IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

Improving Login Process by Salted Hashing Password Using SHA-256 Algorithm in Web Applications

T. Ebanesar[1 *], G. Suganthi[2]

[1]Department of Computer Science, Malankara Catholic College, Mariagiri, Tamilnadu, India
[2]Department of Computer Science, Women's Christian College, Nagercoil, Tamilnadu, India

**Corresponding Author*: t_ebione@rediffmail.com, *Tel.: +91-9442304607.*

DOI: https://doi.org/10.26438/ijcse/v7i3.2732 | Available online at: www.ijcseonline.org

Accepted: 06/Mar/2019, Published: 31/Mar/2019

***Abstract*:** In today's digital world, all the web applications are used password for their login process. It is fact that, all the Internet applications still used the text based passwords with encrypted form. In encryption technique, hackers are easily hacking the password with decryption process. It is not a secure method to implement in password process. There are so many possibilities of decrypting a password and gets the password by hackers. It was the existing method to protect the unauthorized person to access or enter into the account. Today's technology revolution, the hackers are supposed to be hacked the encrypted text based passwords. In order to avoid this, we used salted hashing password technique using SHA-256 algorithm [1]. The main objective of this research paper is to secure the user's password in order to give protection from hacking. In this paper we had implemented password security in SHA-256 hashing algorithm at server side.

***Keywords* –** Password Security, Salt, Salted Password, Password Attacks, SHA-256, Hash, Hashing Algorithm, 2018 Password Stolen, encryption vs hashing

I. INTRODUCTION

Password Security is the main concern of Internet based web applications. Most of the login accounts these days use a combination of text and number as password. In fact, it is not a secured method. Because of, the hackers are able to get the password easily and quickly. If storing password in a plain text or in encrypted method then there are too many possibilities of decrypting of password and stolen by hackers. Almost all the Internet applications still used the encryption method with text based passwords. Utilization of static passwords in login process leads to access the files of any user easily. Hackers, ID thieves and fraudsters are easy to attack the login account and steal passwords so as to gain access the login accounts. One of the most important security features used today are passwords. The Computer Emergency Response Team (CERT) estimates that about 80 percent of the security incidents reported to them are related to poorly chosen passwords.

A strong password with salted hash is your first level of security to defense against online intruders and hackers. It is very important to safe our personal accounts (e-mail, social media accounts).Hashing password is better than encryption of password because hashing is a one-way function. It will not be reversible. We can't get the original password back. Hash function [2] is used to produce the hash value. Salt is used to generate a random value when the user creates an account or changes their password. The password should be hashed using a new random salt. In this paper we implemented salted hashing password at server level.

II. EXISTING PASSWORD METHOD

Today's existing encryption scheme may be easy to crack or hack by hackers. In fact, encrypted passwords can be easily decrypted. It gives more advantage to hackers. Password authentication can also be used as a generic authentication method. Weak passwords can also be discovered by dictionary attacks from a remote machine. As hackers continue to become more savvy and sophisticated, encryption technology must evolve as well. If you use an encrypted password that is easy to guess, your encrypted password is less secure. Most of the web applications are using Two Factor Authentication method. It is not secure for online applications and log in process. Username and password are the most commonly used mechanism for authentication because of simplicity and convenience. When you signed into any website or app, you were probably asked to sign in using a username and password.

The password you entered is considered a single-factor authentication. One factor, your password and username, proved to the website that you are allowed to access the account. Two-Factor Authentication, commonly referred to as 2FA, is a feature that adds an additional factor to your normal login procedure to verify your identity. 2FA adds an

extra layer of security by verifying your identity using OTP via SMS. A unique 4 digit one-time password is generated and then sent to the registered user's phone number. All the social media websites such as facebook twitter and google+ and net banking accounts are using 2FA method to access the account and online transaction. With this method, online accounts and social media accounts may be hacked by cybercriminals. Most of the email service providers use 2FA method. In the month of September 2018, at least 50 million facebook accounts were hacked. Facebook login uses 2FA method. In the year 2013, YAHOO has confirmed that cybercriminals were able to steal personal data including name, address, and security questions from all 3 billion Yahoo user's accounts. Yahoo also uses 2FA method. Table 1 gives the information about the hacking of user accounts in different websites used by 2FA method.

