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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Secure Online Transaction with Hybrid Recommendation System

Aditya Chavan[1], Ajay Mangaj[2], Pritesh Joshi[3], Priti Mithari[4]

B.E Student, Department of Computer Engineering, Pune University, India[1, 2, 3]

Assistant Professor, Department of Computer Engineering, Pune University, India[4]

ABSTRACT: Recommendation System is used for referring products to the user. The objective of filtering is to help users to find out products which they would be interested in. However, current ways suffering from such issues as lack of information, quality, and big inaccuracy in predictions. The paper tends to implement the object normality from psychology and gives a unique Typicality-based Collaborative filtering recommended technique named TyCo. A defining characteristic of Collaborative filtering is that it finds different users in neighbours of users supported user typicality grouped in user teams. E-commerce market is developing rapidly in last 5 years. The ever increasing feature of online searching, Debit or MasterCard scam and private data protection area unit major issues for customers, merchants and banks especially within the case of condition where Card Not Present. The paper gives the implementation about the recommendation system with filtering methods and online payment gateway system using image steganography.

KEYWORDS: Steganography, Online shopping, E-Commerce, Encryption.

I. INTRODUCTION

In rapidly developing E-Commerce market setting, online searching has developed in quality over the years, primarily as a result of people notice it convenient and simple to discount, search from the ease of their home or workplace. During this paper, we have a propensity to area of unit specializing in protection of customer's personal data during on-line searching. On-line searching may be a method of electronic commerce that permits customers to directly get products or services from a vendor over the net employing a browser.

Steganography is the ability of concealing a file, message, image, or video inside another file, message, image, or video [4].The good quality thing about Steganography over cryptography is that, supposed secret message doesn't attract interest to itself as an object of Examination. Plainly noticeable encrypted messages—no matter how much strong—arouse interest, and should in themselves be incriminatory in countries wherever cryptography is forbidden. Thus, whereas cryptography is the ability of securing the contents of a message alone, Steganography is concerned with concealing the very truth that a secret message is being sent, in addition with concealing the contents of the message.

Encryption is that the technique of cryptography messages or data in such the way that exclusively approved parties will surf it. The invented communication, data or message, remarked as plaintext, is encrypted generating cipher text which will exclusively be browse if decrypted. Associate degree secret writing theme sometimes uses pseudo-random secret writing key generated by associate degree formula [2].Electronic commerce is commerce in goods or services mistreatment laptop networks, like the net. Electronic commerce attracts on technologies like mobile E-commerce, electronic funds transfer, provide chain management; web selling, on-line dealing process, Electronic knowledge Interchange (EDI), inventory management systems, and automatic knowledge assortment systems [4].The Major troubles in online shopping are Identity theft and phishing. Identity theft is that the crime of getting the confidential or money info of another person for the only purpose of forwards that person's name or identity so as to form transactions or purchases or the misleading observe of mistreatment another person's name and private info so as to get credit, loans, etc. [6]. Example- In 2010, 7.0% of social unit within the U.S. had a minimum of one member expertise fraud. At about 8.6 million households, 7.0% aren't any tiny threat, thus it's vital to remain on your toes once it involves Information security. Phishing is used to acquire sensitive data like usernames, passwords and MasterCard details (generally, indirectly, money), typically for malicious reasons, by masquerading as a trustworthy entity in associate transmission [2] [3]. Phishing email can usually direct the user to go to a web page wherever they're asked to fill or update personal data, like an Arcanum, MasterCard, Social protection, or verifying account numbers that the genuine organization

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

already has. Phishers target the shoppers of banks and on-line payment services. Emails, purportedly from the inner Revenue Service, are accustomed obtain sensitive knowledge from U.S. taxpayers. Recent analysis has shown that phishers could in theory be ready to confirm that banks potential victims use and target imitative emails consequently.

