thereafter it's going to be generate the tickets to the node. This specific value tag} contains the information like price ticket selection, expire date and time. once get the value tag} the buyer is used to deposit the price ticket in entree system, this module is accustomed deposit the tickets from the node. The entree may be connected to the quite entree then all the entree are below the one or plenty of roof the trustworthy authority. The entree is check the node network access with facilitate of the worth tag expires date and time .If the value tag} is expire means the particular node network access is denied with the particular price ticket.

VII Testing

Testing is also a way of capital punishment a program with the intent of finding a mistake. a good action at law is one that contains a high probability of finding associate as-yet –undiscovered error. A lucky take a glance at is one that uncovers associate as-yet- undiscovered error. System testing is that the stage of implementation, that's aimed toward ensuring that the system works accurately and with efficiency of course before live operation commences. It verifies that the entire set of programs tie. System take a glance testing desires a take a look at consists of the many key activities and steps for run program, string, system and is extremely vital in adopting a lucky new system. this may be the last likelihood to note and correct errors before the system is place sure user acceptance testing. The package testing technique commences once the program is formed and conjointly the documentation and connected data structures area unit designed. package testing is crucial for correcting errors. Otherwise the program or the project is not same to be complete. package testing is that the vital element of package quality assurance and represents the ultimate word the review of specification vogue and committal to writing [15]. Testing is that the tactic of capital punishment the program with the intent of finding the error. A good action at law vogue is one that as a probability of finding a nevertheless undiscovered error. A lucky take a glance at is one that uncovers a nevertheless undiscovered error. Any engineering product are going to be tested in one in each of the two ways:

A WHITE BOX TESTING

This testing is to boot brought up as as Glass box testing. throughout this testing, by knowing the precise performs that a product has been vogue to perform take a glance at are going to be conducted that demonstrate each perform is completely operational at an identical time sorting out errors in each perform. it'sa action at law vogue methodology that uses the management structure of the procedural vogue to derive take a glance at cases. Basis path testing is also a white box testing.

Basis path testing:

- 1.Flow graph notation
2. Cyclometric complexity
- 3, Deriving take a glance at cases
4. Graph matrices management

B RECORDER TESTING

During this testing by knowing the inside operation of a product, take a glance at are going to be conducted to create positive that “all gears mesh”, that is the interior operation performs to keep with since the compiler s will not deduct logical error, the software engineer ought to examine the output. Condition testing exercises the logical conditions contained throughout a module. The potential types of elements throughout a condition embody a scientist operator, scientist variable, a attempt of scientist parentheses A relative operator or on arithmetic expression. Condition take a glance ating technique focuses on take a look ating each condition at intervals the program the aim of condition test is to deduct not exclusively errors at intervals the condition of a program but put together totally different a errors at intervals the program

C SECURITY TESTING

Security testing tries to verify the protection mechanisms built-in to a system well, in fact, defend it from improper penetration. The system security ought to be tested for invulnerability from frontal attack ought to even be tested for invulnerability from rear attack. throughout security, the tester places the role of individual United Nations agency needs to penetrate system.

D VALIDATION TESTING

At the top results of Integration testing, software system package is completely assembled as a package. Interfacing errors area unit uncovered and corrected and a final series of software system package test-validation testing begins. Validation testing area unit usually printed in some ways in which, but an easy definition is that validation succeeds once the software system package functions in manner that is moderately expected by the consumer. Software system package

validation is achieved through a series of recorder tests that demonstrate conformity with demand. once validation take a glance at has been conducted, one amongst a pair of conditions exists.

* The operate or performance characteristics notify specifications and square measure accepted.

* A validation from specification is uncovered and a deficiency created.

Deviation or errors discovered at this step during this paper is corrected before completion of the paper with the help of the user by negotiating to establish the simplest way for partitioning deficiencies. Thus the projected system into thought has been tested by using validation testing and situated to be operational satisfactorily. tho' there are deficiencies within the system they weren't harmful.

E USER ACCEPTANCE TESTING

User acceptance of the system is significant issue for the success of any system. The system into thought is tested for user acceptance by constantly keeping involved with prospective system and user at the time of developing and making changes whenever required. {this is|this is usually|this can be} often drained regarding to the following points.

VIII Conclusion

In this paper, we tend to propose weekday, a security design mainly consisting of the ticket-based protocols, which resolves the conflicting security necessities of unconditional obscurity for honest users and traceability of misbehaving users. By utilizing the tickets, self-generated pseudonyms, and also the ranked identity-based cryptography, the projected design is incontestable to achieve desired security objectives and potency.

Acknowledgment

The author would like to thank the Vice Chancellor, Dean-Engineering, Director, Secretary, Correspondent, Principal, HOD , Dean CSE Dr.A.Kumaravel of Bharath University, Chennai for their motivation and constant encouragement. The author would like to specially thank Dr. V.Khanaa for his guidance and for critical review of this manuscript and for his valuable input and fruitful discussions in completing the work and the Faculty Members of Department of Computer Science & Engineering. Also, he takes privilege in extending gratitude to his parents and family members who rendered their support throughout this Research work.

