Multi level Authentication for secure Attendance System

Ashish Chauhan, Shruti Khosla, Muskan Sharma, Sarthak Sahni

Abstract: *Multi level Authentication means authentication of user at different levels. Attendance system concerns with taking students attendance, with complete efficiency and awareness, this all used to happen in a very conventional way, wherein there were more chances of discrepancy in records.*

Authentication is a major concern as safety is a priority which proves the validity of the user, when designing a software which stores large amounts of data and which has already existed in the past, and has certain loopholes. To fill these loopholes and to make this process more reliable Multi Level Authentication is used.

Multi-Factor Authentication used here have three phases, starting with Login credentials which goes unique even if students share their credentials with their peers their peers won't be able to login using their phones as IMEI was stored initially during the time of registration. This code is stored in the database without the knowledge of the student. We have the next phase which is OTP generation which is secured using RSA sent to the registered mobile number that is very unique as the OTP is sent only to the registered mobile number. The last phase which ensures the presence of student in the class is QR code scanning, where in a student scans QR code shared by the teacher in the class . After scanning the QR code the attendance gets stored in the database. The purpose of this Attendance system is to overcome the drawbacks of the already existing conventional way which includes marking attendance manually which was a time taking process. By introducing this attendance system using multi level authentication we have established a more advanced, more efficient and more secure unlike conventional attendance system. Multi level authentication can be used in various application where security of the assets is the main concern.

Keywords **: Attendance ,Multilevel Authentication ,OTP ,QR code ,RSA ,Smartphone Authentication**

I. INTRODUCTION

No matter what kind of software or application we take, the requirements for the security are essential. If it handles emails or functions as attendance system or banking systems, the unfortunate truth is that hackers,crackers are everywhere who look for an opportunity to seize access and control of the desired application or system.

Accessing attendance system is used in many educational institutions to instill discipline. There are conventional methods to do so, still there are many complexities in handling them, so the new approach which concerns both efficiency and Authentication is very much required.

Multifactor authentication helps to improve security. The chances that unauthenticated user can have the access to assets decreases.

The factors of authentication fall into the following categories:

Knowledge factors includes something that the user must know to get access to resources:Passwords, Pins ,IDs all fall into this category.

Possession factors includes something that the user must have to get the access to the system . It includes smart phones with OTP apps,one-time password tokens (OTP tokens), employee ID cards and SIM cards,key fobs

Inherence factors includes any technical scans, such as QR Code scans or biometrics the user has that are require for getting the access to the system. This category includes the biological traits such as iris scans retina scans, fingerprint scans, facial recognition, voice recognition, hand geometry and even earlobe geometry.

It is important to know that the security doesn't only get affected by the no of factors involved but also how the factors are applied. In each category, the choices we made for authentication rules greatly affect the security.Weak password mechanism, help attackers to hack the password and can get the access to system. The most accurate practices include requiring strong passwords that which are updated regularly. Facial recognition systems can be defeated by holding up a picture, so QR Code Scan System is a unique and non hackable way of improving security.OTP generation system can also have drawbacks as attacker can change the otp during transmission of otp from backend server to the authenticated user.

II. LITERATURE SURVEY

There are several studies to improve attendance-taking using different technology.

1. 'An efficient,automatic Attendance System using Fingerprint Verification technique',(2010)

According to Saraswat, C., & Kumar, A. , biometrics approach is better when dealing with cheating.Temperament of identification and sharing of QR Code can be done.Attendance cheating is insufficient via the use of QR code.

Manuscript received on March 15, 2020.
Revised Manuscript received on March 24, 2020.
Manuscript published on March 30, 2020.

* Correspondence Author

Ashish Chauhan*, Asst. Professor, Department of Information technology, SRM Institute of Science and technology.

Shruti Khosla B.Tech Scholar, Department Information Technology, SRM Institute of Science and Technology.

Muskan Sharma is B.Tech Scholar, Department of Information Technology SRM Institute of Science and Technology

Sarthak Sahni is B.Tech Scholar, Department of Information Technology SRM Institute of Science and Technology.

2. 'Attendance checking system using QR Code,(2014)
'Baban showed the implementation of a basic attendance-taking system via students' smart phones using QR code scanning. The system generates the reports. It is a generic design for re implementation but does not raise issues of cheating in attendance.

