Enhancing PIN distribution Techniques by using Amalgam Encryption in M-commerce

K.Shanmugam, Dr.B.Vanathi, K.Ganesan

Abstract — In last few years, Mobile commerce had seen extreme growth. But to be focused the lot of privacy, security and integrity challenges. This paper proposes, to send the user Pin number and payment details in secure way. Pin number is encrypted by Amalgam encryption. Amalgam encryption means, Encrypt the pin number by using combination of Triple data Encryption standard (3-DES) and RC4 algorithm. Amalgam encryption is does not used for secure transaction in Mobile commerce so current system will be used in this encryption process. User Pin number is divided into two halves(pin1 and pin2).The two halves of the pin are encrypted by using amalgam encryption to be separately. By using amalgam encryption, to provide the more security and increasing the encryption secrecy value.

Keywords: Amalgam Encryption, Triple DES, RC4 algorithm, M-commerce, Pin Distribution, Security, AES algorithm.

1. INTRODUCTION

M-Commerce is the ability to perform commercial transactions using mobile phones or other wireless devices on the move. Each mobile device has certain characteristics that influence its usability such as size and color of display, memory and CPU, network connectivity, bandwidth capacity and support Operating System. Mobile commerce opportunity the significant growth in mobile subscription presents an opportunity to further E-Commerce initiatives through mobile devices. The applications of the mobile commerce [1] as shown in table 1.

TABLE 1: Applications of mobile commerce

Mobile Financial Applications (B2C, B2B)	Banking, brokerage, and payments for mobile users
Mobile Advertising (B2C)	Sending user specific and location sensitive advertisements
Mobile Inventory Management (B2C, B2B)	Location tracking of goods, boxes, People
Product Locating and Shopping (B2C, B2B)	Locating/ordering certain items from a mobile device
Mobile Auction (B2C, B2B)	Services for customers to buy/sell certain items
Mobile Booking and Ticketing (B2C, B2B)	Services allowing customers to book, tickets for travel, hotel and events

Mobile transactions are requiring atomicity. The ranges of the mobile applications characteristics [2] as shown in figure 1.

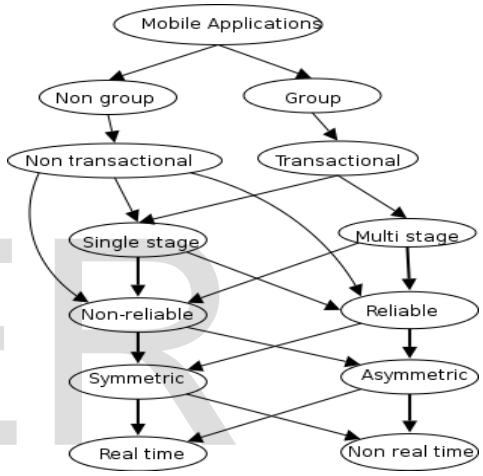

Fig 1: Mobile applications and transactions Requirements [2].

To achieve the security requirement of authorization, authentications, integrity, confidentiality, non-repudiation in mobile commerce are challenging one [3].lot of encryption techniques are used for security, integrity, and confidentiality in mobile commerce.

The main contributions of this paper are

- Pin distribution in more secure way.
- Comparison of Stream cipher and block cipher algorithm.
- Discuss about the amalgam encryption.

2. RELATED WORK

Arunprakash et al[4],proposed the pin distribution techniques. This paper proposed the pin distribution process by using AES encryption. Customer details and Payment details (PIN) are sending by using WAP 1.0. Only, the Mutual authentication is main advantages of this paper. Disadvantages of this paper using WAP 1.0 because WAP 1.0 consists of one security problem, known as the "WAP gap," is caused by the existence of a WAP gateway in a security

session. Encryption, decryption time and throughput is high by using AES algorithm.

2.1 Comparison between Block cipher and Stream Cipher algorithm

Cryptography divides into symmetric ciphers and asymmetric ciphers.cryptograhy area shown in figure 2.

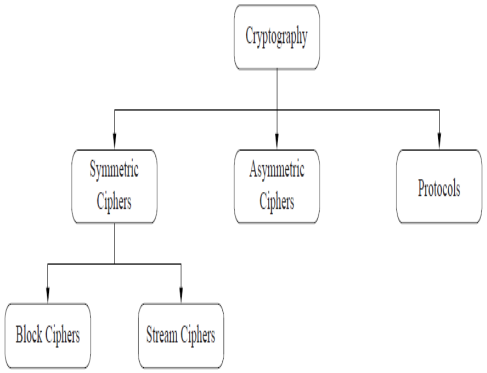

Fig 2: Main area of cryptography [6]

Stream cipher is still being a favorite method for mobile devices for the following valid reasons [5]:

(1) Stream ciphers are typically faster than the block cipher which ensures the low consumption in energy and memory-both of which could drain the battery life.

(2) Block cipher typically requires more memories , since they work on a larger chunks of data and often have "carry over" from previous blocks, whereas since stream ciphers work s on only few bits at a time they have relatively low memory requirements

(3) Stream ciphers doesn't need padding as requires by block ciphers which operates on complete blocks.