References

- [1] A. Brush and K. Inkpen, "Yours, Mine and Ours? Sharing and Use of Technology in Domestic Environments," Proc. Int'l Conf. Ubiquitous Computing, pp. 109-126, 2007.
- [2] A.L. Chavan and D. Gorney, "The Dilemma of the Shared Mobile Phone—Culture Strain and Product Design in Emerging Economies," ACM Interactions, vol. 15, pp. 34-39, 2008.
- [3] M. Hall, "Create a Windows CE Image that Boots to Kiosk Mode," <http://msdn.microsoft.com/en-us/libraryaa446914.aspx>, 2009.
- [4] R. Hull, B. Kumar, D. Lieuwen, P. Patel-Schneider, A. Sahuguet, S. Varadarajan, and A. Vyas, "Enabling Context-Aware and Privacy-Conscious User Data Sharing," Proc. IEEE Int'l Conf. Mobile Data Management, 2004.
- [5] G.C. Hunt and D. Brubacher, "Detours: Binary Interception of Win32 Functions," Proc. Conf. USENIX Windows NT Symp., 1999.
- [6] S. Jain, F. Shafique, V. Djeri, and A. Goel, "Application-Level Isolation and Recovery with Solitude," Proc. Third ACM SIGOPS/ EuroSys European Conf. Computer Systems, 2008.
- [7] P.H. Kamp and R.N.M. Watson, "Jails: Confining the Omnipotent Root," Proc. Second Int'l SANE Conf., 2000.
- [8] A.K. Karlson, A.J.B. Brush, and S. Schechter, "Can I Borrow Your Phone?: Understanding Concerns When Sharing Mobile Phones," Proc. SIGCHI, 2009.
- [9] B. Lampson, "Computer Security in the Real World," Proc. Ann. Computer Security Applications Conf., 2000.
- [10] Z. Liang, V.N. Venkatakrishnan, and R. Sekar, "Isolated Program Execution: An Application Transparent Approach for Executing Untrusted Programs," Proc. 19th Ann. Computer Security Applications Conf., 2003.
- [11] B. des Ligneris, "Virtualization of Linux Based Computers: The Linux-VServer Project," Proc. 19th Int'l Symp. High Performance Computing Systems and Applications, pp. 340-346, 2005.
- [12] J.S. Olson, J. Grudin, and EricHorvitz, "A Study of Preferences for Sharing and Privacy," Proc. Extended Abstracts on Human Factors in Computing Systems, 2005.
- [13] T. Pering, D.H. Nguyen, J. Light, and R. Want, "Face-to-Face Media Sharing Using Wireless Mobile Devices," Proc. IEEE Int'l Symp. Multimedia, 2005.
- [14] D. Price and A. Tucker, "Solaris Zones: Operating System Support for Consolidating Commercial Workloads," Proc. 18th USENIX Conf. System Administration, 2004.
- [15] S. Soltesz, H. Po'tzl, M.E. Fiuczynski, A. Bavier, and L. Peterson, "Container-Based Operating System Virtualization: A Scalable, High-Performance Alternative to Hypervisors," ACM SIGOPS Operating Systems Rev., vol. 41, pp. 275-287, 2007.
- [16] A. Voids, R.E. Grinter, N. Ducheneaut, W.K. Edwards, and M.W. Newman, "Listening In: Practices Surrounding iTunes Music Sharing," Proc. SIGCHI, 2005.

- [17] Y. Yu, F. Guo, S. Nanda, L.-c. Lam, and T.-c. Chiueh, "A Feather-Weight Virtual Machine for Windows Applications," Proc. Second Int'l Conf. Virtual Execution Environments, 2006.
- [18] Likert Scale, http://en.wikipedia.org/wiki/Likert_scale, 2010.

ABOUT THE AUTHOR



K.G.S.Venkatesan received his B.Tech degree in Computer Science & Engineering from JNT University, Hyderabad and received his M.Tech degree in Computer Science & Engineering from Bharath University, Chennai. He is currently pursuing his Ph.D in Computer Science & Engineering at Bharath University, Chennai. He has 10 years of Teaching experience and has guided many B.Tech and M.Tech projects. He is having Membership in Indian Society of Technical Education (MISTE). He attended **HIGH IMPACT Teaching Skills** Programme conducted by WIPRO MXLA (Mission 10X Learning Approach).

K.P.Shyamraj is currently pursuing his B.Tech., Final Year, VIII Semster in Computer Science & Engineering from Bharath University, Chennai. He has secured Second Rank Holder in Schools and many Cultural activities participation certificates in the school.

S.Anand is currently pursuing his B.Tech., Final Year, VIII Semster in Computer Science & Engineering from Bharath University, Chennai. He has secured Second Rank Holder in Schools and many Cultural activities participation certificates in the school