DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5883

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SECRET KEY BASED STRING REVERSE ENABLING USER LEVEL ENCRYPTION TECHNIQUE FOR DATA SECURITY

Kaushik Kumar
Department of Computer Science & Engineering
JIS College of Engineering
Kalyani, Nadia. W.B. India

Sourav Ghosh
Department of Computer Science & Engineering
JIS College of Engineering
Kalyani, Nadia. W.B. India

Sudipta Sahana
Department of Computer Science & Engineering
JIS College of Engineering
Kalyani, Nadia, W.B. India

Abstract: Datain the context of a communication network is nothing but any type of stored digital information and data security is all about protecting that stored digital information. Securing data means taking protective digital privacy measures that are implemented to prevent unauthorized access to any kind of digital information's shared over the communication network. In this paper, we have proposed a technique, how an individual user can protect their data's which is shared over the communication network. One of the principal challenges of data sharing on the data communication network is its security. This is revolving around the fact that once there is connectivity between computers sharing some resources, the issue of data security becomes critical. Cryptography provides functionality for the encryption of data, and authentication of other users. The cryptographic methodologies are one of the popular ways of achieving data security by encrypting the messages to make them non-readable. There are many cryptographic techniques available and it is an essential information security tool. It provides the four most basic benefits – Confidentiality, Authentication, Data Integrity and Non-repudiation. Nowadays the security of communication is a crucial issue over the internet and cryptography has come up as a saviour of this problem. In modern cryptography, it operates on binary bit sequences and it secures communication to possess the secret key only.

Keywords: Data encryption & decryption; Data security; String reverse; user enabled; secret key encryption.

I. INTRODUCTION

We all know how necessary and important to keep secure our data in today's modern world where the world is moving towards digitalization. Data security provides data protection and also prevents from data corruption across the enterprise. Data Information security is an essential view among IT organizations of all sizes and type. To handle and control this growing concern, most of the IT firms are moving towards cryptographic techniques to protect their valuable and secret information's. Cryptography techniques can secure data from unauthorized access. By using data encryption we can protect valuable information from unauthorized parties by transforming actual data of a given format, called plaintext, to another format, called ciphertext, using encryption algorithm and an encryption key.

There are four basic Cryptography goals for data security - Confidentiality, Authenticity, Data Integrity, and Non-repudiation. Cryptography mechanisms are based on mathematical algorithms to encrypt and decrypt data. Cryptographic algorithm alters data from a human readable form (plain text) into a protected form (ciphertext), which is known as encryption and vice-versa known as decryption. Modern cryptography is based on mathematical algorithms; secret key plays an important role in encrypting and decrypting the original information to the authenticated user.

II. RELATED WORKS

In this section, we will discuss acknowledged and published works in the annals of Data Security using cryptographic techniques back supported by robust and stable cryptographic algorithms. Many works have been done earlier in this field related to data security using a secret key or private key provided by the user for securing their personal information's. The most popular well known cryptographic algorithm known as RSA Algorithm, which is very widely used in different ways to protect and secure data while it is being transmitted over the internet to the destination.

Previously an attempt was made by Authors K. Oyetola Oluwadamilola, A. Okubanjo Ayodeji, O. Osifeko Martins, I. SanusiOlufunmi, O. AboladeRapheal in their paper named

"An improved authentication system using hybrid of biometrics and cryptography [1]", they proposed an idea where they presented a combination of cryptography and biometrics; a bimodal biometric Cryptosystem, using fingerprint and face as trait for authentication. Confidential information was encrypted using Advanced Encryption Standard (AES) and biometric templates were stored as Binary Large Object (BLOB) in MYSQL database which was secured with Message Digest 5 (MD 5) Hashing Algorithm. The system was developed and implemented to operate on one-try, two-try and three-try configurations at varying threshold values. The developed system's performance was evaluated using False Reject Rate (FRR), False Accept Rate (FAR) and Receiver Operating Characteristic Curve (ROC graph) as performance metrics for the proposed idea.

