THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Hybrid Cryptographic Algorithm For Ensuring Cross Platform Mobile Security

Kumar Vishal and Dr. Ajay Shriram Kushwaha

School of Computer Applications,Lovely Professional University,

Jalandhar, India

Abstract: -

To design our own cross mobile platform security architecture using cryptographic algorithm, which generate a new way to secure data, which is transmitting through different layers in cross mobile platforms. We already have several cryptographic algorithms to secure services such as Integrity, Confidentiality and Authentication. But our approach is to find viable solution in cross-mobile platform using hybrid cryptographic approach, which is unique idea where researchers have not dig deep into it.

According to hybrid cryptographic algorithm data has been tested with small size and large size also. If data is not a text file if it is image file then size will be large in this case, algorithm performance has to be discussed.

In security concern how data will be more secure that not has been discussed by using implementation. Here we are discussing about data communication between the cloud and mobile phone. But data communication can be done not only from the cloud it can through local server or remote server or data communication can be done through different layers also.

In our modal mobile platform security has been categorized in four parts: during deployment of software, during installation of applications, operation performed during run time and managing platform in regular interval. As security concern, every part is important. When data or information's are communicating between these part then cryptographic algorithms can be used in each part separately. Data is communicating in mobile device not only through the cloud it can be communicating through local server or remote server also. We know our data is very sensitive data (like address book, current location, emails or even health information) and many applications from different sources we are transmitting our data.

Keywords: Xamarin.Forms, Cryptography, cross mobile platforms, AES, DES, Triple DES and RSA algorithm

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

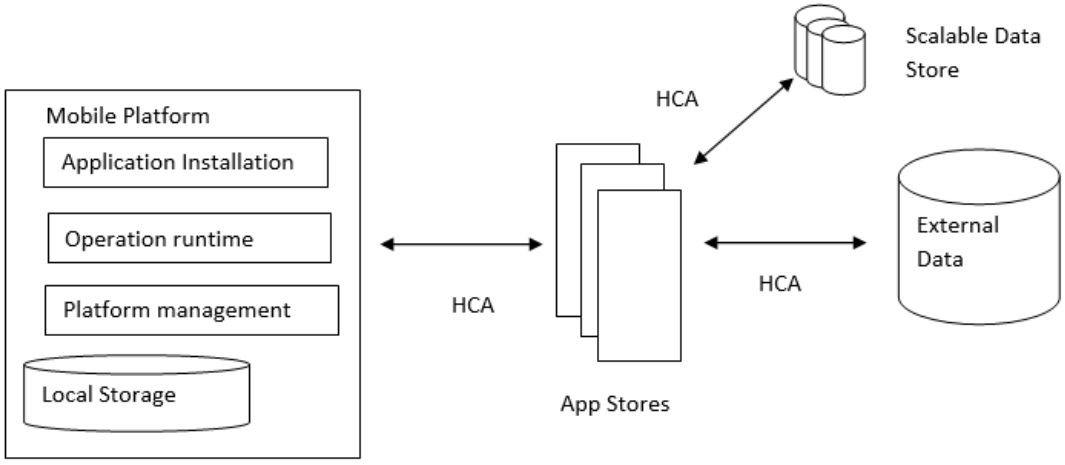
I.Introduction:

Basically, mobile platform security has been categorized in four parts: deployment of software, installation of applications, operation performed during run time and managing platform in regular interval. As security concern, every part is important. When data or information's are communicating between these parts then hybrid cryptographic algorithms can be used in each part separately. For this, we propose a novel architectural approach [1].

Xamarin.Forms is a framework which helps to create cross platform mobile application. Here cross platform means we can deploy our code in any mobile device. Firstly, we have to create a user interface with the help of XAML controls and by using C-sharp which is code behind language in Xamarin.Forms we have to perform encryption and decryption. There are so many frameworks which can be use to create cross platform application but C-sharp programming is very easy to implement because of the coding pattern and concept is very similar to other programming language like C++ or Java [2].

II. Research methodology:

To design our own cross mobile platform security architecture using cryptographic algorithm, which generate a new way to secure data, which is transmitting through different layers in cross mobile platforms. We already have several cryptographic algorithms to secure services such as Integrity, Confidentiality and Authentication. But our approach is to find viable solution in cross-mobile platform using hybrid cryptographic approach, which is unique idea.



HCA (hybrid cryptographic algorithm)

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Fig: Research Methodology

For the better understanding of cryptographic algorithms, a Xamarin.Forms App has been developed which take some amount of data and will be encrypted and decrypted. This effort has been made to cover different layers of security architecture for securing cross mobile platform. To design our own cross mobile platform security architecture using cryptographic algorithm, which generate a new way to secure data, which is transmitting through different layers in cross mobile platforms [3].