Providing a new method which uses steganography and visual cryptography based on text [7], i.e. text-based Steganography that decreases the sharing of information between consumer and online merchantman but empower successful fund transfer from the consumer's account to merchantman's account by protecting customers personal information and anticipating misuse of information from merchants end. Paper implements an Image Steganography and cryptography techniques to provide security to customer's transaction details [2]. The previous transaction history of customer is used to provide a product recommendation [1].

Recommendation technique is use to advise various products or items to the user based on rating given by the related group of other users having same interest and most searched by the user. This paper implements three techniques to recommend products to theuser. Content-Based Recommender technique of such type of recommendation methods comes from the reality that people had their personal assessments on some items in the past and will have the same assessments on other items in the future.Collaborative filtering recommendation technique calculates the associating of active users on items based on the preferences of other items or similar users. Third and the last technique is Hybrid technique which is mixture of both Collaborative and Content Based Filtering technique [1].

II. RELATED WORK

A. *Steganography*:

Steganography is the technique of concealing messages or information within other non-secret text or data or hiding of a secret message within a normal message and the extraction of it at its destination or maybe is the practice of concealing a file, message, Text [4], image [5], audio [6], or video within another file, message, image, or video.

Using text based Steganography, the message remains hidden. For hiding this message various methods are used like shifting the word and line, in open spaces, in word sequence. There are various advantages of choosing text steganography on behalf of other Steganography tec. [2] by making some slight changes to colour values, for example, you can exchange some bits that are practically undetectable. Visual Cryptography (VC) is proposed by MoniNaor and Adi Shamir, in 1994 [10].Video steganography is very important to transmit the important data like banking and military information in a protected manner. It is the process of hiding some secret information inside a video.

Audio Steganography it is a method used to transfer hidden info by altering an audio signal in an unnoticeable manner.

B. *Visual cryptography:*

Visual cryptography is a cryptographic procedure which permits visual information (pictures, text, etc.) to be encrypted in such a technique that decryption converts a mechanical process that does not require a computer. One of the best-known techniques has been credited by Adi Shamir and MoniNaor, who developed it in 1994.[1] They demonstrated a graphic secret structure, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any $n - 1$ parts revealed no information about the original image[8]. Each share was printed on a distinct transparency, and decryption was done by overlaying the shares. When all $n$sharewas overlaid, the original image would appear. There are several simplifications of the basic system, including k-out-of-n visual cryptography [2][3].

C. *Encryption*

Encryption is the procedure of converting plain text data (plaintext) into approximately that appears to be random and worthless (cipher text). Decryption is the process of translating cipher text back to plaintext. To encrypt more than a small quantity of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a specific piece of cipher text, the key that was used to encrypt the data must be used [3].

D. *Recommender System*

Now-a-days there have been many works on recommender systems and most of these works focus on developing new methods of recommending items to users the objective of recommender systems is to assist users to find out items which they would be interested in. Currently, recommendation methods are mainly classified into hybrid methods, content based (CB), collaborative filtering (CF)[2].

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

1. *Content Based Recommender Systems*

Content-Based Recommender Systems of such kind of recommendation methods comes from the fact that people had their subjective assessments on some items in the past and will have the similar assessments on other similar items in the future. The descriptions of items are examined to identify fascinating items for users in CB recommender systems. Based on the items a user has rated, a CB recommender learns a summary of the user's preferences or user's interests [11]. According to a user's interest summary, the items which are comparable to the ones that the user has rated highly in the past or preferred will be recommended to the user. For CB recommender systems, it is vital to learn users' profiles. Various learning approaches have been applied to construct profiles of users [2].

