IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 8, Issue 1, August 2021

IJARSCT
Impact Factor: 5.731

Improve Data Security on Mobile Phone using Encryption Schemes

Divya Solanki[1] and Tosal Bhalodia[2]
P.G. Student, Department of Computer Engineering[1]
Faculty, Department of Computer Engineering[2]
Atmiya University, Rajkot, India

Abstract: *It is a methodology to process and secure data on mobile phone device. It provides the security to mobile user data using Encryption schemes. It is a concept which allows users to secure their personal data on their mobile phones without having to worry about confidentiality even if the mobile is lost. It concentrates on securing data on mobile phones by storing it in an encrypted form. The data is encrypted with using encryption schemes or encryption algorithms and the key which is given by the particular user. If user mobile device is lost then there is no issue of data loss or access by unauthenticated user because the data is in encrypted form. Here different algorithms are implemented for encryption of different type of data. Those algorithms provide more security to data with less time consumption. User can also use these algorithms for data encryption during sharing of data which they want to share with another user. So user can use these encryption algorithms for security of their data. For decryption of data there is a need for key which is given by the user at the time of encryption. This concept will make the data safe on mobile phone and provide better security during data transmission.*

Keywords: Data security, Encryption Scheme, Encryption Algorithms, Mobile Phone Security, Data Encryption, Mobile Encryption

I. Introduction

Now a day's all most every people have mobile phones or android phone. So use of mobile phone is increase day by day and user can store their personal or profession details on their mobile phones. It is necessary to secure data on mobile phones. Day by day, the mobile user are rapidly increased that's why, the chances of mobile losses or data loss on mobile phone and attacks on mobile data are also increased. Data encryption concept deals with providing security to data against malicious usage. If mobile Phone is lost then there is a loss of data also. So data encryption on mobile phone is a concept in which users can store sensitive data on their mobile phone without having to worry about confidentiality even if the mobile is lost. Encryption is used for securing files from thefts. Security is the main purpose of this research and also the Time require for encryption of data or Time complexity of the encryption algorithm should be less. It is also important to take minimum time for encryption of data and for security of data on mobile phones.

Here we are improving existing algorithms for more data security with considering time parameter and implementing different algorithms which are used for encryption of different data. The user's data is encrypted with using encryption algorithm. The user can able to encrypt data such as Text files, Document files, Contact number and Image. Security of data will be provided by encryption/decryption Schemes. Many encryption schemes and encryption algorithms are there for providing security to the data. It is also necessary that the encryption should be done with minimum time complexity. This concept will provide security to data with considering time parameter that minimum time should be taken by algorithm. Algorithms implemented in this research are also used in data sharing to secure data during transmission. So the objective of data encryption on mobile phone is to improve security of the user's data on mobile phone and to minimize Time Complexity for encryption of data.

DOI: 10.48175/568

II. Information Security

2.1 Information Security

Information security means protecting information (data) and information systems from unconstitutional access, use, disclosure, disruption, modification, or destruction. Information security defends information from a wide range of threats, in order to preserve its value to an organization. Information security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure.

2.2 Principles of Information Security

The fundamental principles of security are as follows,

- Confidentiality: The principle of confidentiality specifies that no any unauthorized person can access the user's personal data. Ensuring the meaning of a message is encoded for security and that sensitive information can only be available to authorized users.
- Integrity: Integrity of data is protected when the assurance of accuracy and reliability of information and system is provided, and unauthorized modification is prevented. Only the authorized party is allowed to modify the transmitted information.
- Availability: The Principles of availability states that resources should be available to authorized parties at all times. Availability ensures reliability and timely access to data and resources to authorized individuals.
- Authentication: Authentications mechanisms help establish proof of identities. The authentication process ensures that the origin of a electronic message or document is correctly identified.
- Non-repudiation: There are situations where a user sends a message and later on refuses that he/she had sent that message. Non-repudiation does not allow the sender of a message to refuse the claim of not sending the particular message.
- Access control: The principle of access control determines who should be able to access what.