Authors Sudipta Singha Roy, Shaikh Akib Shahriyar, and Md. Asaf-Uddowla in their paper entitled**"A novel encryption model for text messages using delayed chaotic neural network and DNA cryptography" [2]** proposed a novel model for encrypting text messages using time-varying delayed Hopfield neural network and a posterior DNA cryptographic model. The chaotic neural network applied here is used to generate a binary sequence which is later passed to a permutation function and used to generate the key for the first level encryption. The plaintext is converted to a corresponding binary sequence after a conversion to ASCII value and encrypted by switching of chaotic neural network maps and a permutation function which is dependent on the binary sequence generated from the chaotic neural network. An additional DNA cryptographic model is used over the ciphertext obtained from the first level encryption to robust the security of the proposed model.

Authors Hosam F. El-Sofany, Samir A. El-Seoud in their paper **"Studying Security of Data in Cloud Computing through Cryptographic Approach" [3]** proposed an idea how to secure a communication over Cloud network, how data can be protected by the method of encryption. Encryption exchanges the data by an encryption algorithm using the key in the twisted form. Only that user can access the original message, who have the same key which was used to encrypt data. The purpose of encryption is used to prevent leak or secrecy in communications. Encryption algorithms play a huge role in providing data security against bad and malicious attacks from the intruder's side. This paper presents the basic concepts and analyzes the essentials of data security issues pertaining to Cloud Computing.

Authors Sanket A. Ubhad, Prof. NileshChaubey, Prof. Shyam P. Dubey in their paper titled "**Advanced ASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id**" [4], proposed a technique where they send information over the network in a set of 3 keys. Generally, a hacker tries to get access to the key used for encryption but in their approach, they have used a combination of word range and matrix multiplication in implemented for encrypting the information.**"An Integrated Approachusing Stream Cipher Cryptography and Entropy Encoding"**in [5] describe a methodology which uses both the encryption techniques and data compression. Firstly, theyare reducingthe actual data size by implementing data compression techniques and then the output is encrypted to raise its security.Thus, the technique proposed in their paper is useful in reducing data size, raising data transfer rate and providing security during communication. In their proposed system, encoded string is created from the input string of symbols and characters based on entropy encoding technique.

Authors Deepti Chaudhary, Rashmi Welekar - "**Secure Authentication Using Visual Cryptography" [6],** in their paper proposed a cryptographic technique which allows visual information (text, picture, etc.) to be encrypted in such a way that decryption becomes a mechanical operation on the receiver's side that does not require a computer. Visual Cryptography deals with any type of secrets such as printed or pictures, etc. These secrets are delivered into the system in a digital (image) form. The secrets which are in a digital form divided into different parts based on the pixel of the digital secret. These parts are called shares. To visualize the secret, the shares are then overlapped correctly.

III. PROPOSED WORK

In this paper, we have proposed a technique how an individual user can protect the confidentiality, authenticity, and integrity of their information's over the internet when it is getting shared across the communication network via some web applications used by the user on World Wide Web. Here the user plays the key role for the working of the whole algorithm as the working of the proposed algorithm in this paper is based on the secret key provided by the sole user.

Before discussing the proposed technique and the working of the algorithm in this paper. Let's discuss few points which are pre-requisite it in details, which will give a better insight on the proposed technique and the algorithm functionality. As the proposed algorithm technique is fully based on data, the secret key provided by the user and the encryption-decryption methodology used. For the encryption-decryption process, XOR operation is used explicitly to provide better and secure encryption. So, we should know about the XOR operation (known as eXclusive OR in terms of computer terminology).

(A). Basic Terminology of Cryptography:

Computers are used by millions of people for many purposes such as banking, shopping, military, student records, etc. where Privacy is a critical issue. So we need to make sure that unauthorized parties cannot read or modify messages.

