IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Implementing Electronic Dissemination of Documents Using Three Layers of Security

Banoth Thirumal[1*], R. U. V. N. Satish[2], M. Vivekananda Swamy[3]

[1*,2,3]Indian National Centre for Ocean Information Services, Hyderabad, Telangana, India.

[*]*Corresponding Author: thirumal.bhanoth@gmail.com, Tel.: +91-9966339685*

Available online at: www.ijcseonline.org

Accepted: 12/Jul/2018, Published: 31/Jul/2018

Abstract — Cyber-crime and data breach has been growing exponentially in present world. In this scenario, it is important for any organization to have a robust method for the transactions of confidential data through the internet. The primary purpose of this study is to develop a completely safe and secure application that enables an organisation to disseminate electronic documents over the internet to their subordinate bodies. The current study is implemented in a university for disseminating the examination question papers to its affiliated colleges and examination centres during the examination season using a safe, secure and robust application. In this application there are three layers of security techniques are proposed. Documents can be sent to multiple centers simultaneously and are secured with Advanced Encryption Standard technique. This application involves Automated Interface Module which is used to encrypt the documents at university end and then decrypt them at examination center. This system also provides a feature for scheduling the process of dissemination of documents. This system uses RSA and AES Encryption methods and SHA-512 hashing algorithm for ensuring security as well as privacy of documents to reduce threats of attackers and maintain the confidentiality of this system. In the existing traditional delivery system, delivering a question paper from a university in real time is a challenging task due to involvement of logistics and lack of traceability. Through the empirical review of the existing traditional delivery system, the proposed system eliminates the risk of data breach and even impacts on the financial level by using proactive and pragmatic methods that seeks both security and consistency.

Keywords **—** Hashing, Dissemination, Security, Examination, Document, Encryption, Scheduling, AES, RSA.

I. INTRODUCTION

In recent times the reality is that each and every individual or an organization connected to the internet is vulnerable to cyber-attack. The number, type and sophistication of these attacks are continuing to grow in a rapid phase. Electronic dissemination of documents using three layers of security is secured document delivery system application software developed for providing wide circulation of electronic documents via internet from a server to various clients. These layers of security have been provided by implementing various encryption techniques on the data. In the current application this mechanism is implemented in a University for the process of delivering examination question papers during examination season to all the enrolled or affiliated colleges and examination centers.

A. Existing System: In the present system transport of examination question papers starting from the preparation of question paper till reaching the examination centre, entire processes are done manually at every level as of now. Firstly the question papers are being printed in a different state. Then they are transported by vehicles to various examination centres. This consumes a lot of manpower and also is not a secured way to handle the question papers. It is also very costly process. The entire process seems to be cumbersome and therefore requires a better way.

B. Proposed System: As the existing system has many difficulties and is not secure, there needs to be a way where things are organized and controlled by a centralized authority. This can be achieved by using an application that provides all the required functionalities. The question paper documents are encrypted and zipped with randomly generated password and then sent to examination centers. These exam centers can simply login to the website and download their respective files and later decrypt them with the key received. The entire software usage feels just like a walk in park and an average user with minimum technical knowledge can be easily able to use it. The primary goal of the proposed system is to develop a completely safe and secure application that enables an Organization to disseminate document over the internet to their affiliated bodies.

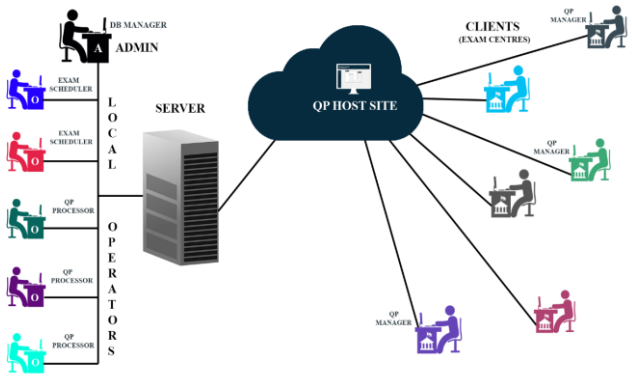

Figure 1: Basic Model of Application Software.

