PROTECTING YOUR MOBILE CLOUD DATA CHAOS -BASED ENCRYPTION

[1] *Mrs.D.Keerthi Reddy,* [2] *N.L.Hari Priya,* [3] *P.Prathyusha,* [4] *Md.Sameer,*[5] *Md.Uzer*
[1] Assistant *Professor,*[2345]*B.Tech Students*
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

ABSTRACT

This project considers the security problem of outsourcing storage from user devices to the cloud. A secure searchable encryption scheme is presented to enable searching of encrypted user data in the cloud. The scheme simultaneously supports fuzzy keyword searching and matched results ranking, which are two important factors in facilitating practical searchable encryption. A chaotic fuzzy transformation method is proposed to support secure fuzzy keyword indexing, storage and query. A secure posting list is also created to rank the matched results while maintaining the privacy and confidentiality of the user data, and saving the resources of the user mobile devices. Comprehensive tests have been performed and the experimental results show that the proposed scheme is efficient and suitable for a secure searchable cloud storage system.

I. INTRODUCTION

Cloud is a model to enable convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) In the current Internet, people can easily access their data stored in the cloud with their mobile devices from anywhere, e.g., check emails, and read the history of online chatting applications, view previously saved photos, videos or other kind of documents. To provide security in all such scenarios, it is essential to store and access the outsourced data in a secure and efficient manner. For the protection of data privacy and control, data is usually encrypted before outsourcing, which makes its effective utilization a challenge. In particular, indexing and searching the outsourced encrypted data becomes problematic. Searchable encryption (SE) allows searching over encrypted data in the cloud and returns to the user the data that correspond to the given keywords, without having to reveal the keywords. It is thus a critical enabler for securing outsourced data.

Traditional searchable encryption schemes allow a user to securely search over encrypted data through keywords but only support 1) exact keyword matching, which is not a practical requirement for current mobile phone input methods and 2) boolean search without capturing the relevance of data files. The system usability can be greatly enhanced by the use of fuzzy keyword search instead of traditional searchable encryption. Fuzzy, or error tolerant, searchable encryption returns to the user the files that match not only the exact predefined keywords but also the closest possible matched files based on keyword similarity semantics. Similarly, system usability is greatly enhanced by ranked search which returns the matched files in a ranked order determined by appropriate relevance criteria. This paper investigates the problem of supporting both ranked and fuzzy keyword search in a single scheme to achieve effective utilization of remotely stored encrypted data in mobile cloud computing applications.

II. LITERATURE SURVEY

TITLE: Cryptographic primitive called Public Key Error Tolerant Searchable Encryption (PKETS)

AUTHOR: Krishna Kowshik Tenneti

ABSTRACT: Many approaches are proposed to enable fuzzy search. Researchers consider the use of wildcards to enlarge the range of possible similar keywords searched, but this technique only covers part of the possible close keywords. A wildcard only permits capturing of errors provided we know where they are located in the keyword.

The authors proposed a new cryptographic primitive called Public Key Error Tolerant Searchable Encryption (PKETS) which is based on public key encryption with keyword search proposed. This algorithm was applied to the biometric data. The author Acceptable erroneous keywords did not have to be specified in advance in their algorithm.

However, this approach was designed for a special type of data, i.e., iris code. This technology is useful at airports as a replacement for passports but it is not designed for text documents. The authors proposed to embed edit distance (Levenshtein distance) into Hamming distance to obtain a fuzzy keyword search suitable for strings and then text files.

This method uses existing locality sensitive hashing (LSH) to enable the fuzziness in the search method and has a very low distortion. However, this method is mainly theoretical and the proposed embedding technique introduces a lot of redundancy, which increases the dimension of the stored data, and is not suitable for the case of mobile usage because of the small amount of memory available. Another method uses bloom filters and Jaccard similarity to perform the translation and the LSH. It also introduces ranking of the retrieved encrypted data. However, the ranking has to be performed by the user himself and not automatically by the server which can add unwanted burden for a mobile users device.

TITLE: Chaotic Searchable Encryption for mobile storage.