III. Literature Review

Table 1: Comparison of Literature Survey

Paper	Publication	Complexity	Algorithm	Advantages	Disadvantages
Implementation of Encryption and Decryption Algorithms for Security of Mobile Devices	International Conference on Communication Technology - IEEE (2019)	65%	bit Swapping, XOR operation	Faster in speed, Data Confidentiality, Complexity of the algorithms used is better than the conventional methods.	Take more amount of memory for encryption.
ISCAP: Intelligent and Smart Cryptosystem in Android Phone	IEEE - 2017	2^254.4	Advanced Encryption Standard(AES)	Simple implementation, High security, strong encryption key.	If phone's sensing device is crash than entire data will be loss.
Mobile Self encryption Techniques	International Journal for Research in Engineering Application &	2^198	RC4 Stream cipher	Variable length key stream is used for encryption so it makes brute	Consumes more battery power.

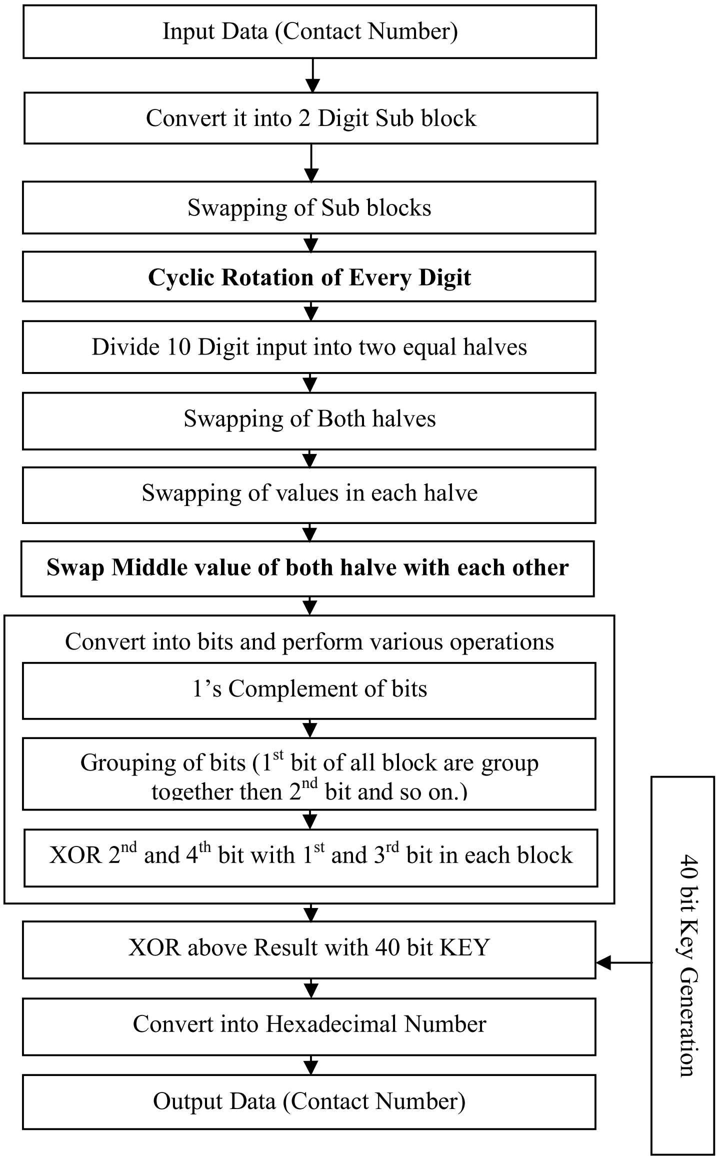
	Management (2018)			force attacks infeasible, Provide high efficiency.	
Data Security using Authenticated Encryption and Decryption Algorithm for Android Phones	International Conference on Computing, Communication and Automation (2017)	2^254.4	Advanced Encryption Standard(AES)	It takes less amount of memory, High computational complexity.	Time Require for encryption increases with increase in the size of the file.
Mobile Self Encryption	International Journal of Advanced Research in Computer and Communication Engineering (2018)	2^251	Stream cipher	Data Confidentiality, Data remains Safe during loss of mobile device	slower in speed, time consuming
Mobile Self Encryption System	International Journal of Innovative Research in Science Engineering and Technology (2019)	2^126.1	Advanced Encryption Standard (AES)	Data Availability, If mobile lost key than OTP will send on another mobile number.	Take more time to encrypt data
Design and Implementation of Text Cryptography for Multi-Languages and Resolving Type Cast Issues	International Journal of Research in Engineering, Science and Management (2019)	O(n^2)	Block Cipher	Adequate Security with Typecast Resolved, Issues of length and language constraint for any cryptographic algorithms has been revoked.	Slower in speed.