The fig 1 shows the basic model of the application software which contains its main users and various components in the entire system. This system has two main users i.e., Administrator and Client.

Rest of the paper is organized as follows, Section I contains the introduction of study, existing system and proposed system, Section II contains the related work of this paper, Section III explains the methodology of the application software and servers side and client side flow charts, Section IV shows the obtained results of the software, section V contains overall conclusion and future scope of this application software.

II. RELATED WORK

Earlier studies compared various encryption and hashing techniques and proposed the necessity of these techniques while sending data via internet. These studies also focused on importance of hybrid encryption and hashing techniques. This paper addresses the implementation of encryption and digital signature technique for electronic health record in prevention of cybercrimes such as Data theft, Data diddling and Identity theft etc., [1]. In this study authors implemented RSA 2048-bit algorithm, AES 256-bit and SHA 256 using java programming. This application is know as Secure Electronic Health Record. In the application, there are two main schemes, namely the protection scheme and verification scheme. Concepts of digital signature and file encryption are used not only to solve data integrity, confidentiality, non-repudiation, availability, and authentication problem but also to prevent robbery, modification and unauthorized access. The cryptography aspect is expected to ensure the file records and electronic documents on patient's identity, examination, treatment, action and service given and the authorized person. The implementation of encryption and digital signature in this research can prevent archive thievery which is shown on implementation and is proven on the test.
RSA Algorithm is first Public-key cryptography implementation, which is named after three MIT mathematicians Ronald Rivest, Adi Shamir, and Leonard Adleman who developed it. In the paper the authors have proposed a unique method for implementing the public-key cryptosystem [2]. This cryptosystem security rests in part on the difficulty of factoring large numbers. The authors in this paper have produced the public key by factoring large numbers. This cryptosystem is under observation and they say that if the method is adequate then it provides secure communication, which reduces the couriers to carry keys. This key-pair in this algorithm is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules; these prime numbers may be of 100 or more digits in length each, yielding an n which contain digits of twice as many digits as the prime factors. According to this study public key contains information of value of n and also a derivative of one of the factors of n; a hacker cannot determine the prime factors of n, from this information alone and that is what makes the RSA algorithm so secure. They have also mentioned cryptanalytic approaches like factoring n, Computing φ(n) Without Factoring n etc.,

The authors in this paper, presents the method to transfer files over internet by secure encryption system [3]. They propose three hybrid encryption techniques like AES, RSA and HMAC. Symmetric AES algorithm here used to encrypt files, asymmetric RSA use to encrypt AES password and HMAC to encrypt symmetric password. This paper makes the secure communication and transfers of the files by using 3 encrypting techniques and makes it hard to attackers by common attacking methods. Communication of information this paper is shown in between the server -client and client and client.

M. S. Abutaha and A. A. Amro are the authors of paper in which they discussed about cloud security by efficiently using RSA, AES and SHA1 [4]. As all the services, information, data and software are stored on cloud; the author says it is vulnerable for attacks by attackers. So the author proposes a modal which uses AES and RSA algorithms for securing variety of data on cloud and connection based on different keys in encryption and decryption of data and information. SHA1 algorithm is used to secure the hash table of data. The specific thing in this cloud security modal is key management center where the author used it as a third party for keys distribution in all stages whenever the key is required by the modal.

Authors of this paper Joan Daemen and Vincent Rijmen, "AES Proposal: Rijndael" speaks about block cipher, inverse cipher and key security [5]. They use mathematical preliminaries like addition, multiplication, polynomial coefficient for encrypting the information and key. The Rijndael Round transformation has been modeled to provide high multiple-round diffusion and even guaranteed distributed nonlinearity. These are perfect requirements for the state updating transformation in a stream/hash module such as Panama [DaCl98]. The author also says about the limitation of this methodology like inverse cipher is less

suited to be implemented on a smart card than the cipher itself: it takes more code and cycles. In software view, the cipher and its inverse make use of different code and/or tables whereas in hardware view, the inverse cipher can only partially re-use the circuitry that implements the cipher.
Here the author says that better security method provides good security and efficiently decreases computational complexity [6]. In this paper, authors implemented, content based algorithm which follows famous symmetric key cryptography method. This method use binary addition operation, circular bit shifting operation and folding method. The process of encryption and decryption is done along with same secret key and moreover the encryption technique has been applied to some small text rather than a file. The secret key is also sent along with the contents encrypted i.e. cipher text. The security of the key is provided by circular bit shifting operation and folding method.