Cryptography is associated with the process of the transformation of human readable and understandable data into a form which cannot be understood by another person except the person whom it is intended can read and process it, in order to secure data. The data that we want to hide, is called the plaintext, it could be in any form or any other sort of

digital information. This plaintext is a human-readable message before encryption or after decryption. The information that will be actually transmitted over the communication network is called the ciphertext or the encrypted message, this term can be referred to the string of "meaningless" data, or unclear text that nobody must understand, except the intended recipients who has the decoding algorithm and key.

The actual data or plaintext is encrypted into ciphertext using aCryptographic algorithm, this method is called encryption or in other words, it's a process of converting human readable and understandable data into "meaningless" data. In the decipher text, the inverse of the key will be used inside the algorithm instead of the original key.

(B). XOR Encryption:

The binary operation XOR operand will compare two input bits and will produce one-bit output in return. The output bit will be equal to 1 if the two compared input bits were unequal, or else 0 if they were equal.

XOR encryption is commonly used in several symmetric cryptography (especially AES). In asymmetric cryptography the same key is used for both the encryption and decryption process. The XOR operand is so useful to each bit between the plain text which we want to encrypt and the key we will choose.

Understanding with examples are better than words, so let's take the word "sourav". We want to encrypt it with the key "kwe".

First, we need to convert the input string and the key in binary representation:

ram: 01110010 01100001 01101101
kwe: 01101011 01110111 01100101

Then we compare each bit of the input string and the key with the XOR operand. Which will give you this:

ram : 01110010 01100001 01101101

kwe: 01101011 01110111 01100101

Output: 110010001011000001000

If we want to go back to the original input ("sourav"), we just need to reapply the XOR between the output and the key.

If the provided key was the same length than the input string, it wouldn't be interesting because we would also have to send the key to the person you want reading the input.

In contrast, when the key and the input string have the same length, it is not possible for someone to crack the cipher. So, when the key is smaller than the input, we just repeat it until we reach the end of input and length of both input string and the key is same. If for example, I want to encrypt the word "sourav" and the key "kwe", I would do it this way:

sourav:

01110011 01101111 01110101 01110010 01100001 01110110

kwe:

01101011 01110111 01100101 01101011 01110111 01100101

Output:
110000001100000010000000110010001011000010011

If you look at the second string, you can see that we simply repeated the key to match the length of the input string. The smaller the key, the easiest it will be to crack your ciphertext.

(C). Cryptography Goals:

By using suitable cryptographic methodologies many goals can be achieved, these goals can be either all achieved at the same time in one application or only one of them.

These goals are:

1. Confidentiality:

It means data privacy. It is the most important goal that ensures that unauthorized individuals will not be able to access the sensitive information except the one who has the secret key.

2. Authentication:

Using this process the user or the system can establish their own identity to other parties who does not have anyownawareness of their identity.

3. Data Integrity:

It ensures that the intended receiver receives the same message that was sent by the sender.The data may get modified by an unauthorized entity intentionally or accidentally in the digital world. Integrity technique confirms protects against unintentional alteration of the message.

4. Non-Repudiation:

When a message is sent, the receiver should have the right information to prove that the message was sent by the real user and when a message is received, the sender should able to prove that the message is received by the actual receiver.

(D). Proposed Technique Ideation and Flowchart:

The proposed algorithm in this paper consists mainly of four parts namely the **raw inputted data** entered by the user, the **secret key** used for encryption process the **encrypted message** and the **decrypted message** after checking the authenticity of the data. There are many ways of classifying data cryptographic algorithms but for the purpose of this, they will be classified based on the number of bits of secret keys and the number of bits of originals data.

The figure below shows the flowchart of the proposed methodology, on which the whole program runs. Starting from the initial phase where the user is asked to enter the data's which is reversed in the second phase of the program after which user is asked to enter a secret key which is used for the encryption process. Then it displays the encrypted text.