2. *Collaborative Filtering*

Collaborative filtering recommendation methods predict the likings of active users on items based on the preferences of other items or similar users. There are two kinds of CF methods, namely item-based CF approach and user-based CF approach. The basic idea of user-based CF approach is to provide reference of an item for a user based on the views of other like-minded users on that item. The basic idea of item-based CF approach is to provide a user with the reference of an item based on the. The user-based CF, the item-based CF approach first finds out a set of nearest "neighbors" (similarly items) for each item [11]. The item based CF recommender systems try to predict a user's ranking on an item based on the ratings given by the user on the neighbors of the target item. For each user-oriented collaborative Filtering and item-oriented collaborative Filtering, the measuring of similarity between users or things could be a vital step. Pearson correlation coefficient, cosine-based similarity, vector house similarity, so on is wide utilized in association measuring in CF strategies. Combining externally specified aggregate ratings information in CF methods [2].

3. *Hybrid Recommender*

Hybrid Recommender Systems are a combination of collaboration and content based methods, so as to help avoid some limitations of content-based and collaborative systems. Naive hybrid approach is to implement collaborative and CB methods separately, and then combines their predictions by a combining function, such as a linear combination of ratings or a voting scheme or other metrics. Some hybrid recommender systems combine item-based CF and user-based CF [11].Hybrid recommender systems combine two or more recommendation techniques to gain better performance with fewer of the drawbacks of any individual one. Most commonly, collaborative filtering is combined with some other technique in an attempt to avoid the ramp-up problem [1].

III. PROPOSED ALGORITHM

Proposed system based onImage Steganography and cryptography techniques to provide security to customer's transaction details.Proposed system combined image based Steganography and visual cryptography authentication system is used for customer authentication in core banking.

A. *System Overview*

Conceptual model defines the System architecture or systems overview which structure, behaviour and more views of a system. System overviews provide a plan that will work together to implement the overall system which products can be procured, and systems developed.

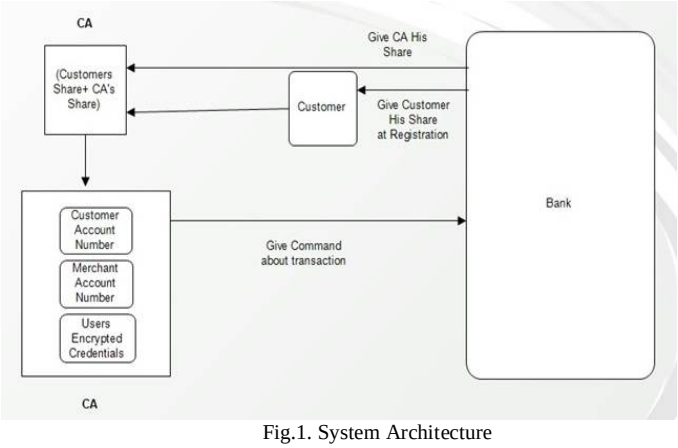

Fig.1. System Architecture

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

There are 3 major contain in the architecture, explain as follows.

User

User First Register in web portal of bank and select image as per there convenient. After selection of image bank will generate another copy of same image and embed half confidential information in on share image and another half in next share using Image Steganography [2].Now one share is kept by the customer and the other share is kept in the database of the certified authority. After successfully completion of registration User gets his own share for future use. On shopping Portal after successfully login user then Checks the Products Recommended by the portal and selects the product for buying. During shopping online, after selectionof desired item and adding it to the cart user will be navigated to the payment gateway. At payment gateway user submits his own share of image that contains User Account Number and there Confidential information which is present in hashing format

CA

Certified Authority is a mediator between user and bank and he will authenticate a user as per there image share.CA already having another copy of image share which is provided by bank in hashing format. First Certified Authority Logged in to their system and checks the customer request.
After Combine the images two shares hashing if that hashes is match then CA Forward a payment request to the bank and complete the payment procedure.

Bank

Bank Password is encrypted using RC6 algorithm [12]. After receiving User Image Share bank will generate another copy of same image and embed half confidential information and password in on share image and another half in next share using Image Steganography (LSB Technique) [2].After Applying Steganography to the image -One copy of image will be sent to the user as a receipt. Second copy is send to the certified authority accountantat a time of payment after receiving Payment request from CA bank will further navigated to Payment Procedure.

