Mobile Data Transfer security through a cryptographic approach

[1]Manikandan,[2]Kumar chowdary, [3]M.Manideep, [4]T.N.Krishnakanth

[1,]Professor, Department of Computer science and Engineering, Vellore Institute of Technology, Vellore - 632014, Tamil Nadu, India
[2, 3, 4] Department of Computer Science and Engineering, Vellore Institute of Technology, Vellore - 632014, Tamil Nadu, India

---***---

Abstract - *As the mobile phones being numerically ascending on a day to day life it's being proportionally effecting other hand (i.e., mobile phone security) utmost cases the important credentials are being stored in their respective mobiles. And use them on daily basis for their business environment and also private life. On the raising technology their found many changes in information technology which is adding up to it commercially which pushed a new risk, on this point the smart phone consists of much sensitive data which should be safeguarded. This paper tells how to protect your mobile or smart phone in cryptographic approach.*

Key Words: cryptography, mobile transfer, Security, Technology, sensitive data

1. INTRODUCTION

Rapid increase in mobile parallels exposing various threats on ABI research the raise in percentage of unique threat is 261% but here we protect our mobiles with password, picture password , pin etc., all these passcode system will be visible to others while you are unlocking it and on the other hand their comes the bio -metric way fingerprint , eye scanner , heart beat scanner, face recognition etc. which is appreciably secured but at some emergency case the device may not be in a position to handle while it may not be possible for access which shows its limitation so in this paper the cryptographic way of securing information is proceeded which brings algorithms into picture to makes the mobile more strong against to get compromise its security on a special note this paper mainly focus on hybrid process through which the data is being secured not only at the storage point but also while pushing the data or at the time ease of access between mobile to mobile or mobile to cloud.

2. METHODOLOGY

Cryptographic approach is being classified in to three types asymmetric cryptosystem ,symmetric cryptosystem and digital signatures here in symmetric cryptosystem the sender and receiver gets the same key which on the aspect of confidentiality and avoid privacy, asymmetric cryptosystem possess different keys one for encryption and the other for decryption which is mainly works for key exchange and authentication and digital fingerprint will encrypt the data irreversibly and pushes for data integrity . Encryption is the new technology which protects through disturbing the data and acts unique for their respective key sizes and even stronger for specific from the another adjacent here involves many algorithms like triple DES (data encryption standards), RSA, blow fish, two fish, AES (advanced encryption standard), MD5, SHA1, ECC which on classifying to modern cryptography functions SHA1, MD5 under Digital signature. DES and AES under symmetric cryptosystem. RSA, ECC under asymmetric cryptosystem. Here considering the transfers in between cloud encryption will be the most preferred way to secure. It divides the clients in to public (open environment access for trusted clients) and private (confidential data usually carried out in encrypted form for avoiding piracy and to self-safeguard).

3. PROPOSED WORK

Here if only encrypted security may not be sufficient on a hack-eye it can be easily decrypted to compromise the security and hence here to follow a hybrid approach and it is a triple tier proposal which runs digital fingerprint as the first tier it doesn't involve any key on a hash function then the second tier will encrypt the encrypted data again and consider to be key (k1) and finally further encryption preceded through RSA/ESS algorithm as per their turnover time and necessity. All the Data encrypted will be stored in a phone memory the series will be applied for both the sides to maximize the security strength.

4. IMPLEMENTATION

4.1 HYBRID APPROACH

Here on implementing the hybrid approach we have both the keys of asymmetry and symmetry are ordered. On encryption the data goes more secured in the environment cloud as well as mobile.

4.2 TRIPLE DES(DATA ENCRYPTION STANDARDS)

Basically it's a symmetric key cipher applies DES to each data block three times and its key length is 168bits.

4.3 RSA ALGORITHM

It involves 2 keys in to the scripting, which has both private and public key, here public key used for encrypting the messages (can be known to anyone) and private key used to decrypt them (confidential), this is also called public key cryptography

4.4 BLOW FISH ALGORITHM

It is a fast free algorithm for the existing encryption, which drops in replacement of other algorithms of DES, the cipher size varies from 32 to 448 bits respectively.

4.5 TWO FISH ALGORITHM

It is optimized for 32-bit CPU, which has its block size as 128bit and ranging it from 128 to 256 bits.

4.6 AES(ADVANCEDENCRYPTION STANDARDS)

AES has round key block, and its block size is 128 bits, each byte of the bit is combined with block using bitwise XOR.