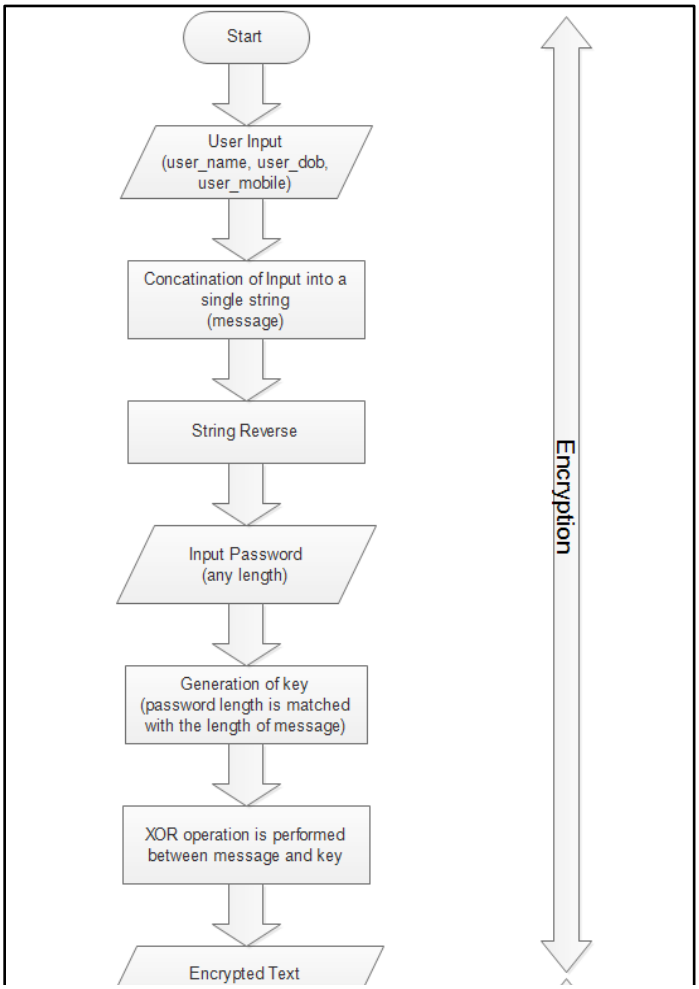


Fig.3 (a) – Flowchart for the Data Encryption with Secret Key

The figure below next shows the flowchart for the decryption process, where the user has the encrypted text and the same key (or cipher) which was used to encrypt the original data. If the user doesn't have the same key and enters a different key the decrypted results will be different from the original data. This result will also indicate that the receiver is not the intended receiver to whom the message was sent by the actual sender. There is ahazard in this system is that if sender or the receiver loses the key or the key is changed, the system is out of order and messages cannot be exchanged safely.