III. METHODOLOGY

During development of this application three layers of security are proposed and then implemented. The first layer of security layer consists of Advanced Encryption Standard (AES) encryption of documents (PDF files in this case). In this layer required document is encrypted by AES with 256 bit key length for 14 rounds. Randomly generated this AES key is saved in database and the same key is sent to corresponding client (QP manager) as SMS just half an hour before the exam which is used during the process of decryption.

The second layer of security layer consists of archiving corresponding documents of an exam center in the form of bundle using zip file with a randomly generated password for each client and then this password of zip is encrypted with the help of RSA encryption technique using the public key of the client and then saved in the server as KUZ file. All these archives will be available to download for clients only just one hour before the exam. Clients will login to web application using username and password just one hour before exam and download these KUZ files. After downloading these KUZ files client will open them using the desktop application installed at client side and automatically decrypt them using the private key of RSA encryption technique and then the client is requested to enter the AES key received in the form of SMS. After successfully entering the key the documents are decrypted and are now readable by the QP manager.

The third layer of security layer consists of saving the passwords and keys only after using hashing algorithm SHA-512. All the passwords of clients and AES keys are not directly saved in the database in readable format but are hashed before saving them in database. The entire system is developed using a well known client server model. The system contains local system, web server and clients. The complete architecture of remote document routing system is given in the following fig 2.

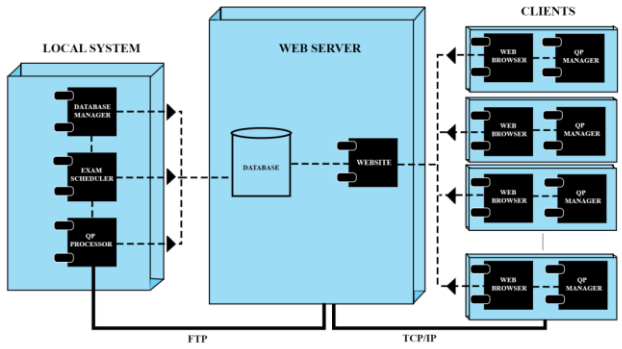

Figure 2: Architecture of the application.

Various components are shown in the component diagram and their functionality is explained below:

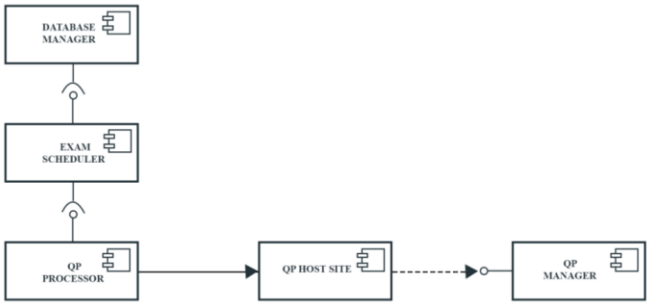

Figure 3: Component Diagram of the application.

A. Database Manager: The main functionality of this module is to enroll various exam centers and examinations which are being held under the examination branch to be enrolled or gathered so that they can be used in the further process. During the enrolment of exam centers the user name has to be entered manually. A password is automatically generated with length 8 and follows secure password policy. RSA Keys both public and private key for each examination centre are also generated simultaneously and they are stored in the server which is further used in the encryption process. The RSA Key generation is done by python script and then transferred from the local machine to the server by using an FTP Connection.