Table 1: Hacking of user accounts in different websites used by encryption method

Sl.No	Website Name	Authentication Used	Year	Total No. of User accounts hacked
1	www.yahoo.com	2FA	2013	3 billion
2	www.facebook.com	2FA	2018	50 million

Table 1 gives the information about the hacking of user accounts in different websites used by encryption method. From the above table; it is found that encryption method is not a best method to secure user's accounts.

III. PROPOSED SALTED HASHING PASSWORD WITH LOGIN SYSTEM

When compared to existing method of text-based username and password, OTP sometimes hackers are to be broken the same. To avoid this, we proposed Five-Factor Authentication (5FA) method with salted hashing password. In the context of passwords a salted password is harder to crack or hack. In password protection, salt is a random string of data used to modify a password hash and can be added to the hash to prevent a collision by uniquely identifying a user's password even if another user in the system has selected the same password. In our project, each password is stored with salted hash value .So that no hacker will be accessed by user's data. For implementing this, hackers are not able to attack any one of the password attacking methods such as Dictionary Attack [3], Brute-Force Attack and Rainbow Table Attack. The block diagram of proposed password system is shown in fig 1.

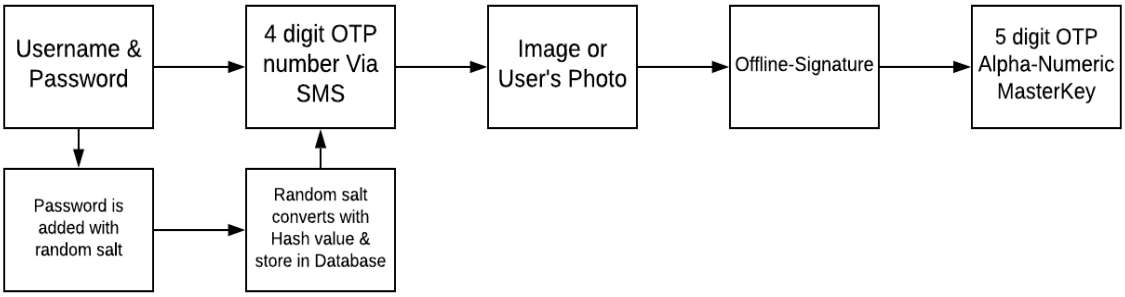

Fig 1: Block diagram of proposed system

3.1) Registration Process: The below diagram shows the registration phase of the 5FA method. In the registration phase, the user enters all the personal information with graphical image and offline-signature. This graphical image and off-line signature is used to confirm to check the user at the time of user log in. When user registers to web application, user selects a password with the following constraints. A strong password should have a minimum of 8 alphanumeric characters and includes a mix of uppercase letters, lowercase letters and numbers. Password is stored with salted hashing value at server side using SHA-256 hashing algorithm. The registration phase process is shown in fig 2.

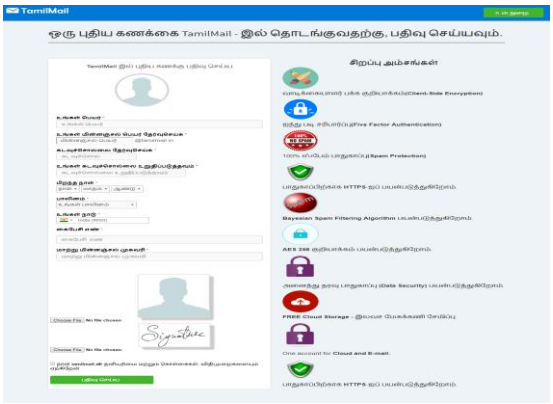

Fig 2: Registration Process

3.1.1) Generating a Good Random Salt: When we are adding salts to passwords, we need to add salts that are cryptographically strong and credential-specific. In our project, we generate append the random salt to the passwords. If two users use the same password, every time different salt is added to the password. Both salted passwords would hash to the different value. The salt generation with hashing process is shown in fig 3.