IV. Methodology

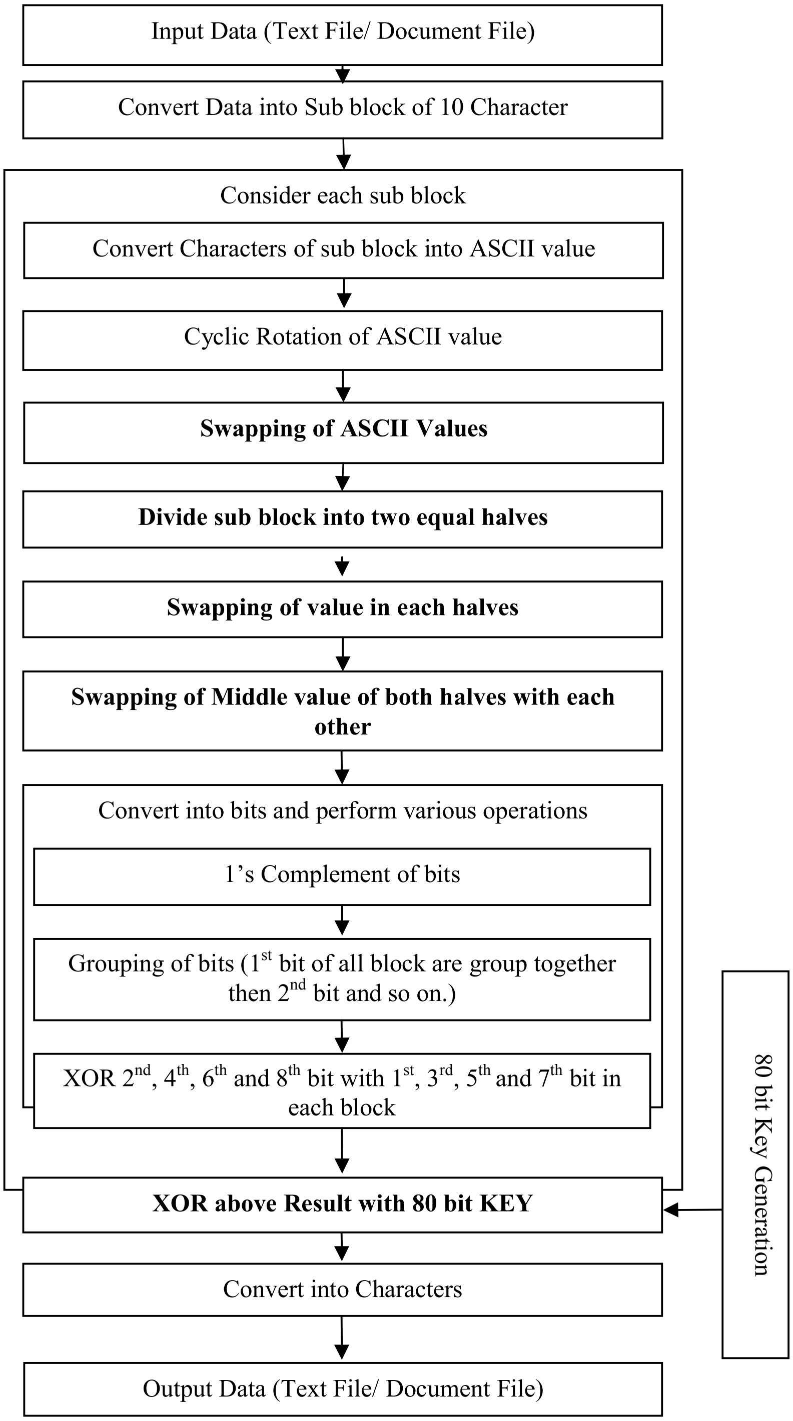
The proposed algorithms are used to encrypt data such as contact number, text files, document files, images. These algorithms less time complexity as compare to another encryption algorithms for encryption of data. Fig. 1 is about encryption of contact number and then Fig. 2 is about encryption of text data and document data files.