AUTHOR: Padala Srinivasa Reddy

ABSTRACT: This paper considers the security problem of outsourcing storage from user devices to the cloud. A secure searchable encryption scheme is presented to enable searching of encrypted user data in the cloud. The scheme simultaneously supports fuzzy keyword searching and matched results ranking, which are two important factors in facilitating practical searchable encryption. A chaotic fuzzy transformation method is proposed to support secure fuzzy keyword indexing, storage and query.

A secure posting list is also created to rank the matched results while maintaining the privacy and confidentiality of the user data, and saving the resources of the user mobile devices. Comprehensive tests have been performed and the experimental results show that the proposed scheme is efficient and suitable for a secure searchable cloud storage system.

Actually, very few searchable encryption schemes support the ranking of matched items though this problem has recently attracted the attention of some researchers. Fuzziness and ranking are currently two different research axes and very few researchers have considered combining them. However, these methods are either not practical for mobile usage as is the case or they suffer from security problems as is the case.

This work proposed a new fuzzy transformation by introducing chaos and enhances the fuzziness through amplification of the LSH, which significantly improves both the security and the efficiency of the fuzzy searching process compared to the existing solutions. A new fuzzy transformation by introducing chaos and enhance the fuzziness through amplification of the LSH, which significantly improves both the security and the efficiency of the fuzzy searching process compared to the existing solutions. Furthermore, comprehensive tests on different LSH methods are performed in order to select the best one to be used in our algorithm.

TITLE: Attribute Based Encryption for Secure Data Access in Cloud.

AUTHOR: Anirudh Mitta

ABSTRACT: Cloud computing is a progressive computing worldview, which empowers adaptable, on request, and ease use of Information Technology assets. However, the information transmitted to some cloud servers, and various protection concerns are arising out of it. Different plans given the property-based encryption have been proposed to secure the Cloud Storage.

In any case, most work spotlights on the information substance security and the get to control, while less consideration towards the benefit control and the character protection. In this project, a semi anonymous benefit control conspires Anony Control to address the information protection, as well as the client character security in existing access control plans. Anony Control decentralizes the central authority to restrain the character spillage. Along these lines, display the Anony Control-F, which ultimately keeps the character spillage and accomplish the full secrecy. Our security assessment demonstrates that both Anony Control and Anony Control-F are secure under the decisional bilinear Diffie-Hellman presumption, and our execution assessment shows the attainability of our plans. According to Park (2011), the Computing service provider cannot be trusted entirely because of data security reasons, the danger of data safety and infringement of protection variables are considered. Particularly, ensuring data classification required to take care of these issues, Yu, Wang, Ren, and Lou (2010) proposed to conspire which guarantees data classification and fine-grained get to control. Be that as it may, data secrecy which was damaged by intrigue assault of repudiated client and cloud server.

TITLE: Towards secure mobile cloud computing: A survey

AUTHOR: Abdul Nasir Khan, M.L. Mat Kiah

ABSTRACT: Mobile cloud computing is gaining popularity among mobile users. The ABI Research predicts that the number of mobile cloud computing subscribers is expected to grow from 42.8 million (1.1% of total mobile users) in 2008 to 998 million (19% of total mobile users) in 2014. Despite the hype achieved by mobile cloud computing, the growth of mobile cloud computing subscribers is still below expectations. According to the recent survey conducted by the International Data Corporation, most IT Executives and CEOs are not interested in adopting such services due to the risks associated with security and privacy.

The security threats have become a hurdle in the rapid adaptability of the mobile cloud

computing paradigm. Significant efforts have been devoted in research organizations and academia to build secure mobile cloud computing environments and infrastructures. In spite of the efforts, there are a number of loopholes and challenges that still exist in the security policies of mobile cloud computing. This literature review:

(a) highlights the current state of the art work proposed to secure mobile cloud computing infrastructures,

(b) identifies the potential problems, and

(c) provides a taxonomy of the state of the art.

To have an in depth understanding of Mobile Cloud Computing , it is necessary to get a complete grasp on cloud computing. Cloud computing provides a new computing paradigm that delivers as a service. The objectives of the new computing paradigm are to increase capacity and capabilities at runtime without investing in new infrastructure, licensing new software, and training new recruits. Cloud computing permits customers to utilize cloud services on the fly in pay-as you-go manner through the Internet.

TITLE: Data Security of Mobile Cloud Computing on Cloud Server.