B. *Technology Used*

1. *Least Significant Bit*

Least significant bit (LSB) [2] insertion could be a common, straightforward approach to embedding data in an exceedingly cowl image. The smallest amount vital bit (in alternative words, the eighth bit) of some or all of the bytes in a picture is modified to slightly of the key message. Once employing a 24-bit image, slightly of every of the red, green and blue color elements will be used, since they're every described by a computer memory unit. In alternative words, one will store three bits in every element. Associate 800 × 600 element image, will so store a complete quantity of 1,440,000 bits or 180,000 bytes of embedded information. As an example a grid of three pixels of a 24-bit image will be as follows:-
For Example:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the amount 300, that binary illustration is 100101100, is embedded into the smallest amount significant bits, this part of the image, the ensuing grid is as follows:

(00101101 00011100 11011100)
(10100111 11000100 00001101)
(11010011 01011000 01100010)

Although the amount was embedded into the primary eight bytes of the grid, solely the three underlined bits required to be modified in step with the embedded message.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

2. RC6

RC6 (Rivest Cipher 6) could be a symmetric key block cipher derived from RC5.RC6 correct encompasses a block size of 128 bits and supports key sizes of 128,then 192, and 256 bits, but, like RC5, it should be parameterized to support a good sort of word-lengths, key sizes, and variety of rounds [12]. RC6 is extremely almost like RC5 in structure, victimization data-dependent rotations, standard addition, and XOR operations; indeed, RC6 can be viewed as interweaving 2 parallel RC5 encoding processes, however, RC6 will use an additional multiplication operation not gift in RC5 so as to form the rotation depends on equally in an exceedingly word, and not simply the smallest amount important few bits [13].

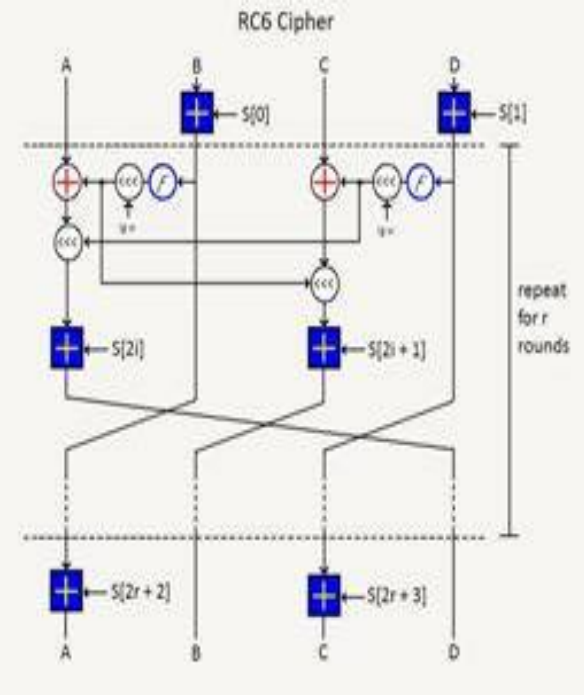

Fig.2. RC6 working principle

3. *One Time Password(OTP)*

A one-time password (OTP) is a keyword that is effective for only one login session or operation, on a computer system or other numerical device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also include two factor authentication by confirming that the one-time password requires access to somewhat a person has (such as a small keying fob device with the OTP calculator built into it, or a smart card or exact cellophane) as well as somewhat a person knows (such as a PIN) [9].

The most important advantage that's self-addressed by OTPs is that, in distinction to static passwords, they're not prone to replay attacks. This implies that a possible interloper who manages to record an OTP that was already wont to log into a service or to conduct a dealing will not be able to abuse it, since it will not be valid.. A second major advantage is that a user, who uses an equivalent (or similar) positive identification for multiple systems, isn't created prone to all of them, if the positive identification for one amongst these is gained by an offender. variety of OTP systems additionally aim to substantiate that a session cannot simply be interrupted or derived while not data of random knowledge created throughout the previous session, so reducing the attack surface more. Ways of delivering OTP area unit text electronic messaging, mobile, exclusive token, web based mostly technique, hard copy [9].