[3]'Student Attendance System using QR Code',(2014)
Masalha & Hirzallah designed a mechanism for attendance using a QR code with multiple security factors that are used for elimination of false registration. The additional factors include biometrics which is GPS location and selfie. GPS seemed to be a good non-biometric approach apart of QR code.

[4] 'Using QR Code for attendace tracking',(2015)
Deugo proposed a unique mechanism according to which the Qr codes need to be generated by students and then bring that Qr code in class so that teacher can scan all the Qr codes generated by student.However this mechanism do not provide time efficiency.

[5] 'Multi-Factor Authentication System',(2018)
Yew Kwang Hooi, Khairul Shafee Kalid and Serdarmammet Tachmammedov proposed that implementes the use of QR code with GPS location to make a secure attendance mechanism.The proposed mechanism helps to tracks student through GPS by maintaining an active login session on the smart phone that is being used. This approach needs phone's IMSI number registration with identity of the user.The continuos tracking of server is the solution for the same.

Literature review has showed preferences for QR codes as compared to biometrics because of scalability reasons. It is not error-proof, which requires additional checks conducted using OTP or IMEI during the registration.None of the work, explains how potential error is detected via information processing.

The report has all the best of conclusions , which works on 3FA, starting with Login credentials wherein checks are conducted using IMEI during the registration, which is unique to every user, then it goes by QR Code in which the scan can be only done during the ongoing class and then OTP features using two algorithm(RSA), so that no attack can occur while generating OTP.

This makes the application efficient yet hack free.

III. METHODOLOGY

The goal of the surveys conducted is to find the issues in taking attendance of students. Surveys and interviews of the faculties and students are conducted to investigate the current methods used and the issues that come across during attendance taking. Data obtained through the feedback of the faculties and the students is analyzed. Cheating during attendance is an issue that came across with the attendance system and therefore Multi level authentication prevents the issue in the current attendance taking process. The process of multi level authentication involves three levels of authentication that is 1. Authentication through smart phones, 2. Authentication through OTP and 3.Authentication through QR Code.

Authentication through smart phones contains a user interface created on Android Studios through which the registration of user and the phone is done. There is a one time registration of the user and phone in which a unique 15 - digit IMEI is stored that identifies a valid mobile phone. This unique code maps the user identity with the device which detects the authentication of the user. The IMEI code gets stored in the database and through this unique code the user and the phone is identified. IMEI of the user is checked against the IMEI number which is stored in database at the time of registration, therefore the user cannot login with any other device. The chances of proxy will decrease. The mapping of the user and the device makes the user to be physically present for the attendance mechanism.

Authentication through OTP is the second level of authentication. This one time password will automatically verified at the receiver side. The OTP is a unique code that is uniquely and randomly generated during each event of authentication which adds an additional layer of security. Even if the attacker hacks the first level of authentication ,OTP helps to keep the system safe. The backend server generates a secret key and shares it with the service generating the OTP. Using the RSA Algorithm, the OTP code is encrypted creating a encrypted code. This encrypted code is then send to the receiver, so during the transmission of OTP no one can change the otp. On the receiver's end the message is decrypted and displayed before the user. Doing this assure the confidentiality of the OTP which is only for user. After verification is done at the backend, the student is asked to follow the third level of authentication.

Authentication through QR code is the third level of authentication, provides the students to access the lectures. The lecturers register to the system by entering the required details.Then the lecturer will enter the subject and unique QR code is then generated by the server. At the beginning of the class, the lecturer displays the QR code via the projector. The first time user, students have to register to the application. The logged in students have to then scan the QR code. The attendance is recorded once the students scan the QR code.