AUTHOR: Muhammad Waseem, Dost Mohammad Baloch, Imran Khan.

ABSTRACT: Mobile Cloud computing is a technology of delivering services, such as software, hardware (virtual as well) and bandwidth over the Internet. Mobile devices are enabled in order to explore, especially Smart phones. The mobile cloud computing technology is growing rapidly among the customers and many companies such as Apple, Google, Facebook and Amazon with rich users. Users can access their data at any time, at any place, even with any device including mobile devices by using the cloud storage services, although these properties offer flexibility and scalability in controlling data, however, at the same time it reminds us with new security threats.

These security issues can be resolved by proper handling of data. The cloud server provider can secure the data by applying the encryption and decryption techniques while storing the data over the cloud. In this paper, we proposed some encryption and decryption methods for securing the data over the cloud so that an unauthorized person or machine cannot access the confidential data owing to encrypted form. Cloud computing with resource constraint mobile devices, ubiquitous wireless infrastructure, mobile web, and location-based services provides a ground for a new computing paradigm called Mobile Cloud Computing (MCC).

The ultimate goal of the MCC is to enable execution of rich mobile applications on a plethora of mobile devices, with a rich user experience. Mobile devices such as Smartphone, Tablets are increasingly becoming an integral part of modern life and culture as the connectivity, communication and sharing have turned out to be easier and convenient among people. Mobile applications (apps) for that matter reduce the performance of a task in a span of minutes and help deliver accurate results.

III. SYSTEM ANALYSIS & DESIGN

EXISTING SYSTEM

In the existing system, Bringer et al. proposed a new scheme permitting search over encrypted data with an approximation of a keyword. An application in the biometric domain is also proposed. A biometric identification scheme arises from this construction; it permits identification of a person using his biometrics in an encrypted way. A specific difficulty concerning biometrics is their fuzziness. It is nearly impossible for a sensor to obtain the same image from biometric data twice.

The classical way to solve this problem is to use a matching function, which basically tells if two measures represent the same biometric data or not, but these methods do not meet the privacy requirements that someone can expect from an such identification scheme. The Bringer et al. algorithm resolves this issue and provides the privacy missing in the existing algorithms. This method uses a combination of LSH method specific for an iris code (beacon indexes) to enable the fuzziness and a Bloom filter with storage to accelerate the search on the encrypted data.

DISADVANTAGES

- Performance is low.
- These existing works are not efficient.
- Less-Security.
- Missing of data.

PROPOSED SYSTEM

This system proposes a new fuzzy transformation by introducing chaos and enhances the fuzziness through amplification of the LSH, which significantly improves both the security and the efficiency of the fuzzy searching process compared to the existing solutions. Furthermore, comprehensive tests on different LSH methods are performed in order to select the best one to be used in our algorithm. Chaotic systems are widely used in the cryptography domain and have attracted the attention of many researchers due to the interesting characteristics of chaos. However, to the best of 7 our knowledge, this is the first paper proposing to use chaos in the searchable encryption schemes. Our proposed system is, in addition, designed to support fuzzy and ranking mechanisms and is proven to be practical for mobile usage.

ADVANTAGES

- Improved encryption techniques.
- Enhanced security measures.
- Data protection

SYSTEM ARCHITECTURE

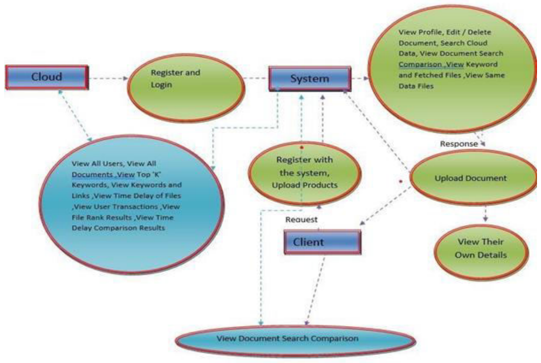

Cloud
Register and Login
System
View Profile, Edit / Delete Document, Search Cloud Data, View Document Search Comparison ,View Keyword and Fetched Files ,View Same Data Files
View All Users, View All Documents ,View Top 'K' Keywords, View Keywords and Links ,View Time Delay of Files ,View User Transactions ,View File Rank Results ,View Time Delay Comparison Results
Register with the system, Upload Products
Response
Upload Document
Request
Client
View Their Own Details
View Document Search Comparison

