ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Dual-Server Hybrid Key Encryption with Multi Keyword Search Scheme for Secure Cloud Storage

Sneha R. Ghorpade[1], Prof. Dr. S. N. Kini[2]

M. E Student, Department of Computer Engineering, Jaywantrao Sawant College of Engineering, Pune, India.[1]

Asst. Professor, Department of Computer Engineering, Jaywantrao Sawant College of Engineering, Pune, India[2]

ABSTRACT: Searchable encryption is of expanding interest for ensuring the information protection in secure searchable cloud storage. In this work, we research the security of a notable cryptographic primitive, to be specific Public Key Encryption with Keyword Search (PEKS). In existing, Rongmao Chen and Yi Mu formalized a Public Key Encryption with Keyword Search (PEKS) structure named Dual Server Public Key Encryption with Keyword Search (DSPEKS) to address the security weakness of PEKS. Unfortunately, it has been demonstrated that the said work can't functions admirably on Query Complexity, (for example, encoded multi-keyword search) and gives less security. To handle the Query Complexity issue, we proposed a novel Dual-Server Hybrid Key Encryption with Multi Keyword Search Scheme for secure distributed storage. For more security, we propose half breed encryption. Half breed encryption is a method of encryption that unions at least two encryption frameworks. It consolidates a blend of deviated and symmetric encryption to profit by the qualities of every type of encryption. These qualities are individually characterized as speed and more security. To additionally enhance the current takes a shot at seeking, an essential and principal capacity is to empower the multi-watchword look with the far reaching rationale operations, i.e., the "AND", "OR" and "NO" operations of catchphrases. This is key for hunt clients to prune the seeking space and rapidly recognize the craved information. By examinations we demonstrate that proposed approach in view of double server half and half key encryption beats existing DSPEKS plot it terms of security and simplicity of supporting multi-watchword seek.

KEYWORDS: Multiple Keyword search, Hybrid encryption.

I. INTRODUCTION

Cloud storage outsourcing has turned into a well known application for endeavors and associations to decrease the weight of keeping up huge information as of late. In any case, in all actuality, end clients may not by any stretch of the imagination believe the cloud capacity servers and may want to scramble their information some time recently transferring them to the cloud server so as to secure the information protection. This as a rule makes the information use more troublesome than the conventional stockpiling where information is kept in the nonappearance of encryption. One of the run of the mill arrangements is the searchable encryption which permits the client to recover the scrambled records that contain the client indicated catchphrases, where given the watchword trapdoor, the server can discover the information required by the client without unscrambling.

Searchable encryption can be acknowledged in either symmetric on the other hand awry encryption setting. In [2], Song et al. proposed watchword seek on ciphertext, known as Searchable Symmetric Encryption (SSE) and a short time later a few SSE plans [3], [4] were intended for changes. In spite of the fact that SSE plans appreciate high productivity, they experience the ill effects of convoluted mystery key circulation. Correctly, clients need to safely share mystery keys which are utilized for information encryption. Else they are not ready to share the encoded information outsourced to the cloud. To determine this issue, Boneh et al. [5] presented a more adaptable primitive, to be specific Public Key Encryption with Keyword Search (PEKS) that empowers a client to look encoded information in the deviated encryption setting. In a PEKS framework, utilizing the beneficiary's open key, the sender appends some

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

encoded watchwords (alluded to as PEKS cipher texts) with the encoded information. The collector at that point sends the trapdoor of a to-be-looked catchphrase to the server for information looking. Given the trapdoor and the PEKS cipher text, the server can test whether the watchword hidden the PEKS cipher text is equivalent to the one chose by the collector. Provided that this is true, the server sends the coordinating scrambled information to the collector.
Using distributed computing, people can store their information on remote servers and permit information access to open clients through the cloud servers. As the outsourced information are probably going to contain touchy protection data, they are normally encoded before transferred to the cloud. This, be that as it may, altogether confines the ease of use of outsourced information because of the trouble of looking over the encoded information. In this work, we explore the security of an outstanding cryptographic primitive, in particular Public Key Encryption with Keyword Search (PEKS) which is extremely valuable in numerous utilizations of distributed storage. Unfortunately, it has been demonstrated that the conventional PEKS system experiences an inborn frailty called inside Keyword Guessing Attack (KGA) propelled by the noxious server. To address this security powerlessness, we require another PEKS system.