4.7 MD5 ALGORITHM

An arbitrary length input produces 128-bit long message in the hash form.

4.8 SHA1 ALGORITHM

It is a 160 bit MD5 algorithm, which is a part of digital signature algorithm.

4.9 ECC ALGORITHM

This is a public key approach which requires smaller keys comparatively, this is applicable to pseudo-random generators.

The architecture of the implementation depends upon the alignment of the algorithms upon mobile device environment. Considering the hybrid approach this paper would propose MD5+ECC+AES and MD5+RSA+AES, this application used to encrypt and decrypt the data, is in the point of view of indulging symmetric ,asymmetric and digital signature hence here consider some data about four samples considering their respective sizes, encrypting the data with these above mentioned algorithms in the mobile devices, upon making a instance server and a dynamic webpage, pushing the encryptions on server based on their input sizes separately and finally compare results.

5. RESULTS

5.1 TURN OVERTIME

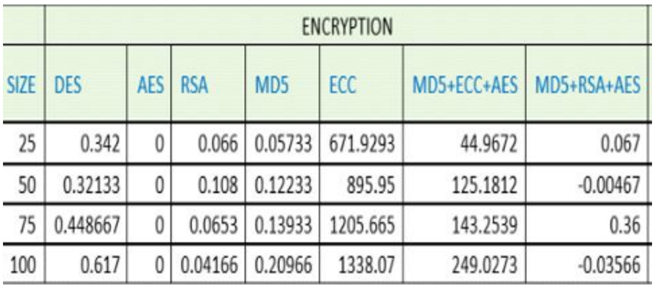
This analysis of time indicates the total time taken to process a request. Which is the algorithm path directed to get from one environment to another the time elapsed in this period is consider to be the turn overtime.

5.2 MEAN PROCESSING TIME

It is the difference in between encryption starting and ending timing. And the time is directly proportional to the size of the data.

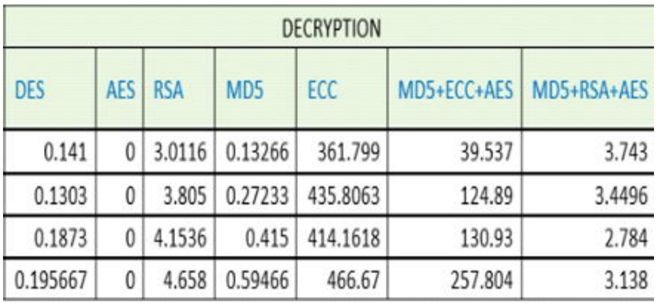
5.3 THROUGHPUT

It is the amount of data passing through the encryption and changes occur on changing it size.



	ENCRYPTION						
SIZE	DES	AES	RSA	MD5	ECC	MD5+ECC+AES	MD5+RSA+AES
25	0.342	0	0.066	0.05733	671.9293	44.9672	0.067
50	0.32133	0	0.108	0.12233	895.95	125.1812	-0.00467
75	0.448667	0	0.0653	0.13933	1205.665	143.2539	0.36
100	0.617	0	0.04166	0.20966	1338.07	249.0273	-0.03566

Fig-1: Time elapsed between cloud and mobile in encryption



DECRYPTION						
DES	AES	RSA	MD5	ECC	MD5+ECC+AES	MD5+RSA+AES
0.141	0	3.0116	0.13266	361.799	39.537	3.743
0.1303	0	3.805	0.27233	435.8063	124.89	3.4496
0.1873	0	4.1536	0.415	414.1618	130.93	2.784
0.195667	0	4.658	0.59466	466.67	257.804	3.138