B. Exam Scheduler: This module is used for preparation of the schedule of all the exams that are going to be held at various centers. The entire schedule is stored in a table in the database. Based on the table the question papers are grouped and hosted on the website. The main functionality of this module is creating a schedule. The schedule is created by selecting the date, then selecting an exam centre and then selecting the exams that are being held at that centre on that particular day. After the process of scheduling is completed then the dissemination of documents using scheduler module is done automatically at prescribed time.

C. Question Paper Processor: The Question paper processor is used for accepting the question paper files, bundling the question papers for each centre, then encrypting them and uploading them to a file server. This module contains three different functionalities which are uploading the question paper files, generating the KUZ files, or postpone an exam which has already been scheduled and question paper has been uploaded. In this module encryption process is defined in the core script in python. The encryption functionalities are used from an imported module called pyCrypto.

D. QP Host Site: The QP Host Site is a website that is used by the clients to download the encrypted KUZ files which contains question papers of exams that are being held in that exam centre. The users who are the operators at the examination centres will be able to login to the website by using the credentials given to them by the examination branch. The website is secure enough to withstand many of the modern day attacks. SQL Injection attacks which are the major percentage of modern day attacks are also handled and taken care of by special function which validates the input fields.

E. QP Manager: This module is used by the clients at examination centers for decrypting the KUZ file that is downloaded from the website. The user has to first login to the website by using the credentials that are provided by the exam branch authorities and download these KUZ files. Then by using the QP Manager software the file can be decrypted. The file must be selected and then the 16 digit decryption key which is received 15 minutes before the examination on the client mobile phone in the form of SMS. The question paper files will be decrypted into the same folder where the KUZ file was downloaded. The decryption process is done by a Python script. The script uses functions for decryption which are imported from a module called as PyCrypto. The executables are created by using another Py2exe.
Timely how the events are carried out is show in the sequence diagram fig 4.

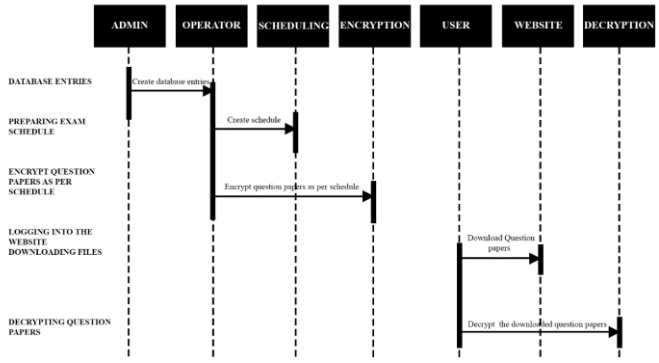

Figure 4: Sequence Diagram of the application.