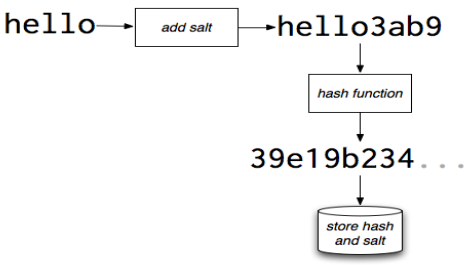

Fig 3: Generate a salted hashing password

3.1.2) Different users, Same password. Different salts, Different hashes:
Hashing and Salting Alice's Password:

Table 2: **Hashing and Salting Alice's Password**

Sl.No	Fields	Action Performed
1	User	Alice
2	Password	farm1990M0O
3	Salt	f1nd1ngn3m0
4	Salted input	farm1990M0Of1nd1ngn3m0
5	Hash (SHA-256)	07dbb6e6832da0841dd79701200e4b179f1a94a7b3dd26f612817f3c03117434

Hashing and Salting Bob's Password:

Table 3: **Hashing and Salting Bob's Password**

Sl.No	Fields	Action Performed
1	User	Bob
2	Password	farm1990M0O
3	Salt	f1nd1ngd0ry
4	Salted input	farm1990M0Of1nd1ngd0ry
5	Hash (SHA-256)	11c150eb6c1b776f390be60a0a5933a2a2f8c0a0ce766ed92fea5bfd9313c8f6

3.2) Login Process: In login process, we had implemented 5 different levels of security to protect the user's data. Login process uses 5FA method. In the year 2016, 3.3 billion login credentials were stolen. 9 out of 10 login attempts were fraudulent in 2016.To protects our data from cybercriminals, it is very essential to implement 5FA method with salted hashing password.

The login process is as follows:

3.2.1) User name & Password (First Factor)
3.2.2) OTP (Second Factor)
3.2.3) Graphical Image or User's Photo (Third Factor)
3.2.4) Offline-Signature (Forth Factor)
3.2.5) MasterKey (Fifth Factor)

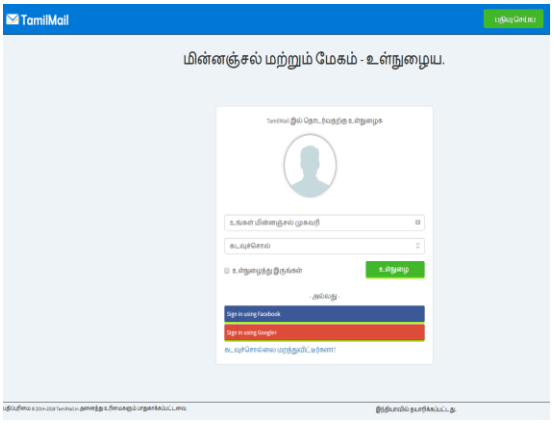

Fig 4: Login Process – Username & Password (First Factor)

3.2.1) User name & Password

A user logs into a website with a username and password. When the user enters their password in the given field, it compares the hash of the given password with the hash from the database. If they match, the password is correct. Otherwise the password is incorrect. When the user enters into their account, a 5 digit alpha-numeric characters are automatically generated in masterkey field in the database with AES-256 encryption. This masterkey will be used as the fifth factor authentication of login process. The login process is shown in fig 4.

3.2.2) OTP

A one-time password [4] (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session. A onetime password as the word indicates is only valid for a specific time interval or one-time usage. If the user credentials are valid, a 4 digit one time password is sent to your registered mobile number through SMS and you are required to enter it when prompted. The OTP Verification

process is shown in fig 5. It is the Second Factor Authentication. If the session of OTP number expires, the user is able to receive a new OTP number when he or she is using the option resend OTP.

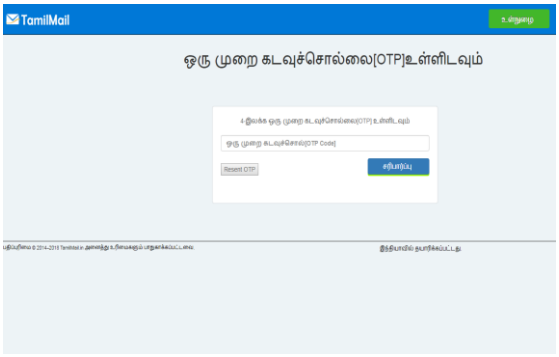

Fig 5: Login Process – Verify OTP (Second Factor)

3.2.3) Graphical Image or User's Photo

If the OTP number is correct, the user is asked to load the image when he or she was stored at the time of sign up. We used similarity measure algorithm for image matching. An important problem in image processing is the comparison of images. The Verification of user's Image or Photo process is shown in fig 6. It is the Third Factor Authentication.