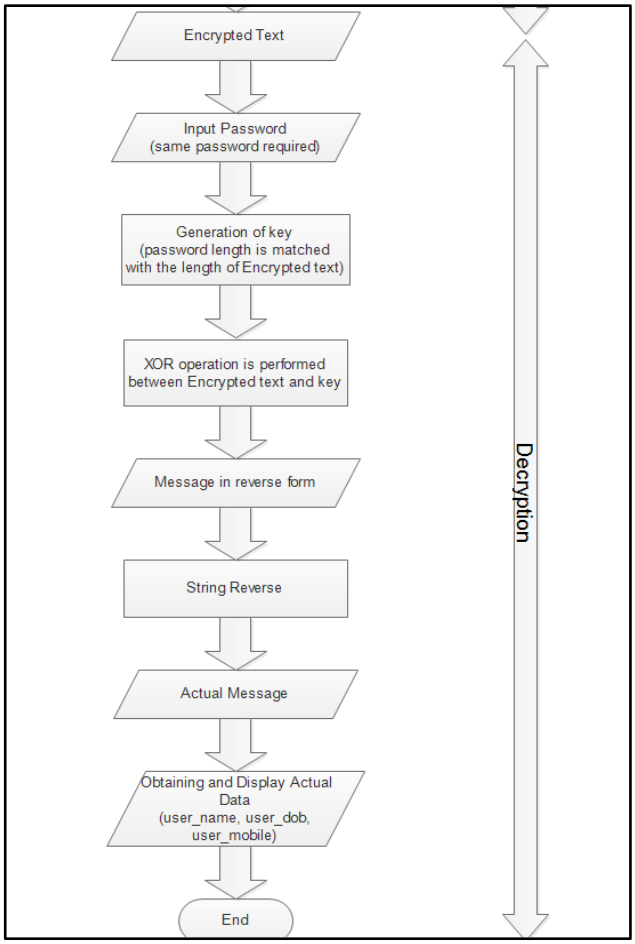


Fig. 3(a) – Flowchart for the Data Decryption with Secret Key

Data Encryption

Data encryption converts data into a form which can be accessed by the people having the secret key or password. Data encryption protects information or data confidentiality while it is transmitted over the internet. Authentication allows for the verification of a message's origin. Data integrity proves that the received message is same as the sent message means the message's content has not changed. Original data or plaintext is encrypted into ciphertext with an encryption algorithm and an encrypted key. The encrypted ciphertext message is then sent to the receiver over the internet. Then the receiver's computer takes the encrypted message and performs decryption with the decryption algorithm and the correct key to obtain the original plaintext message. The decryption algorithm must be same as the encryption algorithm, working methodology should be same which is used in the encryption technique. Public Key, as the name suggests, it can be shared with everyone, but the Private Key must be protected. So, in case of this encryption, the sender should lock the message using recipient's public key (as the public key is known by everyone) so that the receiver can decrypt or unlock the message by his own private key which is only known by the

receiver. Data Encryption protects data from several attacks and from hackers too and also prevents data loss.

IV. PRACTICAL WORKING AND RESULTS

Here, the proposed technique is working in various phases to make the data secure using the user enabled secret key, such that the data can be shared over the communication network and the data get transmitted over the communication network without being accessed or altered in between by any third party and it is delivered to the exact receiver to whom it was intended to be sent. The proposed technique has various phases which include different steps of the algorithm working towards the single goal which is Data Security using user enabled secret key.The proposed algorithm is scripted into a working code written in C++ programming language and was successfully compiled and run Turbo C++ environment running on Windows Operating System and tested successfully with results. The Graphic User Interface (GUI) is designed to be user-friendly and can be used by anyone with or without any knowledge of programminglanguage. The following figures below shows the overall working of the proposed algorithms which was observed while practical implementations of the algorithm. Running the program gives a frame with menus and other options to perform specific tasks.

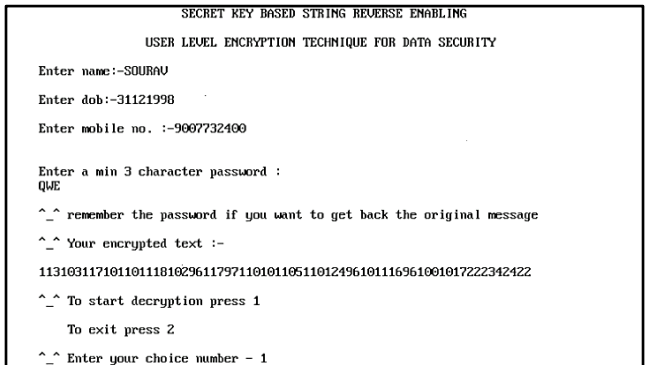


Fig.3 (a) - User Input screen & Encrypted text

First, the Fig. 3(a) shows the input frame where the program asks the user to enter few Identity-related data such as Name, D.O.B and Mobile Number which are taken as raw data by the program and temporarily saved as a single long string and then it is reversed to increase the security of the data.

After receiving the Data input successfully, program asks the same user to enter a secret key (should be minimum of length starting from 3 characters) which should be private to the user and the same will be used by the program to encrypt the raw data by performing XOR operations with the after matching the length of the inputted data and the secret key entered by the user. If the length of the secret key is not same as that of the original data then it is made of the same length by the algorithm in order to perform XOR operations with the original data inputted by the user for encryption. After the XOR operation is performed by the program using the original data inputted by the user and the password provided by the user, the program encrypts the data and displays it to the user.