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

IV. RESULTS

A. *Screen Shots*

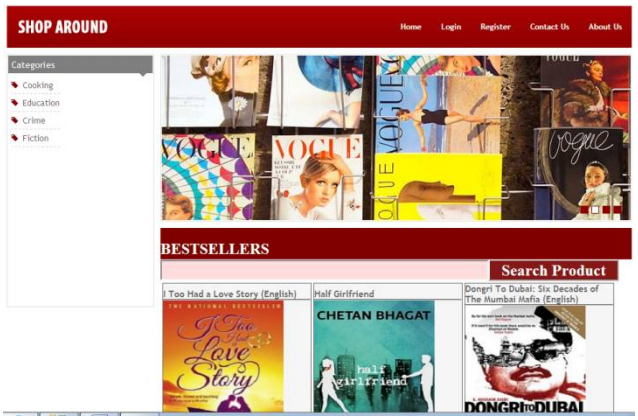

Fig.1. User Home Page

User will register to our system and gets recommendation from algorithm as stated. After choosing a product user can buy that product using our system.

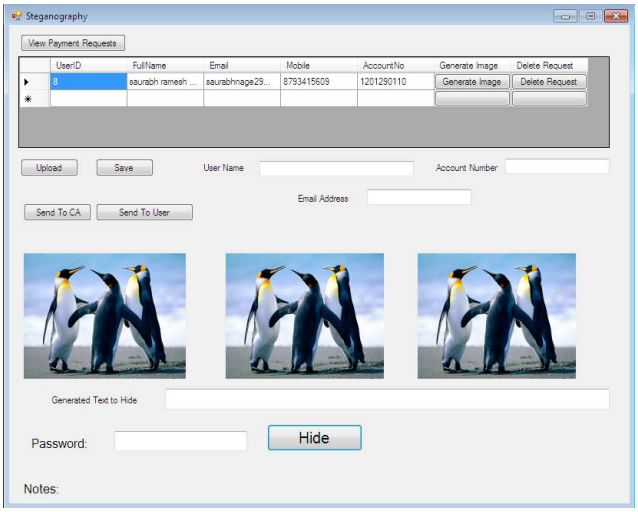

Fig.2. Bank Module

When user registers himself for first time request sent to bank to generate image part for transaction. Bank will then take one random image, make three parts of it and hides pin number and account number by splitting it and in encrypted format. Finally one part will be sent to user and another part will be sent to CA.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

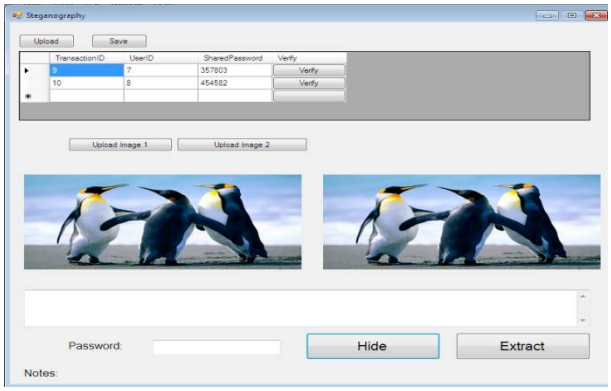

Fig.3. CA Module

CA receives his part and uses that part whenever user request for payment transaction. CA can only see account number if two parts matched else he refuse transaction.

V. CONCLUSION

We implemented payment gateway system that can be applied for E-Commerce for online shopping. It is developed by combining visual cryptography and image based Steganography, It provides privacy for customer data and stops misuse of data at merchant's side. The technique is concerned with prevention of identity theft and customer data confidence. The distinguishing feature is that the other banking application which uses Visual cryptography and Steganography, basically applies for physical banking. We have Implemented Tyco which is a Recommender System which will help user to suggest items on the basis of rating given by the users having similar interest and most searched by the individual user and last recommender system is hybrid system which implements both content based and collaborative system and recommends products to the user.