DOI: 10.48175/568

4.1 Algorithm for Contact Number Encryption


Input Data (Contact Number)
Convert it into 2 Digit Sub block
Swapping of Sub blocks
Cyclic Rotation of Every Digit
Divide 10 Digit input into two equal halves
Swapping of Both halves
Swapping of values in each halve
Swap Middle value of both halve with each other
Convert into bits and perform various operations
1's Complement of bits
Grouping of bits (1st bit of all block are group together then 2nd bit and so on.)
XOR 2nd and 4th bit with 1st and 3rd bit in each block
XOR above Result with 40 bit KEY
Convert into Hexadecimal Number
Output Data (Contact Number)
40 bit Key Generation

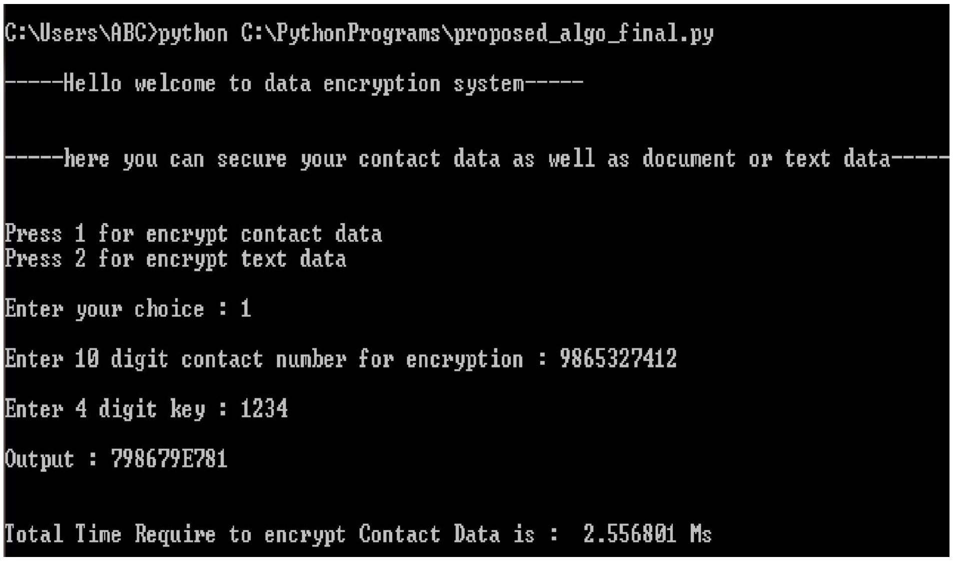
4.2 Algorithm for Text File/Document File Encryption