Fig-2: Time elapsed between cloud and mobile in decryption

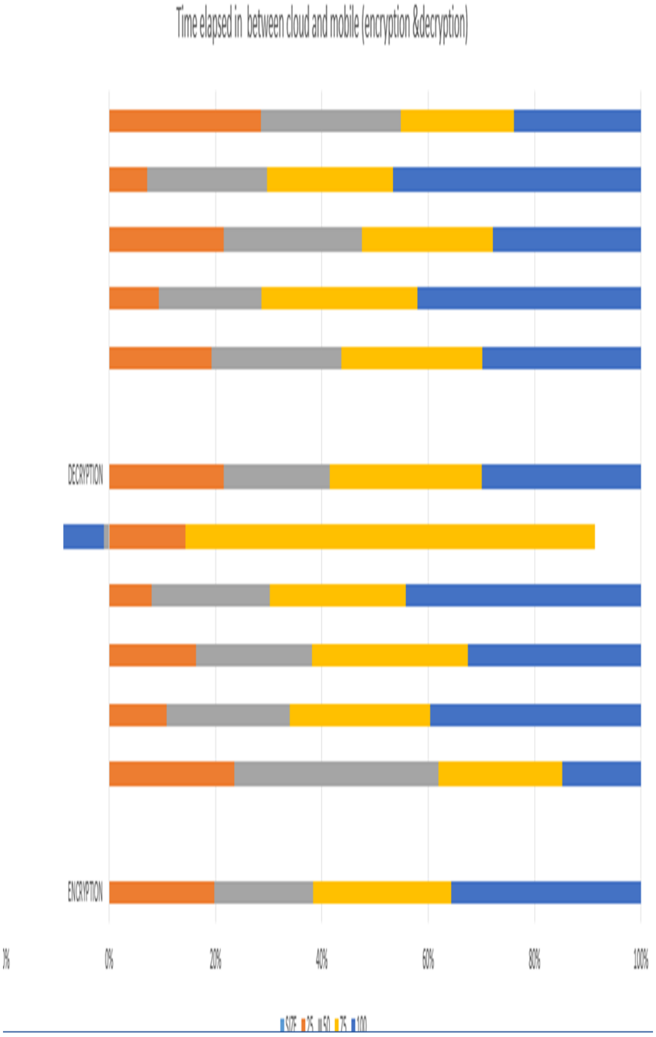
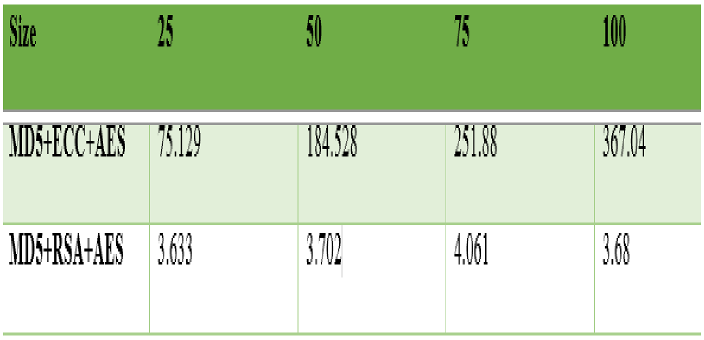


Fig-3: Time elapsed between encryption and decryption



Size	25	50	75	100
MD5+ECC+AES	75.129	184.528	251.88	367.04
MD5+RSA+AES	3.633	3.702	4.061	3.68

Fig-4: Throughput table

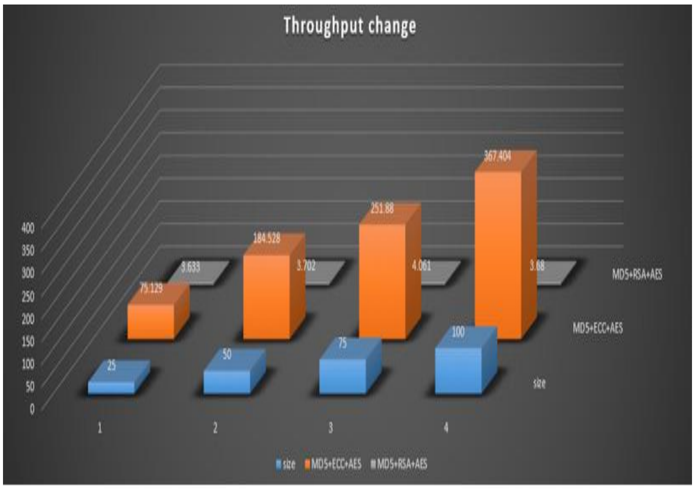
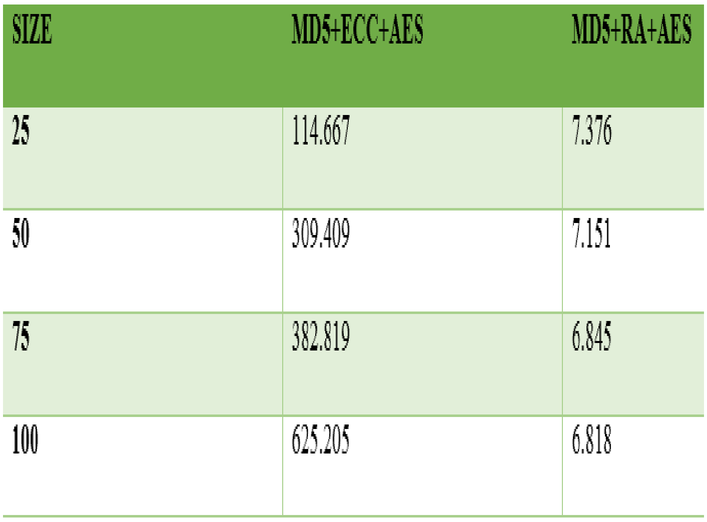