(A) ALGORITHM

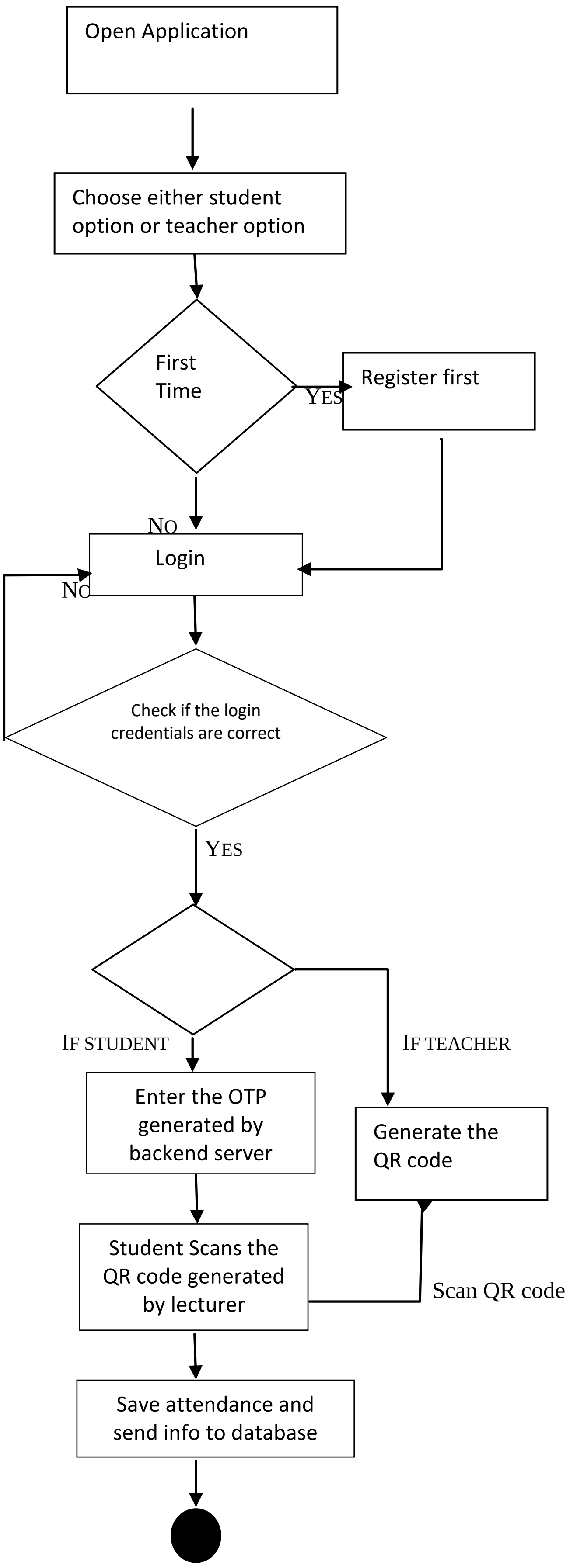
STEP 1. Start and install the app.
STEP 2. If the person is student, then go to student section or else if the person is teacher, then go to teacher section
STEP 3. If Student then, first the student needs to register.
STEP 4. If teacher then, first the teacher needs to register.
STEP 5. The teacher can login after successful registration and go to attendance section and generate the QR code for attendance.
STEP 6.

A) The student can login using the login credentials which is first level of authentication.

B) After login the second level of authentication is OTP which will be sent to user's mobile number.

C)Third level of authentication is QR code which is already generated by lecturer and student will scan the QR code and get the attendance marked.

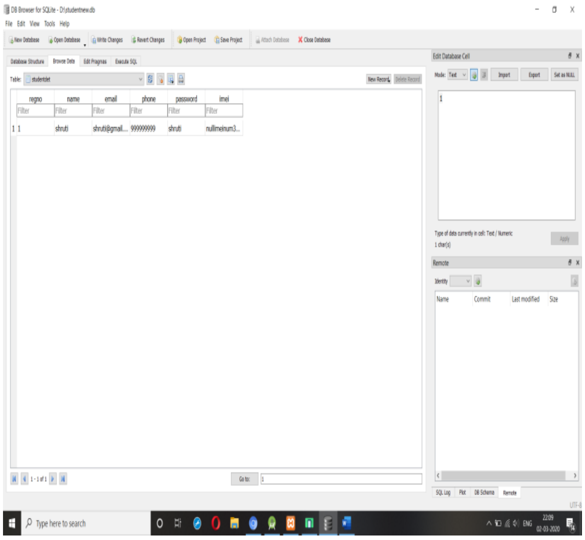
STEP 7. Stop.


Open Application
Choose either student option or teacher option
First Time
YES
Register first
NO
Login
NO
Check if the login credentials are correct
YES
IF STUDENT
IF TEACHER
Enter the OTP generated by backend server
Generate the QR code
Student Scans the QR code generated by lecturer
Scan QR code
Save attendance and send info to database

There are 3 databases used in the system.