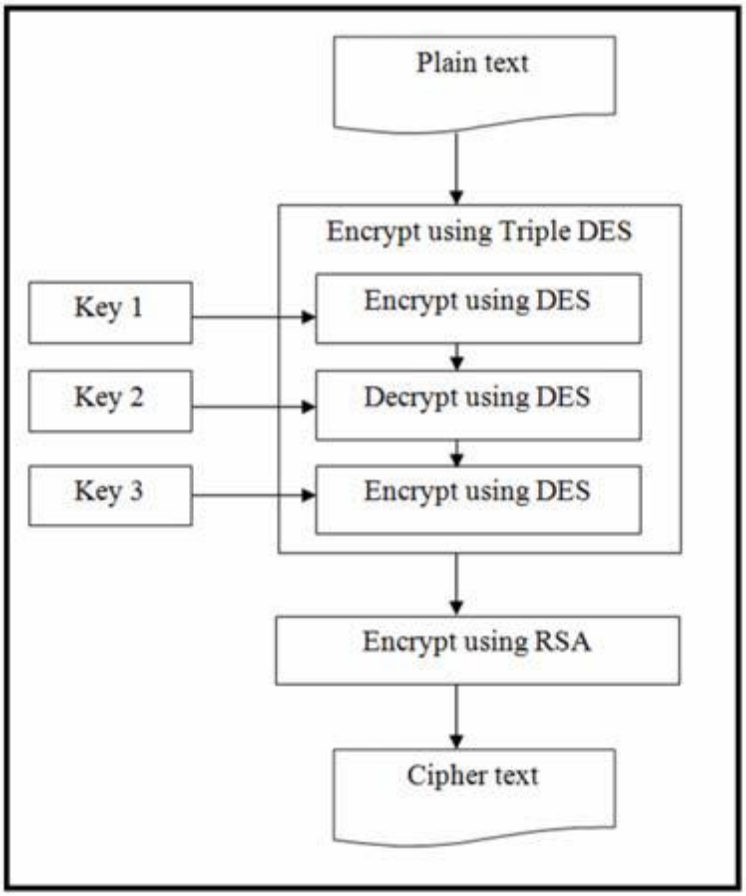
III. Comparative analysis of existing cryptographic algorithm:

Hybrid encryption algorithm using (the RSA encryption algorithm and Triple DES encryption algorithm) [4]:

Algorithm for encryption:

1. Take plain text from a file.
2. Now encrypt using triple DESkey1
3. Now decrypt using triple DESkey2
4. Now encrypt usingtriple DES key3
5. Now encrypt using RSA and result store
6. Now result is final cipher

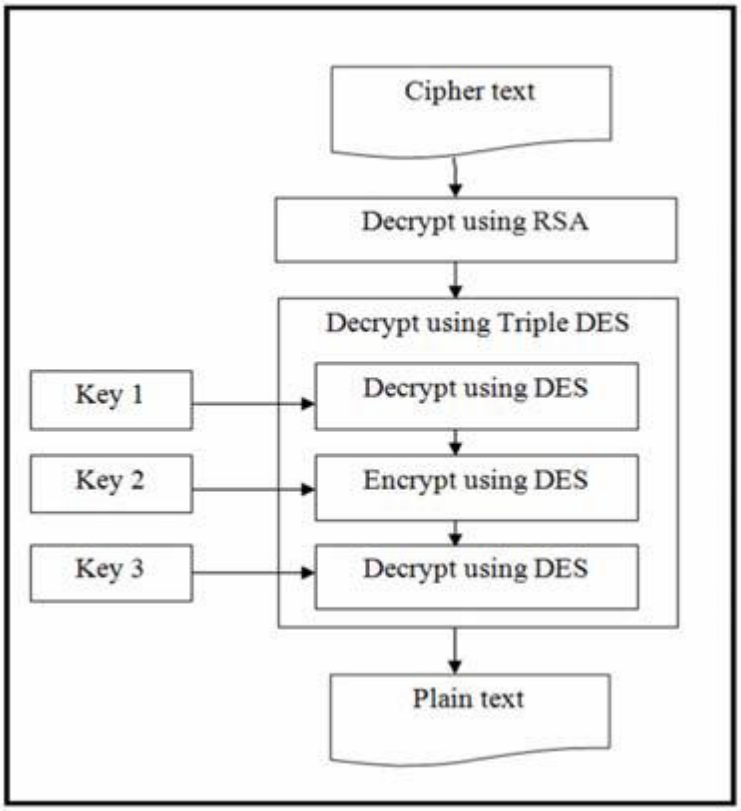
ISSN: 0971-1260
Vol-22-Issue-17-September-2019



Algorithm for decryption:

1. Read cipher text
2. Now decrypt using RSA
3. Now decrypt using triple DES key3
4. Now decrypt using triple DES key2
5. Now decrypt using triple DES key1
6. Result is the final file

ISSN: 0971-1260
Vol-22-Issue-17-September-2019



IV. Experimental and Result

With the help of Xamarin.Forms and C# code which is code behind language has to be used to perform this task. The user will choose the algorithm and press "button" to begin the encryption and decryption process.