PEKS plans experience the ill effects of a characteristic uncertainty with respect to the trapdoor catchphrase protection, to be specific inside Keyword Guessing Attack (KGA). The reason prompting to such a security powerlessness is, to the point that any individual who knows collector's open key can produce the PEKS ciphertext of self-assertive watchword himself. Specifically, given a trapdoor, the antagonistic server can pick a speculating watchword from the catchphrase space and after that utilization the catchphrase to produce a PEKS ciphertext. The server then can test whether the speculating watchword is the one basic the trapdoor. This speculating then-testing method can be rehashed until the right catchphrase is found. Such a speculating assault has additionally been considered in numerous secret key based frameworks. Notwithstanding, the assault can be propelled all the more effectively against PEKS plans since the watchword space is generally the same as a typical lexicon (e.g., all the important English words), which has a much littler size than a secret word reference (e.g., every one of the words containing 6 alphanumeric characters). It is important that in SSE plans, just mystery key holders can create the catchphrase ciphertext and consequently the ill-disposed server is not ready to dispatch within KGA. As the watchword dependably shows the protection of the client information, it is along these lines of down to earth significance to defeat this security risk for secure searchable scrambled information outsourcing.

Searchable encryption can be acknowledged in either symmetric or awry encryption setting. Tune et al. proposed watchword seek on ciphertext, known as Searchable Symmetric Encryption (SSE) and a short time later a few SSE plans were intended for changes. Although SSE plans appreciate high productivity, they experience the ill effects of entangled mystery key circulation. Correctly, clients need to safely share mystery keys which are utilized for information encryption. Else they are not ready to share the encoded information outsourced to the cloud. To resolve this issue, Boneh et al. presented a more adaptable primitive, to be specific Public Key Encryption with Keyword Search (PEKS) that empowers a client to seek scrambled information in the hilter kilter encryption setting. In a PEKS framework, utilizing the recipient's open key, the sender appends some scrambled catchphrases (alluded to as PEKS ciphertexts) with the encoded information. The recipient then sends the trapdoor of a to-be-hunt watchword to the server down information looking. Given the trapdoor and the PEKS ciphertext, the server can test whether the catchphrase fundamental the PEKS ciphertxt is equivalent to the one chose by the collector. Provided that this is true, the server sends the coordinating scrambled information to the recipient.

II. RELATED WORK

R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu [1], " A study on Order-preserving encryption for numeric data ", proposed On Cloud to secure User's delicate information Encryption is one of the best system. In any case, performing seek over such encoded database has dependably been a testing assignment in writing. So Author's available a request protecting encryption conspire named as OPES for numeric information that permits inquiries with correlation administrators to be straightforwardly connected to encoded numeric sections. Question comes about neither contain any false positive nor miss any answer tuple. The specified plan handles overhauls smoothly without activating changes in the encryption of different qualities.

D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano [2] A Public key encryption with keyword search has proposed that Searchable symmetric encryption (SSE) permits a gathering to outsource the capacity of his information

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

to another gathering in a private way, while keeping up the capacity to specifically look over it. This issue has been the concentration of dynamic research and a few security definitions and developments have been proposed. In spite of the fact that SSE plans appreciate high effectiveness, they experience the ill effects of confused mystery key dissemination. Definitely, clients need to safely share mystery keys which are utilized for information encryption. Else they are not ready to share the scrambled information outsourced to the cloud. To determine this issue, Boneh l. presented a more adaptable primitive, to be specific Public Key Encryption with Keyword Search (PEKS) that empowers a client to look scrambled information in the topsy-turvy encryption setting. In a PEKS framework, utilizing the recipient's open key, the sender joins some scrambled watchwords (alluded to as PEKS figure writings) with the encoded information. The collector then sends the trapdoor of a to-be-hunt watchword to the server down information seeking. Given the trapdoor and the PEKS figure message, the server can test whether the catchphrase hidden the PEKS figure content is equivalent to the one chose by the collector. Assuming this is the case, the server sends the coordinating encoded information to the recipient.

M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi et al., [3] proposed "A Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions" shows Creator's formalized anonymous IBE (AIBE) and displayed a non specific development of searchable encryption from AIBE. They likewise demonstrated to exchange a hierarchical IBE (HIBE) scheme into an public key encryption with temporary keyword search (PETKS) where the trapdoor is just legitimate in a particular time interim.