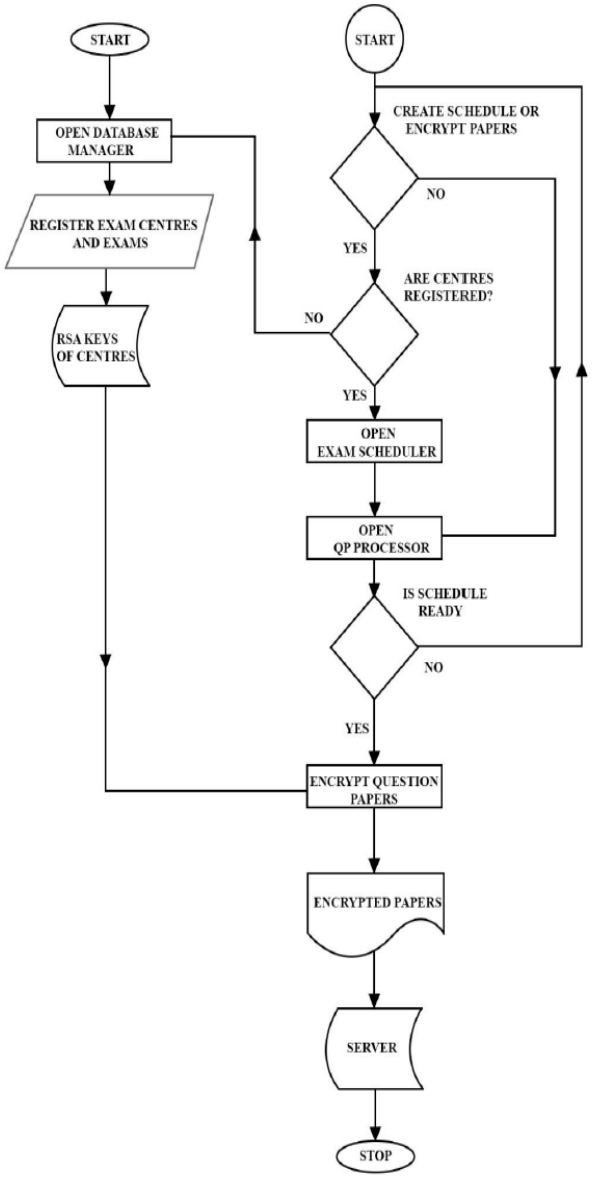

Figure 5: Flow Chart of Server Side Activity.

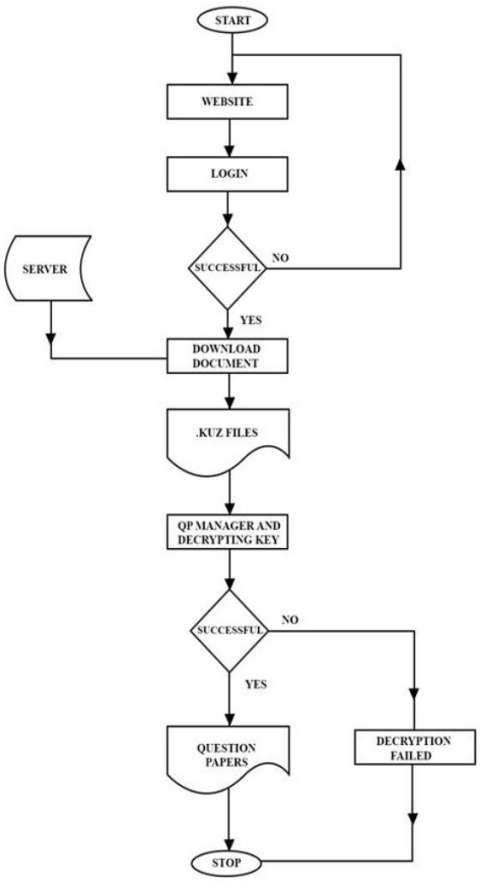

Figure 6: Flow Chart of Client Side Activity.

IV. RESULTS AND DISCUSSION

The complete system is well tested and reviewed. The following are various screen shots of application developed at various levels. Fig 7 interprets the database manager module where admin can perform database transactions. Fig 8 shows QP processor module at server side where encryption and KUZ file generation is done. Fig 9 shows QP processor manager module at client side where decrypting is carried on. Fig 10 interprets Question Paper Manager Module after decryption where client can view the decrypted documents.

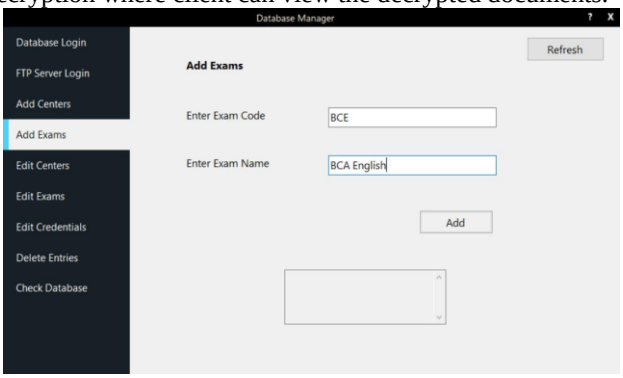

Figure 7: Screenshot of Database Manager Module.