Fig: System Architecture

IV. IMPLEMENTATION

- CLOUD
- CLIENT

MODULES DESCRIPTION

CLOUD

In this module, the Cloud has to login by using valid user name and password. After login successful he can perform some operations such as View All Users, View All Documents, View Top 'K' Keywords, View Keywords and Links, View Time Delay of Files, View User Transactions, View File Rank Results View Time Delay Comparison Results

Friend Request & Response

In this module, the admin can view all the friend requests and responses. Here all the requests and responses will be displayed with their tags such as Id, requested user photo, requested user name, user name request to, status and time & date. If the user accepts the request then the status will be changed to accepted or else the status will remains as waiting

CLIENT

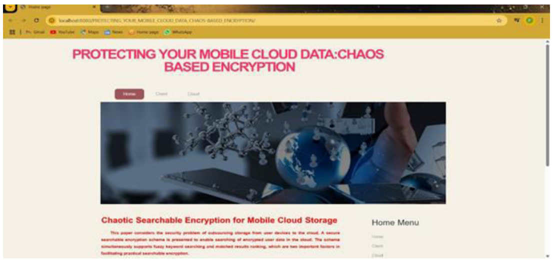
In this module, there are n numbers of clients are present. Client should register before performing any operations. Once Client registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password.

Verify finger print and Login Once Login is successful Client can perform some operations like View Profile, Upload Document, Edit / Delete Document, Search Cloud Data, View Document Search Comparison, View Keyword and Fetched Files, View Same Data Files

Searching Users to make friends

In this module, the user searches for users in Same Network and in the Networks and sends friend requests to them. The user can search for users in other Networks to make friends only if they have permission

V. SCREENSHOTS

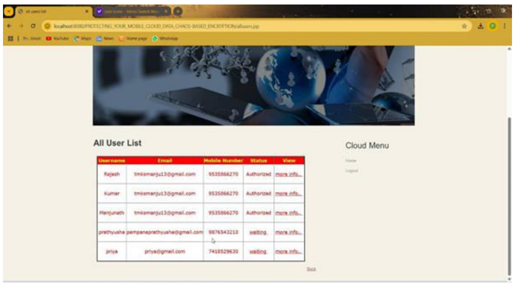


PROTECTING YOUR MOBILE CLOUD DATA:CHAOS BASED ENCRYPTION

Chaotic Searchable Encryption for Mobile Cloud Storage

This paper considers the security problem of outsourcing storage from user devices to the cloud. A secure searchable encryption scheme is presented to enable searching of encrypted user data in the cloud. The scheme simultaneously supports fuzzy keyword searching and matched results ranking, which are two important factors in facilitating practical searchable encryption.

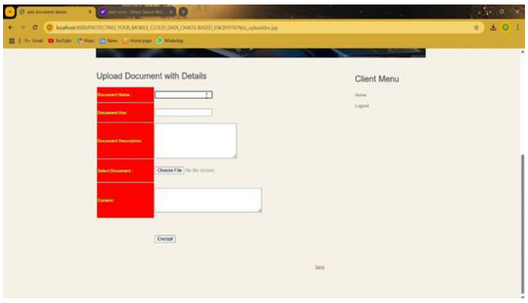
FIG-1: Home Screen



All User List

Username	Email	Mobile Number	Status	View
Rajesh	tmksmanju13@gmail.com	9535866270	Authorized	more info...
Kumar	tmksmanju13@gmail.com	9535866270	Authorized	more info...
Manjunath	tmksmanju13@gmail.com	9535866270	Authorized	more info...
prathyusha	pampanaprathyusha@gmail.com	9876543210	waiting	more info...
priya	priya@gmail.com	7418529630	waiting	more info...