J. Baek, R. Safavi-Naini, and W. Susilo [4], " A Public key encryption with keyword search revisited ", It proposes that The first PEKS plot requires a protected channel to transmit the trapdoors. To beat this constraint, Author's proposed another PEKS plot without requiring a safe channel, which is alluded to as a secure channel-free PEKS (SCF-PEKS). The thought is to include the server's open/private key combine into a PEKS framework. The catchphrase figure content and trapdoor are produced utilizing the server's open key and thus just the server (assigned analyzer) can play out the pursuit. New PEKS plot specified as SCF-PEKS don't requires a protected channel to transmit trapdoor as in conventional PEKS.In this Mentioned conspire the assailant is permitted to get the relationship between the non-challenge figure writings and the trapdoor. Outside foes can catch the trapdoors sent in an open channel can uncover the encoded watchwords through disconnected catchphrase speculating assaults and they can perform disconnected watchword speculating assaults against the said (SCF-PEKS) plans.

As per R. Cramer and V. Shoup et al., [5] "A Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption" In this paper Authors proposes smooth projective hash work (SPHF). Many plan in writing turns out to be effective against versatile Chosen figure content assault however every one of them require a trusted outsider contribution during the time spent client enrollment for both sender and recipient. Creators then propose a down to earth conspire that can be demonstrated secure against versatile picked figure content assault under a sensible obstinacy supposition is smooth projective hash function (SPHF) that of Cramer and Shoup . This plan depends on Paillier's Decision Composite Residuosity (DCR) suspicion [P], while another is situated in the established Quadratic Residuosity (QR) presumption.

III. PROPOSED SYSTEM

Using distributed computing, people can store their information on remote servers and permit information access to open clients through the cloud servers. As the outsourced information are probably going to contain touchy protection data, they are normally encoded before transferred to the cloud. This, be that as it may, altogether confines the ease of use of outsourced information because of the trouble of looking over the encoded information. In this work, we explore the security of an outstanding cryptographic primitive, in particular Public Key Encryption with Keyword Search (PEKS) which is extremely valuable in numerous utilizations of distributed storage. Unfortunately, it has been demonstrated that the conventional PEKS system experiences an inborn frailty called inside Keyword Guessing Attack (KGA) propelled by the noxious server. To address this security powerlessness, we require another PEKS system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Searchable encryption can be acknowledged in either symmetric or awry encryption setting. Tune et al. proposed watchword seek on cipher-text, known as Searchable Symmetric Encryption (SSE) and a short time later a few SSE plans were intended for changes. Although SSE plans appreciate high productivity, they experience the ill effects of entangled mystery key circulation. Correctly, clients need to safely share mystery keys which are utilized for information encryption. Else they are not ready to share the encoded information outsourced to the cloud. To resolve this issue, Boneh et al. presented a more adaptable primitive, to be specific Public Key Encryption with Keyword Search (PEKS) that empowers a client to seek scrambled information in the hilter kilter encryption setting. In a PEKS framework, utilizing the recipient's open key, the sender appends some scrambled catchphrases (alluded to as PEKS cipher-texts) with the encoded information. The recipient then sends the trapdoor of a to-be-hunt watchword to the server down information looking. Given the trapdoor and the PEKS cipher-text, the server can test whether the catchphrase fundamental the PEKS cipher-text is equivalent to the one chose by the collector. Provided that this is true, the server sends the coordinating scrambled information to the recipient.

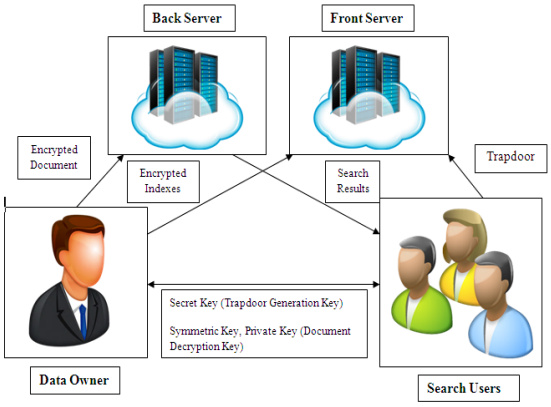

Figure.1. System Architecture

The information proprietor outsources her information to the cloud for advantageous and dependable information access to the relating look clients. To ensure the information protection, the information proprietor encodes the first information through symmetric with open key encryption then produce a hash signature utilizing Smooth Projective Hash Functions (SPHFs). To enhance the hunt productivity, the information proprietor creates a few watchwords for each outsourced record. The comparing file is then made by watchwords and a mystery key. After that, the information proprietor sends the scrambled archives with hash marks to back server and the comparing files to the front server, and sends the symmetric key, mystery and private key to pursuit clients. A hunt client inquiries the outsourced reports from the cloud server with taking after three stages. In the first place, the hunt client gets all the symmetric key, mystery key and private key from the information proprietor. Second, as per the hunt catchphrases, the pursuit client utilizes the mystery key to produce trapdoor and sends it to the front server. At the point when an inquiry client sends a watchword trapdoor to the front server, it would separate a gathering of coordinating archives in light of specific operations. Ultimately, she gets the coordinating record gathering from the cloud server and decodes them with the symmetric and private keys. At long last it creates another hash signature for decoded report. At that point coordinated both hash marks are equivalent or not. In the event that both are equivalent, report is protected. Generally are not protected.