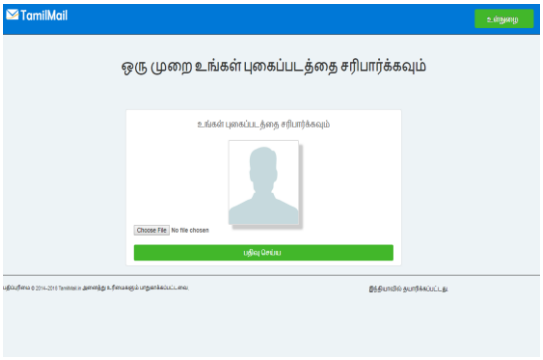

Fig 6: Login Process – Verify Image or Photo (Third Factor)

3.2.4) Offline-Signature

After the image matches, user selects his signature for forth level of security. The Verification of user's Offline-Signature process is shown in fig 7. It is the Forth Factor Authentication.

Fig 7: Login Process – Verify your Signature (Fourth Factor)

3.2.5) MasterKey

After the Offline-Signature matches, the 5 digit alpha-numeric OTP code is sent to your registered mobile number through SMS. This OTP is the MasterKey or MainKey to login the system. The MasterKey is generated using random algorithm by which it is making unique for each and every time the user requests for login. This is the Fifth Factor Authentication. The Verification of masterkey process is shown in fig 8.

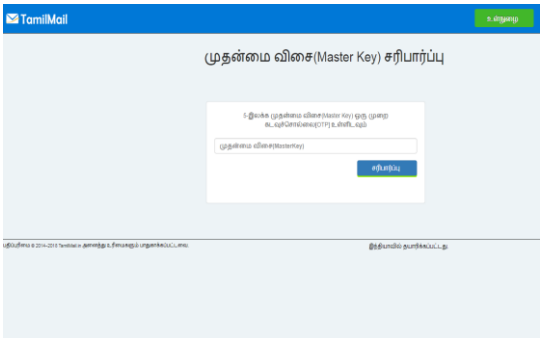

Fig 8: Login Process – Verify MasterKey (Fifth Factor)

IV. FIVE-FACTOR AUTHENTICATION (5FA) METHOD

Five-factor authentication is the highest secured authentication method in IT field. Five-factor authentication, or 5FA, is a 5 different layer of security used when logging into websites or web applications. This method is used to strengthen the security by requiring 5 method or levels (also called as factors) to verify your identity. These factors are user name & password, OTP, graphical image or user's photo, offline-signature and masterkey. There have been several cases of stolen and hacked passwords in 2FA method [5]. Web application with just simple username and password combinations getting hacked is very easy. In this situation, implementing five factor authentications will prevent hackers from gaining access to your accounts even if your password is stolen. The extra layers of protection that 5FA offers ensure that your account is more secure. Five-factor authentication is the most reliable way to ensure the security of your users.

5FA with salted hashing password protects against phishing, social engineering & password brute-force attacks and password hacking. Five-Factor authentication provides an extra layer of security and makes it harder for attackers to gain access to a person's devices & online applications.

V. DIFFERENCE BETWEEN ENCRYPTION AND HASHING

Encryption is the process of encoding simple text and other information that can be accessed by the sole authorized entity if it has a decryption key. Hashing and encryption are

different but also have some similarities. They are both ideal in handling data, messages, and information in computing systems. They both transform or change data into a different format. While encryption is reversible, hashing is not. Hashing is used to generate random strings to avoid duplication of data stored in databases. Hash [7] can be used to store passwords. A hash algorithm is a function that can be used to map out data of random size to data of fixed size. Hash values, hash codes and hash sums are returned by functions during hashing. The difference between encryption and hashing is shown in fig 9.