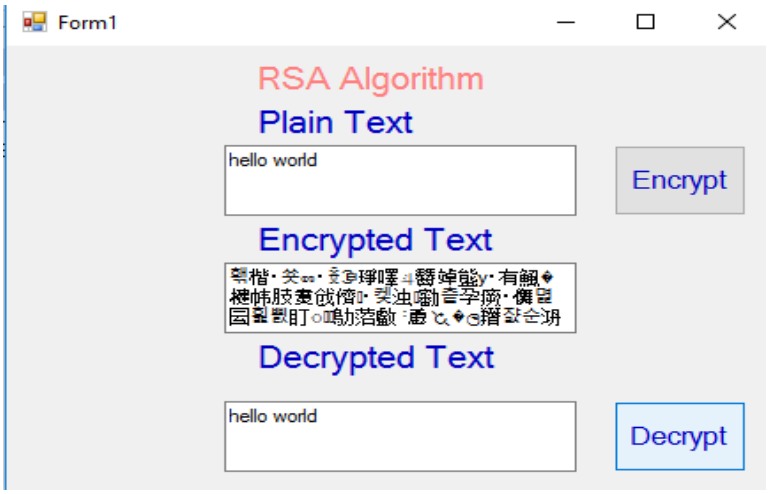
The parameter has been identified. Identified parameters are given below:

•Throughput

•Encryption/Decryption Time.

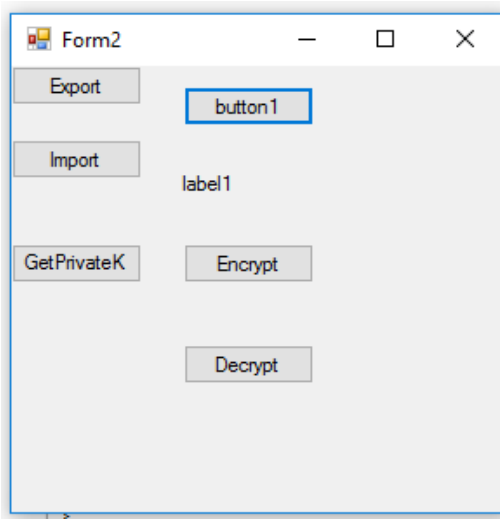
•Jitter.

ISSN: 0971-1260
Vol-22-Issue-17-September-2019



No. of characters: 11

	File Size	Time consumed in sec
RSA Algorithm	11 characters	0.6 sec
RSA Algorithm	23 Characters	0.18 sec



	File Size	Time consumed in sec
RSA Algorithm	200 Bytes	0.80 sec
RSA Algorithm	400 Bytes	0.90 sec

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Algorithm	Memory used (KB)	Avalanche effect (according to file size)	Average entropy per byte of encryption
RSA	31.5	25%	3.0958
3DES	20.7	50%	2.9477

# chars	Encryption time (ms)	Decryption time (ms)	Sending time (ms)
500	53	100	4299
1000	96	130	4172
1500	139	121	4636
2000	212	135	4934
2500	289	145	4301
3000	333	163	4338

# chats	Average encryption time (ms)	Average decryption time (ms)	Accuracy (%)
25	689.2	701.8	100
50	698.44	716.66	100
75	695.6133	725.7867	100
100	678.68	732.18	100

V. CONCLUSION:

To design our own cross mobile platform security architecture using cryptographic algorithm, which generate a new way to secure data, which is transmitting through different layers in cross mobile platforms. We already have several cryptographic algorithms to secure services such as Integrity, Confidentiality and Authentication. But our approach is to find viable solution in cross-mobile platform using hybrid cryptographic approach, which is unique idea where researchers have not dig deep into it.

References:

[1]Prabir Bhattacharya,Li Yang,Minzhe Guo, Kai Qian, Ming Yang,"Learning Mobile Security with Labware",ieeexplore,Volume: 12,Issue: 1,Year: 2014

[2]N.Asokan,LucasDavi,Alexandra Dmitrienko,Stephan Heuser,"Mobile Platform Security",Morgan and Claypool eBooks,Year: 2013

[3]Ziqiang Zhou,Changhua Sun,Jiazhong Lu,fengmaoLv,"Research and Implementation of Mobile Application Security Detection Combining Static and Dynamic",2018 10th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA),Pages:243-247,Year: 2018

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

[4]Walter Squires,Paolina Centonze,"Cross-Platform Access-Rights Analysis of Mobile Applications", 2016 IEEE/ACM International Conference on Mobile Software Engineering and Systems (MOBILESoft),Pages:295-296,Year:2016