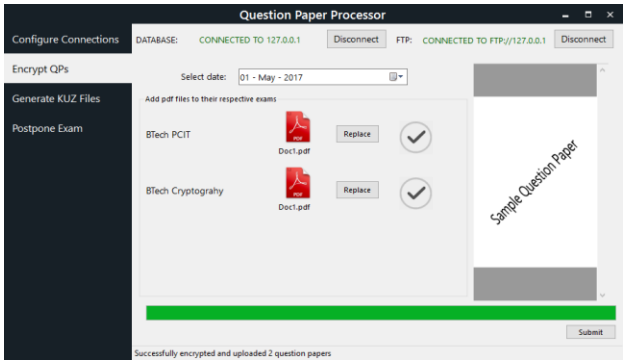

Figure 8: Screenshot of Question Paper Processor Module at server side.

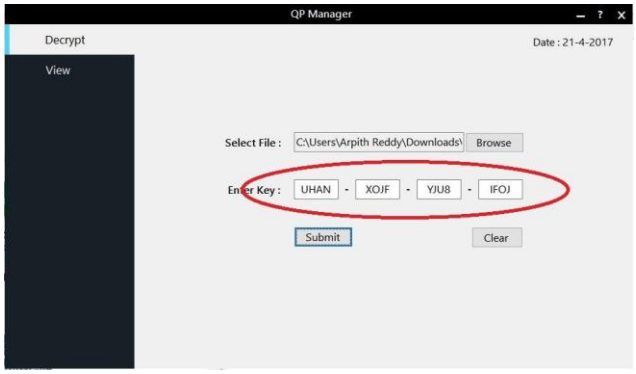

Figure 9: Screenshot of Question Paper Manager Module at client side.

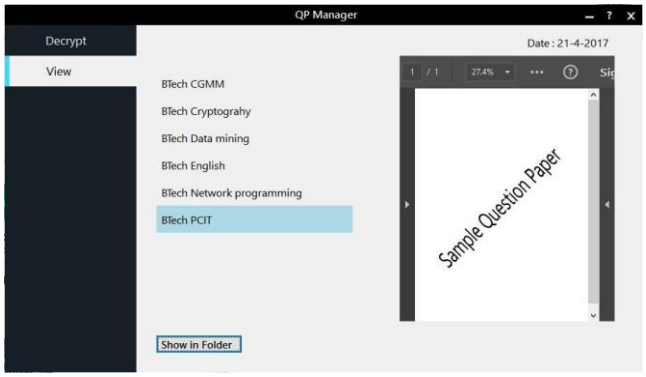

Figure 10: Screenshot of Question Paper Manager Module after decryption.

V. CONCLUSION and Future Scope

The primary goal of the proposed system is to develop a completely safe and secure application that enables an Organisation to disseminate document over the internet to their affiliated bodies. The main purpose of the application is to eliminate the time and expense of traditional document delivery in the existing system. In addition to this user can also even schedule the process of dissemination of documents using scheduler module. This system ensures security as well

as privacy of documents and also reduces the threat of attackers and maintains the confidentiality of this system.
The present project deals with only electronic documents as per the requirement but in future the same application can be upgraded to transfer various other types of files. Furthermore there is a vital need for continuously upgrading and updating the security protocols, policies, mechanisms and their dynamic adaptation to cope with the evolving security threats.

ACKNOWLEDGMENT

We would like to acknowledge every person who is directly or indirectly connected with this project and for the output of this paper. We especially thank our Parents and other Family Members for their encouragement without which it was highly impossible to take up this task. We thank our organization administration for providing sufficient tools to make use of them and get this activity successfully done. We thank each and every Colleague and Friend for their support and help in writing this paper.