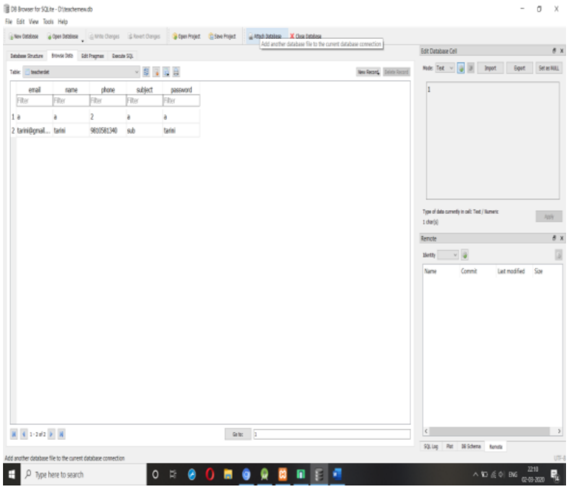
1. Student_details
2. Attendance_details
3. Teacher_details

The first one is for student which is used to store the details of student



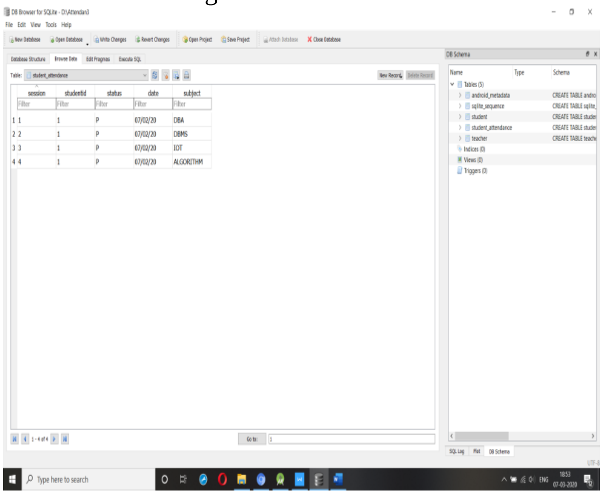
	regno	name	email	phone	password	imei
1	1	shruti	shruti@gmail....	999999999	shruti	nullimeinum3...

The second one is for teacher which is used to store the details of teacher.


DB Browser for SQLite - D:\teachernew.db
File Edit View Tools Help
Table: teacherdet

	email	name	phone	subject	password
1	a	a	2	a	a
2	tarini@gmail....	tarini	9810581340	sub	tarini

The third is for storing the attendance of student.


DB Browser for SQLite - D:\Attendan3
File Edit View Tools Help
Table: student_attendance

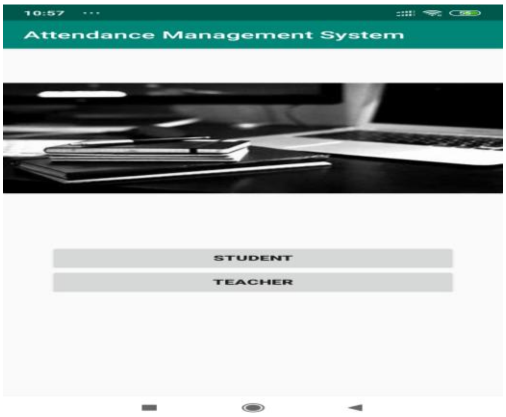
	session	studentid	status	date	subject
1	1	1	P	07/02/20	DBA
2	2	1	P	07/02/20	DBMS
3	3	1	P	07/02/20	IOT
4	4	1	P	07/02/20	ALGORITHM

Retrieval Number: F9247038620/2020©BEIESP
DOI:10.35940/ijrte.F9247.038620
Journal Website: www.ijrte.org

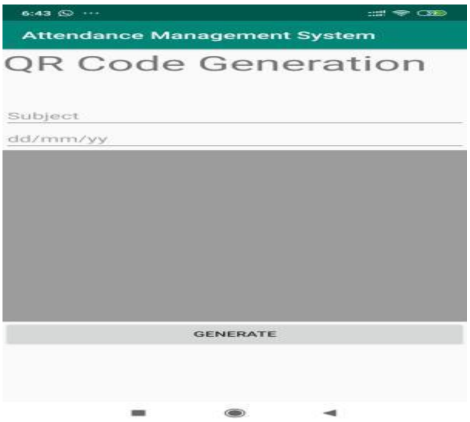
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

IV. IMPLEMENTATION

- Start and install the app.
- After the installation of the app, there will be two option if the person is student, then the person will select student option and if the person is teacher then the person will select teacher option.