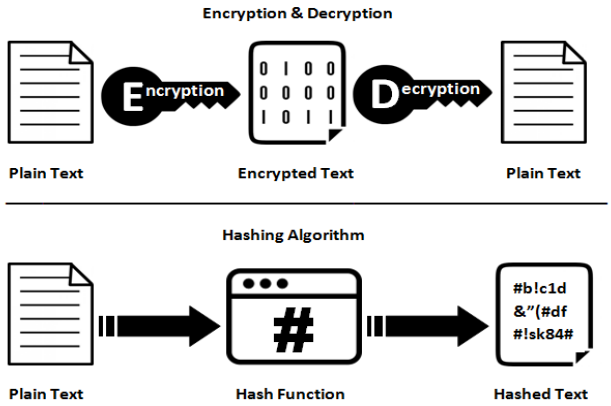

Fig 9: Difference between Encryption and Hashing

VI. SYSTEM DESIGN

The system design of the proposed five factor authentication (5FA) method with salted hashing password is shown in fig 10.

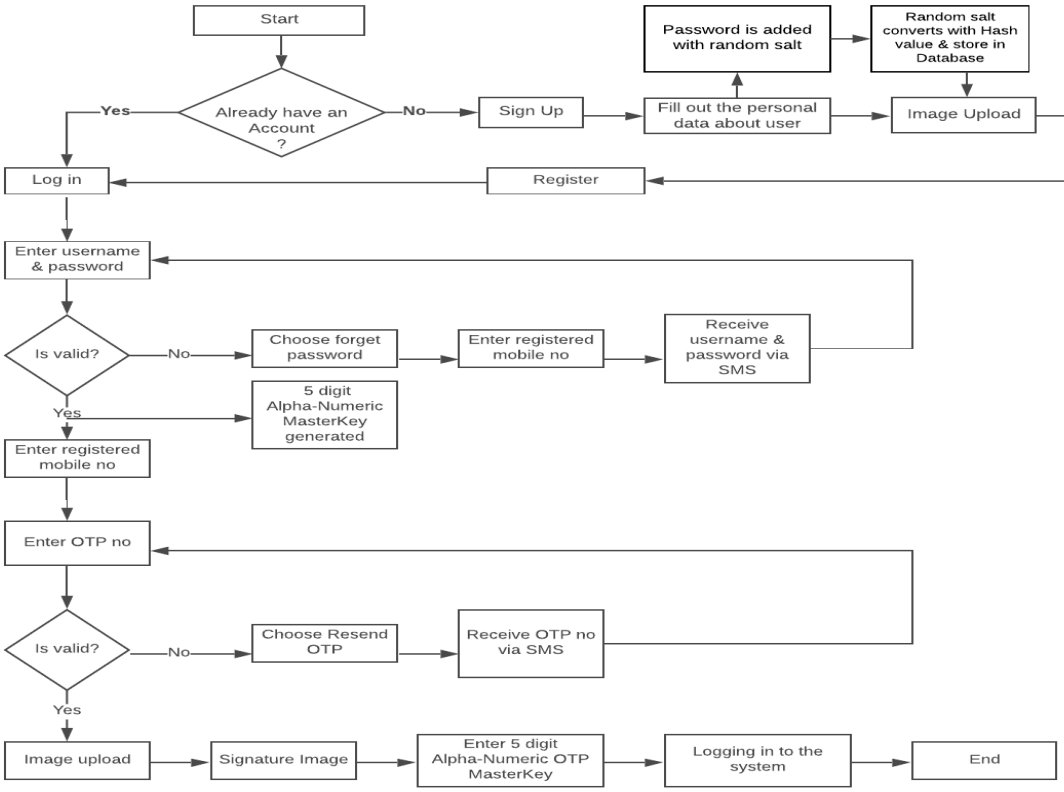

Fig 10: The new system design of the proposed five factor authentication (5FA) method with salted hashing password

VII. IMPLEMENTATION

Implementation of algorithm has been done using ASP.NET with C#. Installation of Visual Studio 2010 and SQL server 2008 is necessary for our system. This paper was successfully completed with the implementation of Five-factor Authentication method with salted hashing password.

VIII. RESULTS AND DISCUSSION

The result that we get after implementing the proposed 5FA method with salted hashing password is given in Figure 1. We apply our project in PG students of computer Science at the Malankara Catholic College computer lab and perform the login process with 25 students (10 male students and 15 female students) between ages of 20-23.We had successfully

verified and executed the project with 5FA method with salted hashing password using SHA-256 algorithm. The time taken to complete the log in process is given in table 4.

Table 4: Time taken to complete log in process

Sl. No	Gender	Total no. of Students	Average Time(minutes)
1	Male	10	1.001
2	Female	15	1.101

Column 4 of table 4 shows that the average time to complete log in process are 1.001 and 1.101for both male and female students. When compared with 2FA method it takes much more time to complete log in process. But at a same time it is the most secured login process.