REFERENCES

[1] M. A. Sadikin, R. W. Wardhani, *"Implementation of RSA 2048-bit and AES 256-bit with digital signature for secure electronic health record application"* in ISITIA, Lombok:IEEE, pp. 387-392, 2016.
[2] R.L. Rivest, A. Shamir, and L. Adleman, "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"*, Communications of the ACM. 21 (2): pp. 120–126, 1977. doi:10.1145/359340.359342.
[3] Eman Salim Ibrahim Harba, "*Secure Data Encryption Through a Combination of AES, RSA and HMAC*", Engineering, Technology & Applied Science Research Vol. 7, No. 4, 2017, pp. 1781-1785.
[4] M. S. Abutaha, A. A. Amro, *"Using AES, RSA, SHA1 for Securing Cloud"*, International Conference on Communication, Internet and Information Technology, Madrid, Spain, 2014.
[5] Daemen, Joan, Rijmen, Vincent. (March 9,), *"AES Proposal: Rijndael".* National Institute of Standards and Technology 2003; pp. 1. Retrieved 21 February 2013.
[6] Sourabh Chandraa, Bidisha Mandalb, Sk. Safikul Alamc, Siddhartha Bhattacharyya, *"Content based double encryption algorithm using symmetric key cryptography",* in International Conference on Recent Trends in Computing (2015).
[7] Sachin sharma1, Jeevan Singh Bisht, "*Performance Analysis of Data Encryption Algorithms*", in International Journal of Scientific Research in Network Security and Communication Volume-3, Issue-1, 2015, pp. 1-5.
[8] V. Kapoor, "*Data Encryption and Decryption Using Modified RSA Cryptography Based on Multiple Public Keys and 'n'prime Number*", in International Journal of Scientific Research in Network Security and Communication Volume-1, Issue-2, 2013, pp. 35-38.
[9] G. van Rossum, "*Python tutorial*", Technical Report CS-R9526, Centrum voor Wiskunde en Informatica (CWI), Amsterdam, May 1995, pp 1-71.
[10] Behrouz A. Forouzan, "*Cryptography and Network Security*", the Mc-Graw Hil Companies, USA, pp. 293-336, 2007.
[11] Stalling, W., "*Cryptography and Network Security: Principles and Practice*", 6th ed.; Prentice Hall, Inc.: Upper Saddle River, NJ, USA, pp. 327-361, 2014.

Authors Profile

Mr. B. Thirumal pursed Bachelor of Technology from Kakatiya University Warangal, Telangana in 2017. Prior to this he pursued special diploma in computer programming from Government Institute of Electronics, Maredpally, Secunderabad in the year 2013. He is currently working as Scientific Assistant in Ocean Information and Forecast Services Group, Indian National Centre for Ocean Information Services (INCOIS), Hyderabad, Telangana since 2017.. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. He handled many projects as project head during his education in diploma and Bachelor of technology in computer science.

Mr R U V N Satish pursued Bachelor of Science in Computer Science and Engineering from Osmania University, Hyderabad, Andhra Pradesh and Master of Science in Computer Science from Acharya Nagarjuna University Guntur, Andhra Pradesh in the year 2015. He also pursued Master of Science in Mathematics from Osmania University Hydeabad, Telangana in the year 2017. He is currently working as Scientific Assistant in Indian National Centre for Ocean Information Services (INCOIS), Hyderabad, Telangana since 2013. He is a life member of Indian Meteorological Society (IMS) since 2015. He has published 4 research papers in reputed international journals and 4 technical reports and it's also available online. His main research work focuses on Application Development, Data Encryption and Hashing, Data Processing, Data Analytics, Data Mining, Data Visualization and Computational Intelligence based education. He has 5 years of experience in Web and Mobile Applications Development and 5 years of Research Experience.

Mr M. Vivekananda Swamy pursed Bachelor of Technology degree in Computer Engineering from Jawarharlal Nehru Technological University(JNTU) Hyderabad and Masters in Computer Science Engineering from Jawarharlal Nehru Technological University(JNTU) Hyderabad. He also have Diploma in Computer Management Engineering from State Board of Technical Enducation and Training(SBTET). He worked as a Software Developer in the field of IT. He is currently working as Scientific Assistant in Indian National Centre for Ocean Information Services(INCOIS) since 2010. He has already published 4 research paper in reputed international and UGC approved journals. His main research work focuses on Application Development, Data Security, Computer Software Application Systems, E-Learning Techniques, Android Applications, Web Services, Cryptography Algorithms, Data Handling Algorithms and Techniques and Intelligence based education techniques. He has 2 years of software application development and 8 years of Research(R) and Development(D) Experience.