Fig-5: Throughput Graph



SIZE	MD5+ECC+AES	MD5+RA+AES
25	114.667	7.376
50	309.409	7.151
75	382.819	6.845
100	625.205	6.818

Fig-6: Turn over time from mobile to mobile table

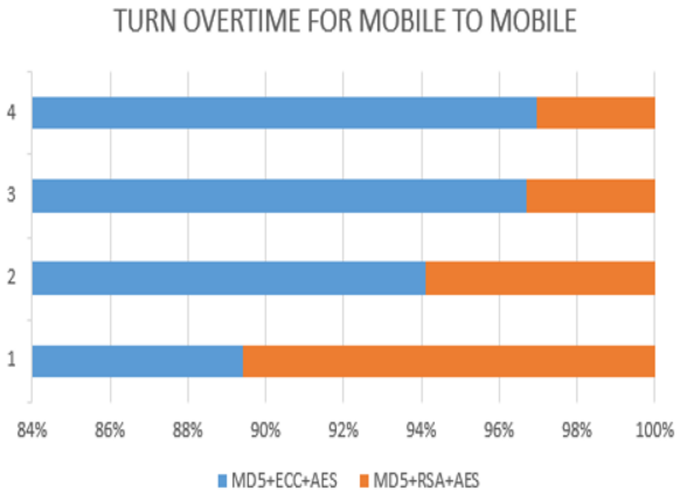
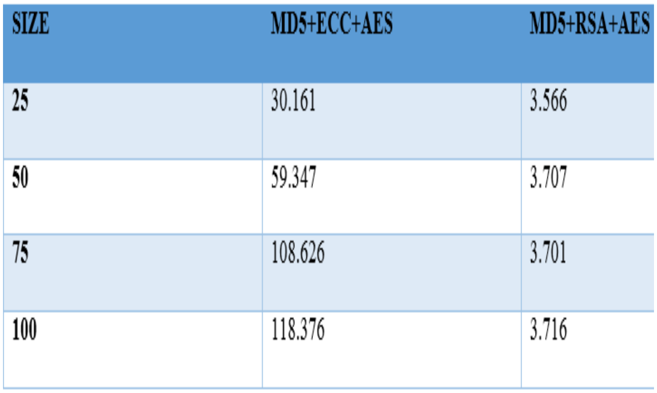