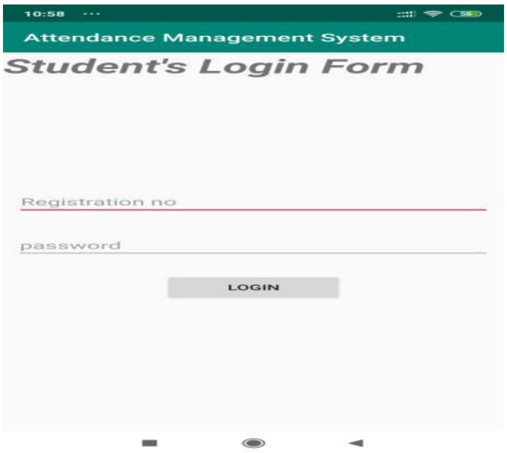


- If the person is teacher, then teacher will register using the registration form in the app.
- After successful registration, teacher can login using the login credentials and go to attendance activity.
- The teacher will have to generation a QR code using the subject and the date .

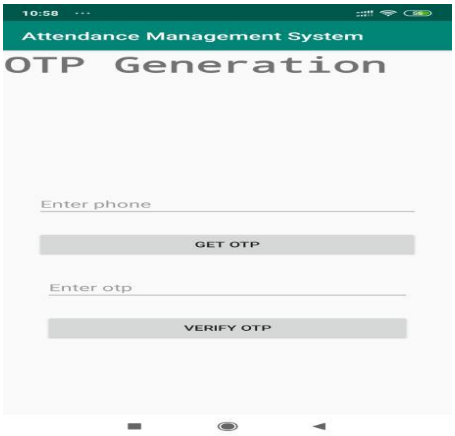


In the student section the student will have to register and at the time of registration the IMEI code the mobile will automatically be stored in the database with al the other details without letting the student know.

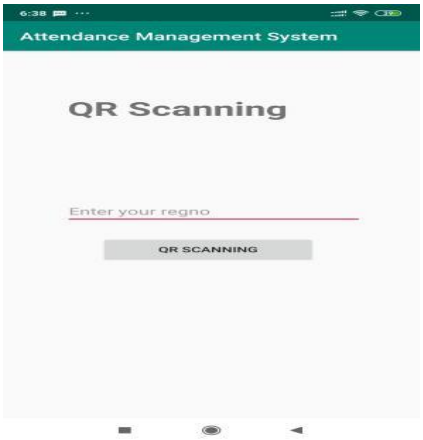
- Student can login using the login credentials and at the time of login the IMEI code will also be checked by the system.



- After successfully login into the system, the system will ask student to enter the registered mobile number and a OTP will be sent to student's mobile number which is second level of authentication



- If the user enter the correct OTP number then,the OTP received will automatically be filled .After verified by the system, the next activity will come which is QR scanning which is third level of authentication.
- For successful QR scanning the system will ask student to enter the registration number.
  When the student will scan the QR code generated by lecturer ,attendance will be marked.



V. LIMITATIONS

This system had been designed using Android studio which limits the use of application for some deice like iPhones.
Also, as the first authentication is through smart phones which is using IMEI number so every time students need to inform the administration before changing their phones .
The students must carry their phones all the time as attendance will be marked through this application only.
Moreover, the internet connection is required,

VI. RESULT AND DISCUSSION

The proposed System requires amalgamation of multiple factors – IMEI code, QR code, OTP for authentication of the Attendance system as built under this research has cleared out discrepancy in storage of data and also false attendance pattern.

The multiple combinations used such as OTP generation for increasing the security, Login linked with mapping of IMEI number of mobile phones to the database, and then QR code scanning marking a confirmed presence of student in the class.

The manual work of the teacher reduces.