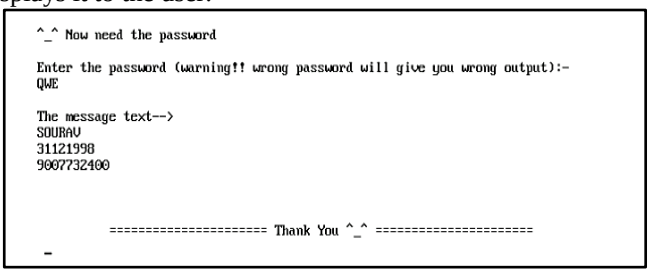


Fig. 3(b) – Authenticity check and decrypted text

The figure – Fig. 3(b) above shows the frame where the program asks the user to enter the same secret key to decrypt the encrypted message. The decryption process the similarly performed again by the program by performing XOR operation of the secret key and the decrypted message. If the same key is provided to decrypt the encrypted message then the user will get exact data which was encrypted using that secret key.Otherwise, if the wrong key is provided to decrypt the encrypted message then the concerned user will not get the original data.

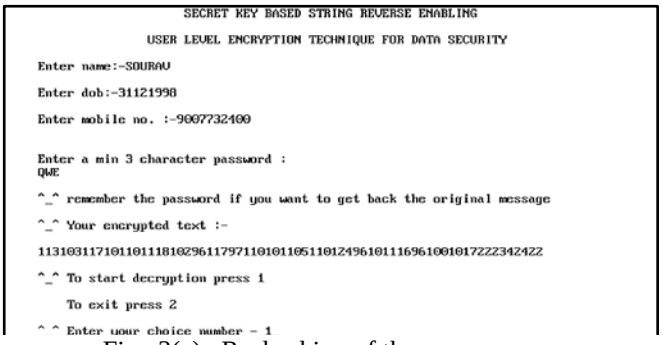
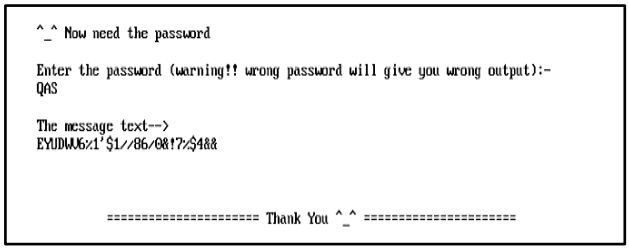


Fig. 3(c) –Rechecking of the program



The above figure – Fig. 3(c) shows an output frame where the same data is encrypted with a secret key but we intentionally provide a key that is different from the original secret key. Hence the user receives incorrect display, as the user has entered a wrong secret key dissimilar to the original secret key which was initially used for encryption which is shown in the figure Fig. 3(d).

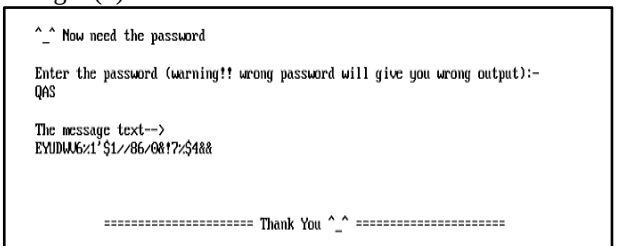


Fig. 3(d) – Rechecking using a different key.

V. CONCLUSION

This paper has presented a technique for data encryption and decryption by using a user enabled secret key. With the help of this Cryptographic Software, a confidential data can be kept secured by a user when it is shared over the communication network environment. Here in this paper cryptography method is used in such a way in that it ensures that the contents of a message are confidentiality transmitted and would not be altered by any third person other than the specified receiver. By Confidentiality I mean to say that nobody can understand the received message except the one (the intended receiver) who has the samekey which was used at the time of encryption, and "data cannot be changed" means the original information cannot be changed during transmission.