REFERENCES

1. Yi CAI, Ho-Fung Leung, Qing Li, Huaqing Min, Jie Tang, and Juanzi Li, "*Typicality-Based Collaborative Filtering Recommendation*", IEEE Transactions On Knowledge And Data Engineering, Vol. 26, No. 3, March 2014.Hong-ryeol Gil1, Joon Yoo1 and Jong-won Lee2 ,'An On-demand Energy-efficient Routing Algorithm for Wireless Ad hoc Networks', Proceedings of the 2nd International Conference on Human. Society and Internet HSI'03, pp. 302-311, 2003.
2. Souvik Roy and P. Venkateswaran, "*Online Payment System is using Steganography and Visual Cryptography*", IEEE Students' Conference on Electrical, Electronics and Computer Science 2014.
3. Jihui Chen, XiaoyaoXie, and Fengxuan Jing, "*The security of shopping online*," Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), vol. 9, Pp. 4693-4696, 2011.
4. "*Suspicious emails and Identity Theft*", *Internal Revenue Service*. Archived from the original on 2011-01-31, Retrieved July 5, 2006.
5. Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "*Techniques for Data Hiding", IBM Systems Journal*, Vol. 35, Nos. 3 & 4, pp. 313- 336, 1996.
6. K. Bennet, "*Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding information in Text*", Purdue University, Series Tech Report 2004—2013.
7. J.C. Judge, "*Steganography: Past, Present, Future*", SANS Institute, November 30, 2001.
8. M. Naor and A. Shamir, "*Visual cryptography*", Advances in Cryptography: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.
9. M. Abadi, L.Bharat, and A.Marais, "System and Method For Generating Unique Passwords," U.S. Patent 6 141 760, 1997
10. KalavathiAlla, Dr. R. Siva Rama Prasad, "*An Evolution of Hindi Text Steganography*", Proceeding of Sixth International Conference on Information Technology, pp. 1577-1578, Las Vegas, NV, 2009.
11. I.M. Soboroff and C.K. Nicolas, "Combining Content and Collaboration Text Filtering,"Proc.IJCAI'99 Workshop Machine Learning for Information Filtering,pp .86-91,1999.
12. Abdul Hamid M.Ragab, Nabil A.Ismail, Senior member IEEE, and Osama S. Farag Allah, "Enhancements and Implementation of RC6 Block Cipher for Data Security", IEEE Catalogue No. 01 CH37239-O-7803-7101-1/01 2001 IEEE
13. "RC6 Block Cipher", "rsa.com". Available at: http://www.rsa.com/rsalabs/node.asp?id=2512.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

BIOGRAPHY

Aditya Anil Chavanis a B.E. Student in the Computer Science Department, Dr. D. Y. Patil Institute of Engineering & Technology, Pune, Savitribai Phule Pune University (SPPU). He is pursuing his Bachelor of Engineering degree from SPPU University, Pune, Maharashtra, India.

Ajay ParisaMangajis a B.E. Student in the Computer Science Department, Dr. D. Y. Patil Institute of Engineering & Technology, Pune, Savitribai Phule Pune University (SPPU). He is pursuing his Bachelor of Engineering degree from SPPU University, Pune, Maharashtra, India.

PriteshPravinJoshiis a B.E. Student in the Computer Science Department, Dr. D. Y. Patil Institute of Engineering & Technology, Pune, Savitribai Phule Pune University (SPPU). He is pursuing his Bachelor of Engineering degree from SPPU University, Pune, Maharashtra, India.

Priti Mithari is an Assistant Professor in the Computer Science Department, Dr. D. Y. Patil Institute of Engineering & Technology, Pune, Savitribai Phule Pune University (SPPU).