FACTORS	RESULT
Login Credentials	No unauthorized user can access the system without knowing the correct login credentials, the user has to login from the same device since the IMEI code generated is mapped with the IMEI code stored in the database.
OTP Generation	It is a security measure which changes everytime we login into the system and becomes invalid after sometime, therefore the OTP cannot be hacked even if the attacker figure outs the login credentials
QR Code	This ensures the physical presence of the student

VII. CONCLUSION

This study has investigated that:

1. The attendance system can be made more efficient, less complex and cheat free by using 3F authentication system also called Multi Factor Authentication system.
2. This system is a new age, verified, well tested, promising, cost effective and technologically sound. That marks a bar for a cheat free Attendance system making cheating unappealing and easily detectable.
3. Attendance system as build under this research has cleared out discrepancy in storage of data and also false attendance pattern.
4. This attendance system has reduced all the time taking manual work that the lecturer had to go through before starting the lecture.
5. This system reduces the drawbacks of the previous existing system as it is less time consuming because the students have to scan the QR code at the same time.

REFERENCES

1. Baban, M. H. M. (2014). Attendance checking system using quick response code for students at the university of sulaimaniyah. Journal of Mathematics and Computer Science (JMCS)
2. Yew Kwang Hooi, Khairul Shafee Kalid and Serdarmammet Tachmammedov (2018). MULTI-FACTOR ATTENDANCE AUTHENTICATION SYSTEM at the University Technology PETRONAS. Department of Computer and Information Sciences
3. Aleksandr Ometov , Sergey Bezzateev ,Niko Mäkitalo ,Sergey Andreev, Tommi Mikkonen and Yevgeni Koucheryavy(2018). Multi-Factor Authentication. Laboratory of Electronics and Communications Engineering, Department of Security of Cyberphysical Systems, Department of Computer Science, University of Helsink.
4. Masalha, F & Hirzallah, N. (2014). A student attendance system using QR code. International Journal of Advanced Computer Science and Applications.
5. Deugo, D. (2015). Using qr-codes for attendance tracking. In Proceedings of the International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS)
6. Saraswat, C., & Kumar, A. (2010). An efficient automatic attendance system using fingerprint verification technique. International Journal on Computer Science and Engineering,
7. Rahul Kale, Neha Gore, Kavita, Nilesh Jadhav, Swapnil Shinde (2013)" Review Paper on Two Factor Authentication Using Mobile Phone" International Journal of Innovative research and Studies.
8. Dongare Priyanka, Gunjal Pratiksha, Gujar Prashant(2018), "An implementation of fingerprint and aadhar based student attendance system",
9. Benfano Soewito, Ford Lumban Gaol, Echo Simanjuntak, Fergyanto E. Gunawan "Attendance System on Android Smartphone" International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), 2015.
10. Josphineleela. R. and M. Ramakrishnan, An Efficient Automatic Attendance System Using Fingerprint Reconstruction Technique . International Journal of Computer Science and Information Security, Vol. 10, No. 3, March 2012.
11. O. Shoewu and O. A. Idowu, Development of Attendance Management System using Biometrics. The Pacific journal of Science and Technology. Volume 13, Number 1, May 2012.

AUTHORS PROFILE

Ashish Chauhan is working as Asst. Professor In Department of Information technology at SRM Institute of Science and technology. He has done his B.Tech from UPTU and M.Tech from UTU and currently pursuing Ph.D. He has experience of more than 10 years in field of teaching and research. He is Member of many International Societies and Associations like UACCE, IACSIT, IFERP and ASSET. He has published many research papers in the field of cyber security in many National and International Journals of repute. His area of interest is Information Security, Network Security and Distributed computing.

Shruti Khosla B.Tech Scholar in Department Information Technology from SRM Institute of Science and Technology. Her area of interest in her degree program are database management, Information and Network Security.
She is keen to learn new technologies and expert in python and Android Studio She is currently studying research project on Information security. She is being selected for MS program for RMIT, Australia

Muskan Sharma is B.Tech Scholar inDepartment of Information Technology
SRM Institute of Science and Technology. Her area of interest in her degree program are database management, Information and Network Security.
She is keen to learn new technologies and expert in python, data Science and Android Studio. She is placed Cognizant and currently undergoing training at Cognizant training centre Pune

Sarthak Sahni is B.Tech Scholar inDepartment of Information Technology SRM Institute of Science and Technology. His area of interest in his degree program are database management, Information and Network Security.
She is keen to learn new technologies and expert in java, python and Android Studio. He is placed Cognizant and currently undergoing training at Cognizant training centre Pune