IX. CONCLUSION

Secure hashing is the best way to protect passwords. Hashing passwords could not be reversed, stolen and hacked. A stolen hash code could not be used by anybody. Hashing the password prevents an attacker with access to the database from modifying application privileges because the attacker won't know which user record is update. Existing authentication methods are two level security methods. 5FA method with salted hashing password improves security with 5 different levels of security. No hackers and cybercriminals will be accessed into the user's account. Five-factor authentication is a recommended best-practice for protecting sensitive data. Graphical Based Image Authentication is more security than any other authentication. It is impossible to hack the data and also to avoid the brute force attack. If you are looking to increase online security, turn on Five-Factor Authentication method. It is the best and secured authentication method than any other method. 5FA method with salted hashing password can help protect you from a potentially devastating account breach.

REFERENCES

[1] R. Roshdy, M. Fouad, M. Aboul-Dahab "*Design And Implementation A New Security Hash Algorithm Based On Md5 And Sha-256*", International Journal of Engineering Sciences & Emerging Technologies (IJESET), Vol.6, Issue.1, pp.29-36, 2013

[2] H. B. Pethe, Dr. S. R. Pande "*An overview of Cryptographic Hash Functions MD-5 and SHA*", IOSR Journal of Computer Engineering (IOSR-JCE), Vol.4, Issue.3, pp.37-42, 2016

[3] Pritesh N.Patel,Jigisha K.Patel and Paresh V.Virparia "*A Cryptography Application using Salt hash Technique*", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol.2, Issue.6, pp.236-239, 2013

[4] Samir Pakojwar, Dr.N.J.Uke "*Security in Online Banking Services-A Comparative Study*", International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), Vol.3, Issue.10, pp.16850-16857, 2014

[5] S.Vaithyasubramanian, A.Christy and D.Saravanan "*Two Factor Authentications for Secured Login in Support of Effective Information Preservation and Network Security*", APRN Journal of Engineering and Applied Sciences (APRN), Vol.10, Issue.5, pp.2053-2056, 2015

[6] S.Vaithyasubramanian, A.Christy and D.Saravanan "*Access to Network by Three-Factor Authentication for Effective Information Security*", Hindawi Publishing Corporation,The Scientific World Journal, Vol.10, Issue.4, pp.127-132, 2016

[7] Sirapat Boonkrong and Chaowalit Somboonpattanakit "*Dynamic Salt Generation and Placement for Secure Password Storing*", IAENG International Journal of Computer Science, Vol.43, Issue.1, pp.18-27, 2016

[8] Dr.Abdelrahman Karrar,Talal Almutiri,Sultan Algrafi,Naif Alalwi,Ammar Alharbi "*Enhancing Salted Password Hashing Technique Using Swapping Elements in an Array Algorithm*", International Journal of Computer Science and Technology, Vol.9, Issue.1, pp.21-25, 2018

AUTHORS PROFILE

T.Ebanesar MCA., M.Phil. B.Ed is currently pursuing Ph.D and working as an Assistant Professor of Department of Computer Science, Malankara Catholic College, Mariagiri, Tamilnadu, INDIA since 2008. Earlier I had worked as a Lecturer in N.M.S.S.Vellaichamy Nadar College, Madurai from 2004 to 2008. His main research area focuses on Cloud Computing, Email Technologies, Artificial Intelligence, Machine Learning and Security in Computing. He has 13 years of experience in teaching. My personal website www.ebanesar.in

Dr.G.Suganthi M.Sc., M.Phil, B.Ed., PGDCA, Ph.DShe is working as an Associate Professor of Department of Computer Science, Women's Christian College, Nagercoil, Tamilnadu, INDIA since 1998. She is Guiding 6 Ph.D Scholars. She has presented 15 papers in national and international conferences and published 8 papers in international journals. She has authored 2 books. She is serving as the IQAC Co-coordinator since 2012.She is the doctoral committee member of St.Joseph′s College (Autonomous), Thiruchirapalli. She received two awards namely Shiksha Rattan Pureskar in October 2012 at New Delhi and Best Citizen Award by International publishing house, New Delhi in February 2013. She has 20 years of teaching experience and 8 years of research experience.