Input Data (Text File/ Document File)
Convert Data into Sub block of 10 Character
Consider each sub block
Convert Characters of sub block into ASCII value
Cyclic Rotation of ASCII value
Swapping of ASCII Values
Divide sub block into two equal halves
Swapping of value in each halves
Swapping of Middle value of both halves with each other
Convert into bits and perform various operations
1's Complement of bits
Grouping of bits (1st bit of all block are group together then 2nd bit and so on.)
XOR 2nd, 4th, 6th and 8th bit with 1st, 3rd, 5th and 7th bit in each block
XOR above Result with 80 bit KEY
80 bit Key Generation
Convert into Characters
Output Data (Text File/ Document File)

Here we are improving existing algorithms for encryption of different types of data. With adding more steps in encryption algorithm the security is increased. Also the time parameter is in consideration. In proposed encryption algorithms we are added more steps which are in bold. So with less time complexity these algorithms provide more security to data such as contact number, text file or document file. For decryption we have to perform these algorithms in reverse manner with particular KEY.

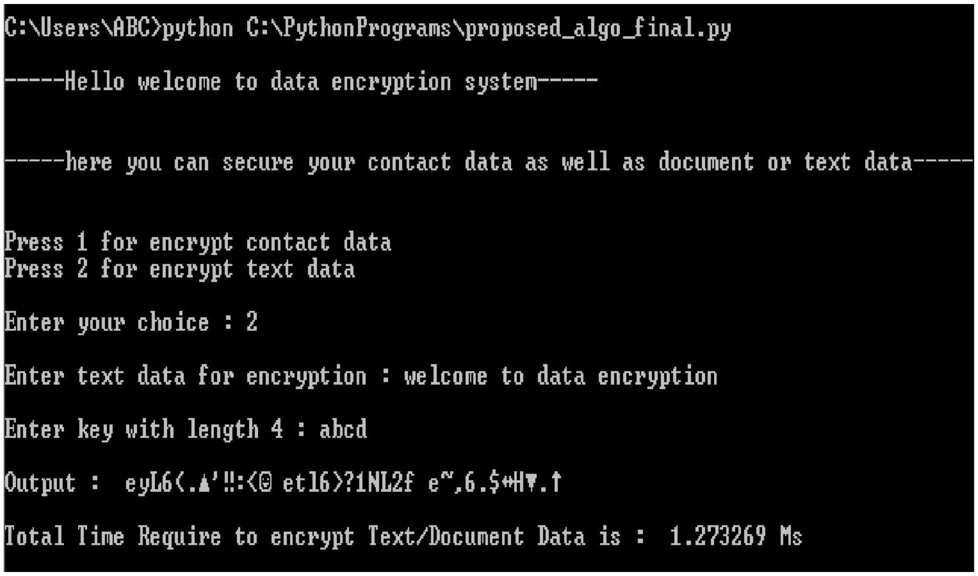
V. Result

Proposed algorithms are developed in python programming language. The results of proposed algorithms are shown in Fig.1 and Fig.2. User can give the data which they want to encrypt and also the key to encrypt data is given by user with the specified key length. The output of contact number encryption is shown in Fig.1 and Fig.2 shows the output of Text/Document data encryption. The output gives encrypted data with time measurement in milliseconds.



```
C:\Users\ABC>python C:\PythonPrograms\proposed_algo_final.py

-----Hello welcome to data encryption system-----


-----here you can secure your contact data as well as document or text data-----


Press 1 for encrypt contact data
Press 2 for encrypt text data

Enter your choice : 1

Enter 10 digit contact number for encryption : 9865327412

Enter 4 digit key : 1234

Output : 798679E781


Total Time Require to encrypt Contact Data is :  2.556801 Ms
```

Figure 1: Algorithm Output for Contact Number Encryption



```
C:\Users\ABC>python C:\PythonPrograms\proposed_algo_final.py

-----Hello welcome to data encryption system-----


-----here you can secure your contact data as well as document or text data-----


Press 1 for encrypt contact data
Press 2 for encrypt text data

Enter your choice : 2

Enter text data for encryption : welcome to data encryption

Enter key with length 4 : abcd

Output :  eyL6(.▲'‼:<☻ et16>?1NL2f e~,6.$↔H▼.↑

Total Time Require to encrypt Text/Document Data is :  1.273269 Ms
```

Figure 2: Algorithm Output for Text/Document Data Encryption

As shown in below Fig.3 Proposed algorithms provide better security then existing algorithms and provide less time complexity as compare to existing algorithms.