FIG-2: All user list



Upload Document with Details

Document Name :

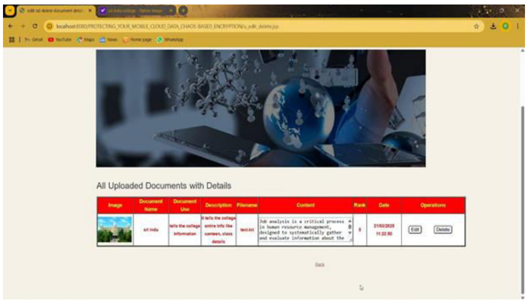
Document Use :

Document Description :

Select Document : Choose File No file chosen

Content :

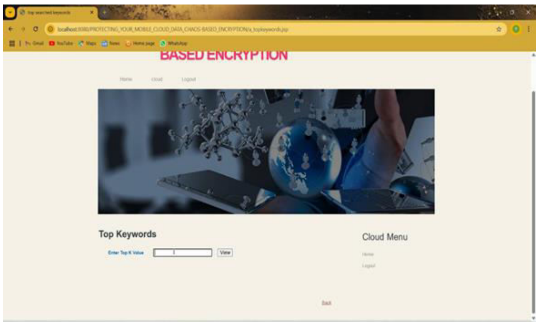
FIG-3: Upload document with details



All Uploaded Documents with Details

Image	Document Name	Document Use	Description	Filename	Content	Rank	Date	Operations
	sri india	tells the college information	it tells the college entire info like canteen, class details	test.txt	Job analysis is a critical process in human resource management, designed to systematically gather and evaluate information about the	0	21/03/2025 11:22:50	Edit Delete

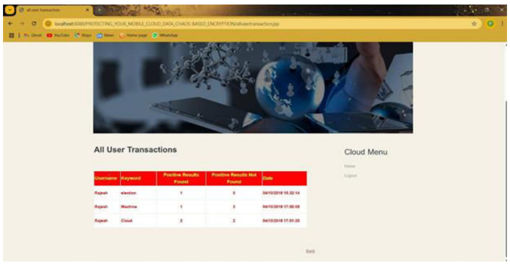
FIG-4: All Document list



Top Keywords

Enter Top K Value:

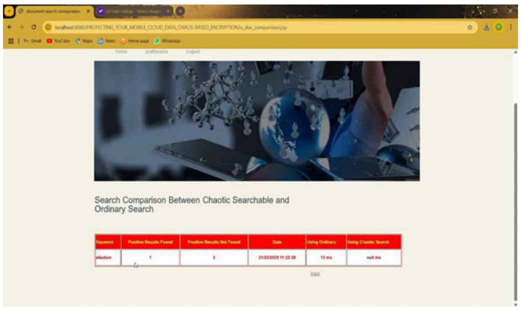
FIG-5: Top keyword



All User Transactions

Username	Keyword	Positive Results Found	Positive Results Not Found	Date
Rajesh	election	1	0	04/10/2018 15:22:14
Rajesh	Machine	1	3	04/10/2018 17:00:05
Rajesh	Cloud	2	2	04/10/2018 17:01:20

FIG-6: All user transactions



Search Comparison Between Chaotic Searchable and Ordinary Search

Keyword	Positive Results Found	Positive Results Not Found	Date	Using Ordinary	Using Chaotic Search
election	1	3	21/03/2025 11:23:38	12 ms	null ms

FIG-7: Chaotic Search

VI. CONCLUSION

CONCLUSION

In this paper, we proposed the first chaos based searchable encryption approach which also allows both ranked and fuzzy keyword searches on the encrypted data stored in the cloud. Our approach guarantees the privacy and confidentiality of the user even vis-à-vis the cloud provider who is semi-trusted in our case. The proposed method is designed to achieve effective retrieval of remotely stored encrypted data for mobile cloud computing scenarios. This scheme is implemented and evaluated using two databases: RFCs and the Enron database.

FUTURE SCOPE

The proposed scheme uses chaotic random noise to improve the strength of encryption keys. The strength of the encryption keys does not rely on the length of the key but the random and chaotic nature of the input noise. Several experiments were conducted to test different aspects of the solution implemented. Overall, it is concluded, based on the results, that chaos theory can be applied in cryptography to improve the strength of ciphers. The result show that Cryptor is a lightweight, strong client-end encryption scheme. Hence, Cryptor is a better encryption scheme in terms of encryption and decryption times. The chaos-based encryption keys can be used to improve the strength of existing cryptosystems such as DES, 3-DES and AES. Future perspectives include: experimenting on encrypting multimedia digital content, implementing the Cryptor system to have rounds of encryption to increase layers of security, and to test the proposed neural key store against various types of key attacks. Searchable encryption (SE) allows searching over encrypted data in the cloud and returns to the user the data that correspond to the given keywords, without having to reveal the keywords.