VI. ACKNOWLEDGMENT

This section was introduced late in the life of this paper and so I apologize to all of you who have made helpful comments that remain unacknowledged. If you did make comments that I adopted — from catching typographical or factual errors to suggesting a new resource or topic — and I have failed to recognize you, please remind me! Thanks are offered to my technical mentor and guide Mr. Sudipta Sahana, my co-workers Shrabanti Saha, Aniket Kumar, Sourav Ghosh.

VII. REFERENCES

[1] K. Oyetola Oluwadamilola, A. Okubanjo Ayodeji, O. Osifeko Martins, I. SanusiOlufunmi, O. Abolade Rapheal -"An improved authentication system using hybrid of biometrics and cryptography", Electro-Technology for National Development (NIGERCON), 2017 IEEE 3rd International Conference on, URLhttp://ieeexplore.ieee.org/document/8281915/, Date of Conference: 7-10 Nov. 2017, Date Added to IEEE Xplore: 08 February 2018, ISBN Information: Electronic ISSN: 2377-2697.

[2] Sudipta Singha Roy, Shaikh Akib Shahriyar, and Md. Asaf-Uddowla, Kazi Md. Rokibul Alam, Yasuhiko Morimoto - "A novel encryption model for text messages using delayed chaotic neural network and DNA cryptography", Computer and Information Technology (ICCIT),2017 20th International Conference of Computer and Information Technology (ICCIT).ISBN Information: Electronic ISBN: 978-1-5386-1150-0, USB ISBN: 978-1-5386-1149-4, Print on Demand(PoD) ISBN: 978-1-5386-1151-7.

[3] Hosam F. El-Sofany, Samir A. El-Seoud – "Studying Security of Data in Cloud Computing Through Cryptographic Approach", International Conference on Interactive Collaborative Learning, URL-https://link.springer.com/chapter/10.1007/978-331950340-0_38, Online ISBN978-3-319-50340-0.

[4] Sanket A. Ubhad, NileshChaubey and Shyam P. Dubey. "Advanced ASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id" IJCSMC (2015) Available at http://works.bepress.com/article/8/.

[5] Bobby Jasuja and Abhishek Pandya. Article: Crypto-Compression System: "An Integrated Approach using Stream Cipher Cryptography and Entropy Encoding". International Journal of Computer Applications 116(21):34-41, April 2015.

[6] Deepti Chaudhary, Rashmi Welekar - "Secure Authentication Using Visual Cryptography". International Journal of Computer Science and Applications Vol. 8, No.1, Mar 2015 ISSN: 0974-1011 Proc. Of NCRMC-2014, RCoEM, Nagpur, India as a Special Issue of IJCSA 65.

VIII. AUTHORS

Kaushik Kumar is currently pursuing his Bachelors with specialization in Computer Science and Engineering from JIS College of Engineering, Kalyani. He is currently a Web Developer (Trainee) at National Informatics Centre, Kolkata.

Have pitched himself through various innovative projects & competitions on behalf of CII Lab. Also have recently filed an Indian Patent, journals for his Innovative Projects. Also, have participated and delivered a speech at National and International Technical Submits like NASSCOM, JISTech, Industry Conclave, 2nd Regional Science & Technology Congress, 2017 and extra. His major interest is in Web Development and related technologies.

Sourav Ghosh is currently pursuing B.Tech-CSE from JIS College of Engineering, Kalyani, W.B India. He has completed his 10^{th} and 12^{th}board exams from Birla High School, Kolkata, W.B., India under C.B.S.E in the year 2015 and 2017 respectively.

He finds interest in software development and has acquired knowledge in computer languages like C/C++.

Sudipta Sahana is an assistant professor of a renowned engineering college of West Bengal. For more than 5 years, he has worked in this region. He has passed his M.Tech degree in Software Engineering and B.Tech Degree in Information Technology from West Bengal University of Technology with a great CGPA/DGPA on 2010 and 2012 respectively. He is recently working in Ph.D. in the domain of "Cloud Computing". He is a member of the Computer Science Teachers Association (CSTA), and also a member of International Association of Computer Science and Information Technology (IACSIT).