A. *Design Considerations:*

- Before requesting for upload owner must have generated Private Key.
- Trapdoor is generated using the secret key.
- Decrypt the document only if Keys provided is satisfied with set of documents.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

B. *Description of the Proposed Algorithm:*

Anonymization / encrypt and upload
Encrypt Document based on Symmetric Key (AES Encryption) --> Cipher text and generate hash signature using Smooth Projective Hash Functions (SPHFs).
Encrypt that Cipher text once again based on Public Key (RSA Encryption) --> Ciphertext1
Encrypt Keywords based on Secret Key --> index
Encrypt that index once again based on Data Owner Identity (Identity Based Encryption) --> Encrypted Index

Duplication check to reduce data on cloud storage eliminating duplicate copies of repeating data

Search user:
Encrypt Search Keywords based on Secret Key --> trapdoor
Encrypt that trapdoor once again based on Data Owner Identity (Identity Based Encryption) --> Encrypted trapdoor
Send Encrypted trapdoor with any one Operation (AND, OR, NO) to front Server. Now front server match the trapdoor to all indexes and find the matched document
Then Retrieve the matched encrypted document collections with hash signature from back server and forward to user.
Encrypted Documents (Ciphertext1) --> Decrypt that C1 based on Private Key (RSA Decryption) --> Cipher text

The information proprietor outsources her information to the cloud for advantageous and dependable information access to the relating look clients. To ensure the information protection, the information proprietor encodes the first information through symmetric with open key encryption then produce a hash signature utilizing Smooth Projective Hash Functions (SPHFs). To enhance the hunt productivity, the information proprietor creates a few watchwords for each outsourced record. The comparing file is then made by watchwords and a mystery key. After that, the information proprietor sends the scrambled archives with hash marks to back server and the comparing files to the front server, and sends the symmetric key, mystery and private key to pursuit clients. A hunt client inquiries the outsourced reports from the cloud server with taking after three stages. In the first place, the hunt client gets all the symmetric key, mystery key and private key from the information proprietor. Second, as per the hunt catchphrases, the pursuit client utilizes the mystery key to produce trapdoor and sends it to the front server. At the point when an inquiry client sends a watchword trapdoor to the front server, it would separate a gathering of coordinating archives in light of specific operations. Ultimately, she gets the coordinating record gathering from the cloud server and decodes them with the symmetric and private keys. At long last it creates another hash signature for decoded report. At that point coordinated both hash marks are equivalent or not. In the event that both are equivalent, report is protected. Generally are not protected.

IV. PSEUDO CODE

The Pseudo code for the system is as follows:
Step 1) Register
Step 2) Login
Step 3) Symmetric Key (AES), Secret Key (DES), Public and Private Key Generation
Step 4) Enter Document name and contents of Document
Step 5) Enter Some Keywords about Document
Step 6) Encrypt Document based on Symmetric Key (AES Encryption) --> Ciphertext and generate hash signature using Smooth Projective Hash Functions (SPHFs). Encrypt that Ciphertext once again based on Public Key (RSA Encryption) --> Ciphertext1
Step 7) Encrypt Keywords based on Secret Key --> index. Encrypt that index once again based on Data Owner Identity (Identity Based Encryption) --> Encrypted Index
Step 8) Upload Ciphertext1 with hash signature to back server and Encrypted Index to front Server
Step 9) Send Symmetric, Secret and Private Keys to Authenticated Search Users

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

V. SIMULATION RESULTS

In this paper, we proposed a new framework, Dual-Server Hybrid Key Encryption with Multi Keyword Search Scheme for secure cloud storage (DSPEKS), that can tackle the Query Complexity problem of existing DSPEKS framework. We also introduced a new Smooth Projective Hash Function (SPHF) and used it to construct a generic DSPEKS scheme. An efficient instantiation of the new SPHF based on the Diffie-Hellman problem is also presented in the paper, which gives an efficient DS-PEKS scheme without pairings.