REFERENCES

1. B.Yang, X. Pang, Q. Du, and Dan Xie, "Effective Error-Tolerant Keyword Search for Secure Cloud Computing," Journal of computer science and technology, vol. 29, no.1, pp. 81 89, Jan. 2014.
2. D. Boneh, G. D. Crescenzo, "Public key encryption with keyword search," in C. Cachin and
3. J. Camenisch, editors, Advances in Cryptology, Eurocrypt, vol. 3027 of LNCS, pp. 506 522, Springer, 2004.
4. S. Kamara, K. Lauter, "Cryptographic cloud storage, " in Financial Cryptography and Data Security, pp. 136-149, Springer Berlin Heidelberg, 2010.
5. S. Kamara, C. Papamanthou, T. Roeder, "CS2: A searchable cryptographic cloud storage system," Microsoft Research, Tech. Report MSR-TR, 2011.
6. Y. Earn, R. Alsaqour, M. Abdelhaq, T. Abdullah, "Searchable symmetric encryption: review and evaluation," Journal of Theoretical and Applied Information Technology, vol. 30, 2011.
7. R. Koletka, A. Hutchison, "An architecture for secure searchable cloud storage," IEEE, Information Security South Africa (ISSA), pp. 15-17, Aug., 2011.
8. E. Stefanov, C. Papamanthou, E. Shi, "Practical Dynamic Searchable Encryption with Small Leakage," IACR Cryptology ePrintArchive, 2013.
9. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," INFOCOM, 2010 Proceedings IEEE, Dept. of ECE, Illinois Inst. of Technol., Chicago, IL, USA, Mar. 2010.
10. J. Bringer, H. Chabanne, B. Kindarji, "Error-tolerant searchable encryption," Communication and Information Systems Security Symposium, International Conference on Communications (ICC), Dresden, Germany, pp. 14-18, Jun. 2009.
11. J. Yu, J. Li, X. Wang, W. Gao, "Conjunctive Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," TELKOMNIKA Indonesian Journal of Electrical Engineering, vol.12, no.3, pp. 2104-2109, Mar. 2014. 75
12. S. R. Chidamber and C. F. Kemerer, „„A metrics suite for object oriented design,““ IEEE Trans. Softw. Eng., vol. 20, no. 6, pp. 476–493, Jun. 1994.
13. R. Harrison, S. J. Counsell, and R. V. Nithi, „„An evaluation of the MOOD set of object oriented software metrics,““ IEEE Trans. Softw. Eng., vol. 24, no. 6, pp. 491– 496, Jun. 1998.
14. R. V. Binder, „„Design for testability in object-oriented systems,““ Comms. ACM, vol. 37, no. 9, pp. 87–101, Sep. 1994.
15. S. Purao and V. Vaishnavi, „„Product metrics for object-oriented systems,““ ACM Comput. Surveys, vol. 35, no. 2, pp. 191–221, Jun. 2003.
16. M. Lorenz and J. Kidd, Object-Oriented Software Metrics: A Practical Guide. Upper Saddle River, NJ, USA: Prentice-Hall, 1994.
17. B. Henderson-Sellers, L. L. Constantine, and I. M. Graham, „„Coupling and cohesion (towards a valid metrics suite for objectoriented analysis and design),““ Object Oriented Syst., vol. 3, no. 3, pp. 143–158, Sep. 1996.
18. V. R. Basili, L. C. Briand, and W. L. Melo, „„A validation of object-oriented design metrics as quality indicators,““ IEEE Trans. Softw. Eng., vol. 22, no. 10, pp. 751– 761, Oct. 1996.
19. G. Costagliola, F. Ferrucci, G. Tortora, and G. Vitiello, „„Class point: An approach for the size estimation of object-oriented systems,““ IEEE Trans. Softw. Eng., vol. 31, no. 1, pp. 52– 74, Jan. 2005.
20. S. L. Pfleeger and J. M. Atlee, Software Engineering: Theory and Practice. Chennai, India: Pearson Ed., 1998.