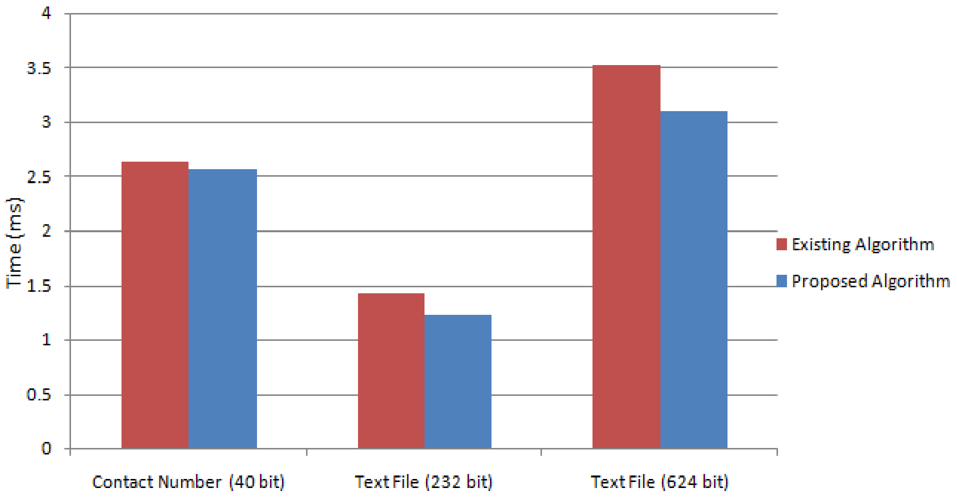


Figure 2: Comparison of Existing and Proposed Algorithms with considering Time Parameter

Here encryption is done in such a way that minimum time should be taken by the encryption algorithm to encrypt particular data. Analysis graph for encrypting data with different data size is given below in Fig.4:

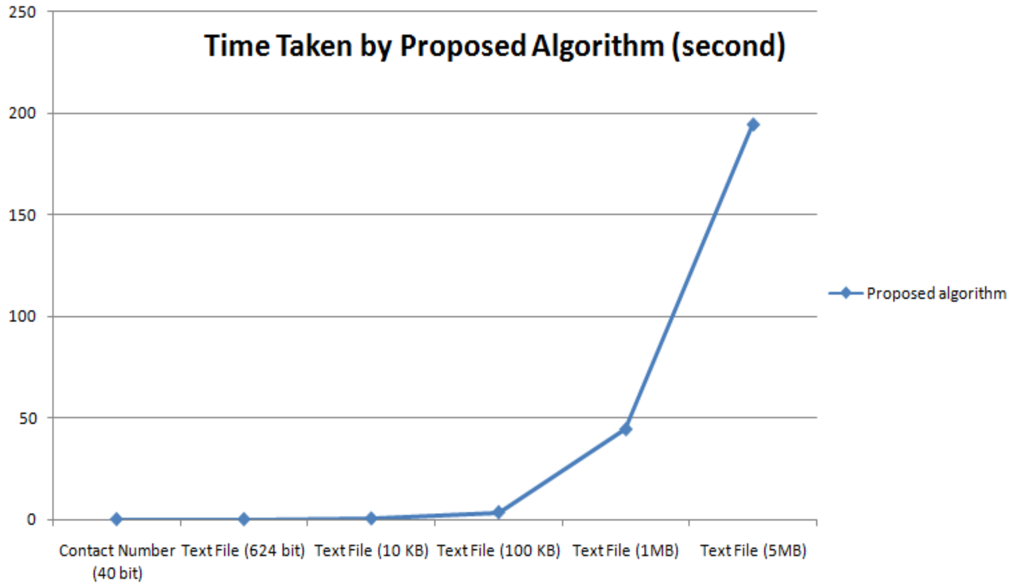


Figure 4: Time Analysis of Proposed Encryption Algorithm based on Data Size

VI. Conclusion

In this, we improve some existing algorithms and proposed algorithms for encryption of data such as contact number, text file or document file on mobile phone. These algorithms are used to encrypt data on mobile device. In existing system the complexity of existing system algorithm is checked and is found to be better than the conventional method. We are improving existing algorithm and providing more security to data with less time complexity. So from this work it is conclude that using these proposed encryption algorithms data security is more and time complexity is less as compare to existing encryption algorithms.

DOI: 10.48175/568

VII. Future Work

We are work on improving data security on mobile device and it is very important to secure data on mobile device. In future encryption of image, audio and video is also possible with using encryption scheme. The complexity of algorithm can be further improved.

Acknowledgment

I am thankful to all those who directly or indirectly help me in accomplishing my task. Last, but not the least I am grateful thank my institute, Atmiya University for giving me this opportunity to work in the great environment.

References

[1]. B V Varun, Abhishek M V, Akshay Chanabasappa Gangadhar, Purushotham U "Implementation of Encryption and Decryption Algorithms for Security of Mobile Devices" International Conference on Communication Technology - IEEE (2019)

[2]. Brindha S, Deepalakshmi D, Dhivya T, Arul U, Sivakumar S, Dr Nattar Kannan K "ISCAP: Intelligent and Smart Cryptosystem in Android Phone" IEEE - 2017

[3]. Ms. N.S.Gurdhalkar, Ms. S.S.Gurdhalkar, Ms.P.D.Belhekar, Ms.J.S.Mane "Mobile Self Encryption " International Journal of Advanced Research in Computer and Communication Engineering (2018)

[4]. Viraj Jagtap, Tushar Ingale, Vaibhav Walke, Sahil Satpute, A. S.Khandagale "Mobile Self Encryption System" International Journal of Innovative Research in Science Engineering and Technology – IEEE (2019)

[5]. Mitesh Parmar, Summedh Kharat, Nilesh Palve, Chetan deokate, Prof. Yogesh shahare "Mobile Self Encryption Techniques" International Journal for Research in Engineering Application & Management (2018)

[6]. Tarun Kumar Mishra, Nimish Arvind "Design and Implementation of Text Cryptography for Multi-Languages and Resolving Type Cast Issues" International Journal of Research in Engineering, Science and Management (2019)

[7]. Kalyani P. Karule , Neha V. Nagrale "Comparative Analysis of Encryption Algorithms for Various Types of Data Files for Data Security" International Journal of Scientific Engineering and Applied Science (2016)

[8]. Prosper Kandabongee Yeng, Joseph KobinaPanford, James Ben Hayfron-Acquah, Frimpong Twum "An Efficient Symmetric Cipher Algorithm for Data Encryption" International Research Journal of Engineering and Technology (2016)

[9]. Abhishek Vichare Tania Jose, Jagruti Tiwari, Uma Yadav "Data Security using Authenticated Encryption and Decryption Algorithm for Android Phones" International Conference on Computing, Communication and Automation - IEEE (2017)

[10]. Pushpendra Verma, Dr. Jayant Shekhar, Preety, Amit Asthana "A Survey for Performance Analysis Various Cryptography Techniques Digital Contents" International Journal of Computer Science and Mobile Computing (2015)

[11]. Omar G. Abood, Shawkat K. Guirgui "A Survey on Cryptography Algorithms" International Journal of Scientific and Research Publications (2018)

[12]. Yogesh P. Surwade* Dr. Hitendra J. Patil "INFORMATION SECURITY" Knowledge Librarian: An International Peer Reviewed Bilingual E-Journal of Library and Information Science Special Issue, January 2019

DOI: 10.48175/568