Fig-7: Turn over time from mobile to mobile



SIZE	MD5+ECC+AES	MD5+RSA+AES
25	30.161	3.566
50	59.347	3.707
75	108.626	3.701
100	118.376	3.716

Fig-8: Turn over time from cloud to mobile table

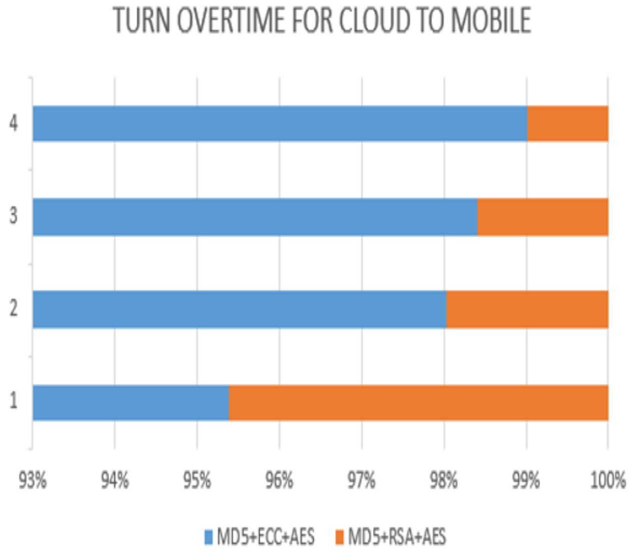
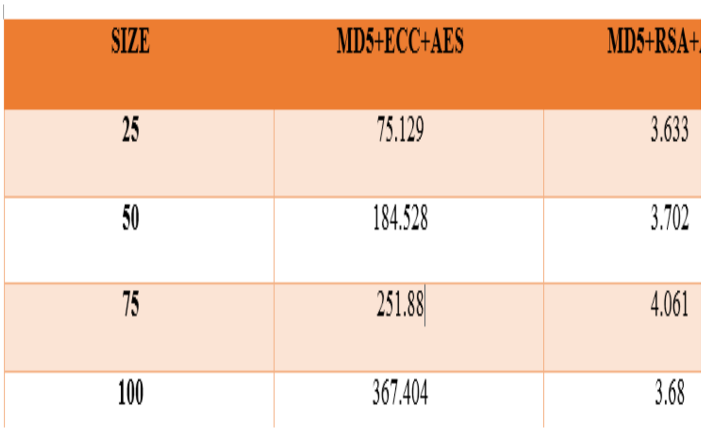