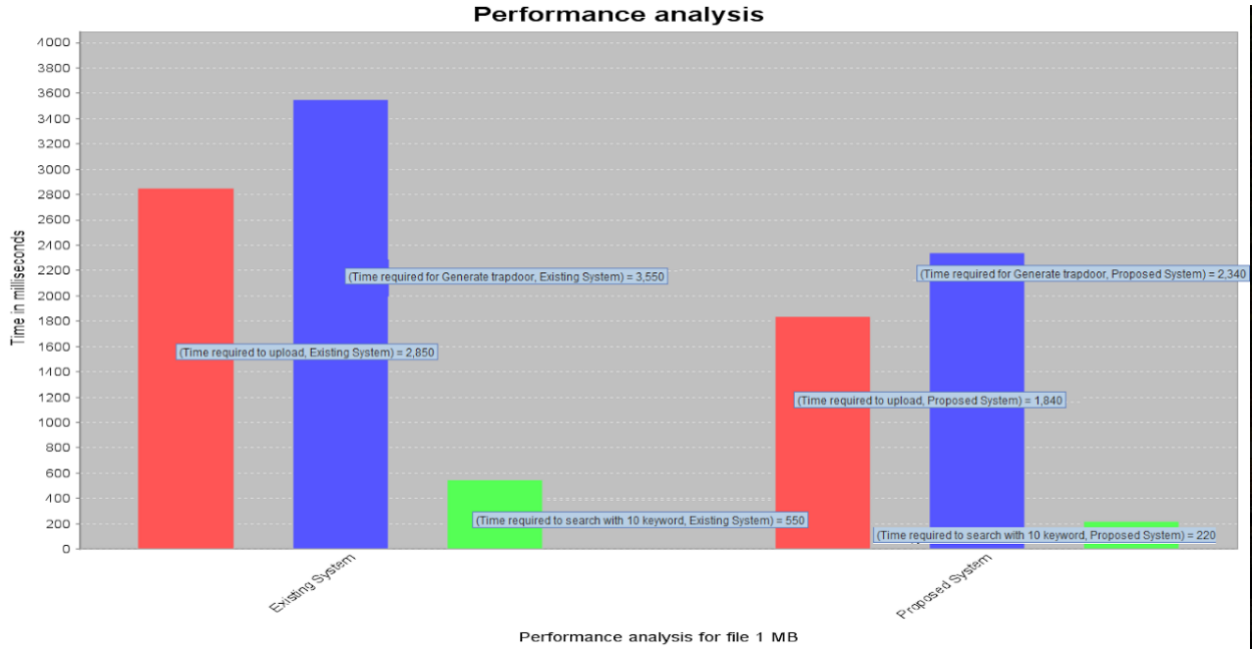

Figure.2 Performance analysis

Figure 1. shows Graph is expected for document D , red color says Time required to upload , blue color Time required for Generate trapdoor , green color Time required to search with 10 keyword

VI. CONCLUSION AND FUTURE WORK

In this paper, we proposed a new framework, Dual-Server Hybrid Key Encryption with Multi Keyword Search Scheme for secure cloud storage (DSPEKS), that can tackle the Query Complexity problem of existing DSPEKS framework. We also introduced a new Smooth Projective Hash Function (SPHF) and used it to construct a generic DSPEKS scheme. An efficient instantiation of the new SPHF based on the Diffie-Hellman problem is also presented in the paper, which gives an efficient DS-PEKS scheme without pairings.

Our framework designed currently secures data transmission and allows data owner to search using multiple keyword search using various logic operations as like AND, OR, NOT. In future we plan to address the same issue in to work for multi cloud environment.

REFERENCES

1. R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, “A new general framework for secure public key encryption with keyword search,” in Information Security and Privacy - 20th Australasian Conference, ACISP, pp. 59–76, 2015.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

2. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in IEEE Symposium on Security and Privacy, pp. 44–55, 2000.
3. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order-preserving encryption for numeric data," in Proceedings of the ACM SIGMOD International Conference on Management of Data, pp. 563–574, 2004.
4. R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, pp. 79–88 , 2006.
5. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in EUROCRYPT, pp. 506–522 , 2004.
6. R. Gennaro and Y. Lindell, "A framework for password-based authenticated key exchange," in EUROCRYPT, pp. 524–543, 2003.
7. M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions," in CRYPTO, pp. 205–222, 2005.
8. D. Khader, "Public key encryption with keyword search based on k-resilient IBE," in Computational Science and Its Applications - ICCSA, pp. 298–308, 2006.
9. P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," IEEE Trans. Computers, vol. 62, no. 11, pp. 2266– 2277, 2013.

BIOGRAPHY

Sneha R. Ghorpade is a ME student of Computer Department, Jayawantrao Sawant College of Engineering Hadapsar, Savitribai Phule Pune University.