Fig-9: Turn over time for cloud to mobile



SIZE	MD5+ECC+AES	MD5+RSA+
25	75.129	3.633
50	184.528	3.702
75	251.88	4.061
100	367.404	3.68

Fig-10: Turn over time from mobile to cloud table

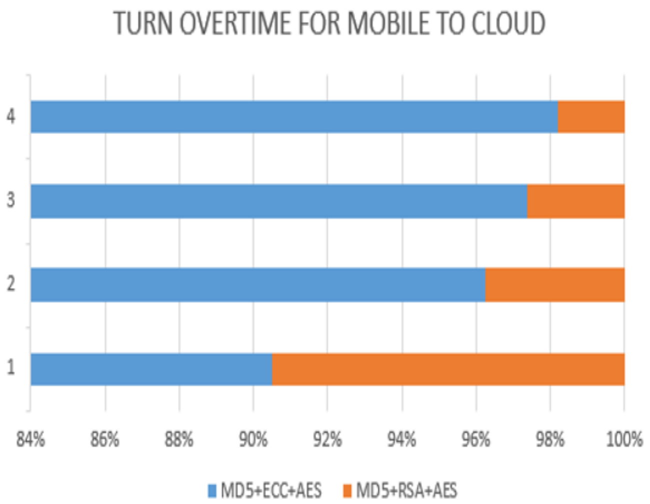


Fig -11: Turn over time for mobile to cloud

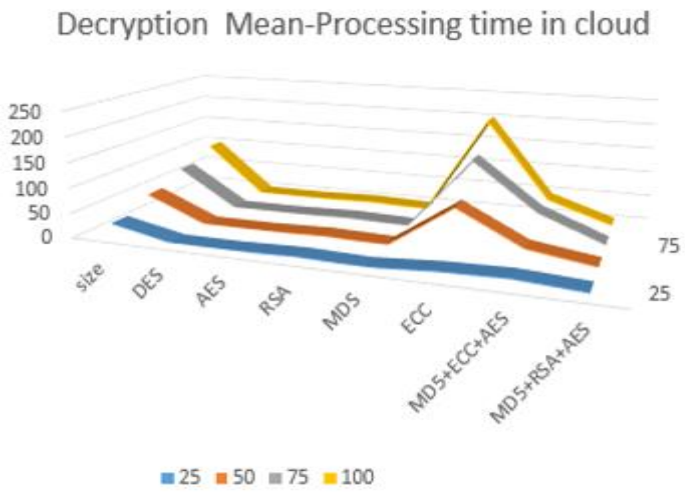


Fig-12: Decryption mean-processing time in cloud

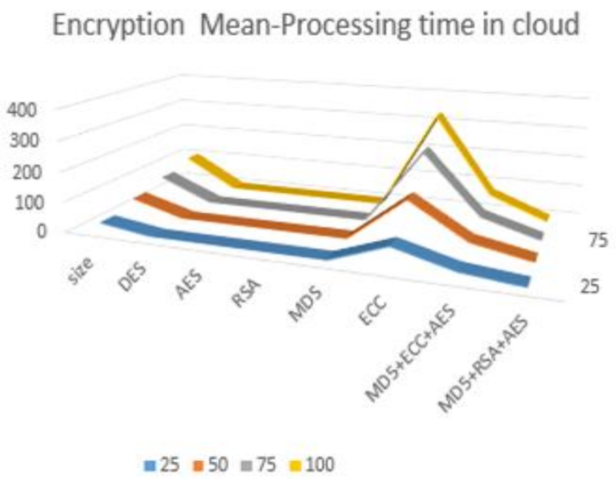


Fig-13: Encryption mean-processing time in cloud

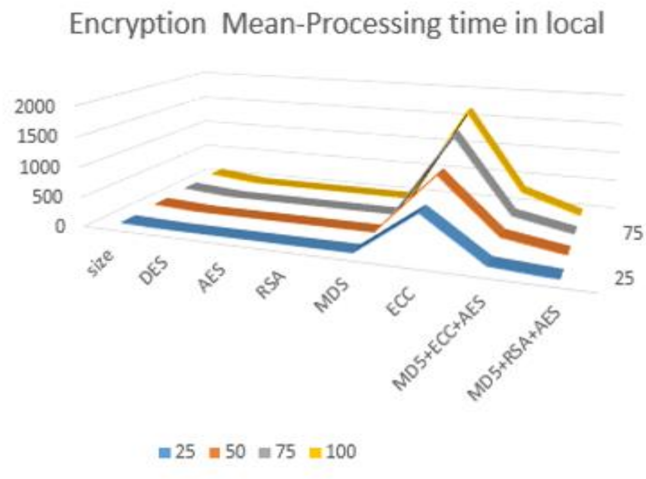


Fig-14: Encryption mean-processing time in local

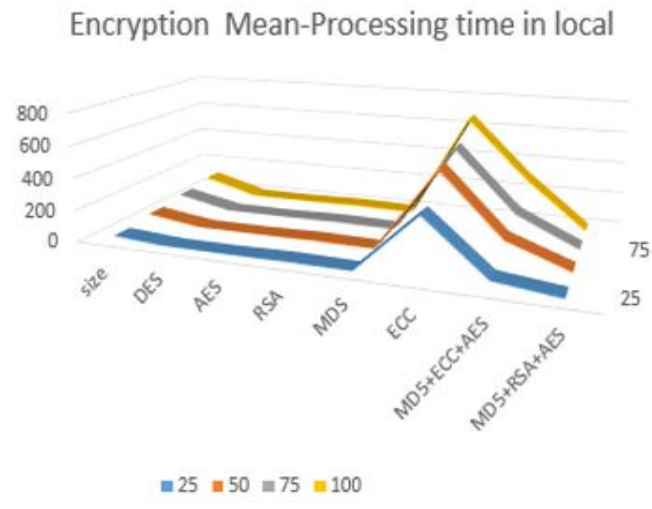


Fig-15: Encryption mean-processing time in cloud

6. CONCLUSION AND FUTURE WORK

As the evolved new technology cryptographic algorithms can perform even more stronger than before considering that this is proposed in multi system environment (mobile & cloud) and cryptography proposed on their access (mobile to mobile) & (mobile to cloud). This proposed system is strong enough but for the rapidly changing technology double digital signature algorithms may provide even more strength to the cryptography hence it is planned for future work especially in including of SHA1 as the second digital print.

7. REFERENCES

[1] Display Solution for mobile cloud computing simeons P., De Turck F.

[2] Comparative Analysis of encryption algorithms for Data Communications by Shashi mehrotra.

[3] Privacy Manager for Cloud Computing by Zhang Q, Cheng L, Boutaba R.

[4] Security Framework for Cloud Computing Environment by Ayesha Malik, Muhammad Mohsin NazirA.

[5] Privacy Manager for Cloud Computing by Zhang Q, Cheng L, Boutaba R.

[6] SECURITY IN CLOUD COMPUTING by P. Syam Kumar, R. Subramanian and D. Thamizh Selvam.

[7] ieeexplore.ieee.org/document/7148427/

[8] https://en.wikipedia.org/wiki/mobilecomputing

[9] https://en.wikipedia.org/wiki/Cryptography

[10] https://en.wikipedia.org/wiki/encryption

[11] Advances and Applications in Mobile Computing.

[12] www.sciencedirect.com/science/article/pii/S1877050915005001

[13] https://www2.clarku.edu/offices/its/security/encryption.cfm.