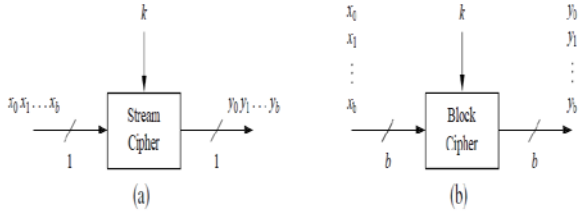

Fig 3: Principles of encrypting *bits* with a) stream cipher b) block cipher [6]

TABLE 2: Comparison of Stream cipher and Block Cipher

S.no	Stream cipher	Block Cipher
1.	Stream cipher that only encryption and decryption data one bit at a Time	Encryption and decryption data one block at a time
2	More suitable in military applications.	More suitable In trading applications
3.	**Advantages:** • Speed of transformation: algorithms are linear in time and constant in space. • Low error propagation: an error in encrypting one symbol likely will not affect subsequent symbols. • Less vulnerable • Less susceptible to cryptanalysis compare than block cipher • Really suitable for hardware implementation • Easy to analyze mathematically	**Advantages:** • High diffusion: Information from one plaintext symbol is diffused into several cipher text symbols. • Immunity to tampering: Difficult to insert symbols without detection. • Block ciphers can be easier to implement in software • Not sufficient in hardware but maybe used to connect keyboard to cpu
4.	**Disadvantages:** ✓ Not suitable in the software ✓ Low diffusion ✓ Susceptibility to insertions and modifications	**Disadvantages:** ✓ Slowness of encryption ✓ Error propagation

2.2 RIVEST CIPHER(RC4) ALGORITHM:

This algorithm is stream cipher and produces a stream of pseudo-random values. The input stream is XOR ed with these values, bit by bit. The encryption and decryption process is the same as the data stream is simply XOR ed with the generated key sequence. If it is fed in an encrypted message, it will produce the decrypted message output, and if it is fed in plaintext message, it will produce the encrypted version [7][8]. RC4 encryption method [9] has its strength that would increase the security of Bluetooth environment. It is a shared key stream cipher algorithm requiring a secure exchange of a shared key.

RC4 has its strength that would increase the security of Bluetooth environment as listed below [5]:-

(1) The difficulties of knowing values in the table

(2) The difficulties of knowing the location in the table used to select each value in sequence

(3) A meticulous RC4 key can be utilized only once

(4) Encryption process is 10 times faster than DES

2.3 FEATURES OF RC4 ALGORITHM:

Some of the RC4 algorithm features can be summarized as[8]:

- ❖ Symmetric stream cipher
- ❖ Variable key length.
- ❖ Very quick in software
- ❖ Used for secured communications as in the encryption of traffic to and from secure web sites using the SSL protocol.

Based on the performance, Stream cipher is better than block cipher [10]-[12]. Stream cipher(RC4 algorithm) is better than

block cipher(AES and DES) comparing the factors like, Image based Encryption and decryption time,CPU time, throughput and memory utilization[10]-[12].performance results as shown in figure 4.

2.4 Block cipher algorithm:

Block cipher algorithm consists of Data encryption standard (DES), Advanced Encryption Standard (AES), Triple DES, Rivest cipher 2(RC2), Blowfish, Rivest cipher6 (RC6). Encryption, Decryption, through put is high in Block cipher algorithm [13].

2.4.1Triple-DES

3DES is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods.[10]-[13].

TABLE3:Algorithm Encryption Performance[10]-[12]

Cipher	Key Length	Speed (Mbps)
DES	56	9
3DES	168	3
RC2	variable	0.9
RC4	variable	45

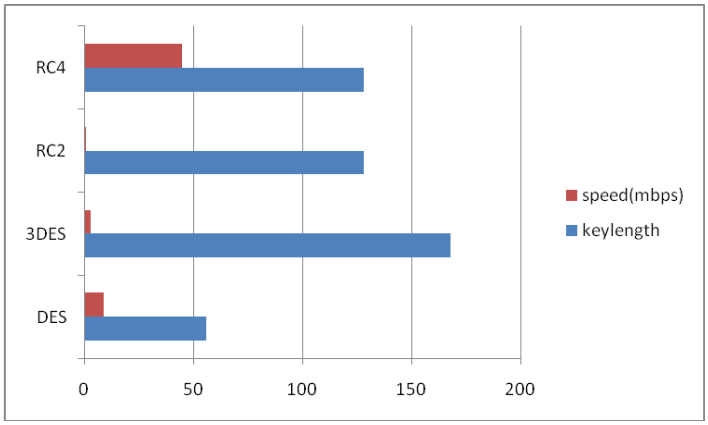

Fig 4: various algorithm performance results on encryption

3. Proposed work

Single encryption does not increase the secrecy value [13],This leads to the proposed level. Amalgam (Hybrid) encryption consists of combination of Triple Data encryption standard (3-DES) and RC4 (3-DES+RC4).another one combination of Advance encryption standard (AES) and RC4 (AES+RC4).These type of amalgam (hybrid) encryption increases the secrecy values [13].

3.1 Pin verification process of proposed system:

The PIN given by the customer is divided into two halves (P1 and p2).PIN 1 is encrypted by amalgam encryption method and verified by remote server. PIN 2 is encrypted by amalgam encryption method and verified by Authentication server. Two halves of the pin verified separately by using amalgam encryption. Finally, verification PIN sends to the Third party by remote server for further process. Pin verification process as shown in fig 5.

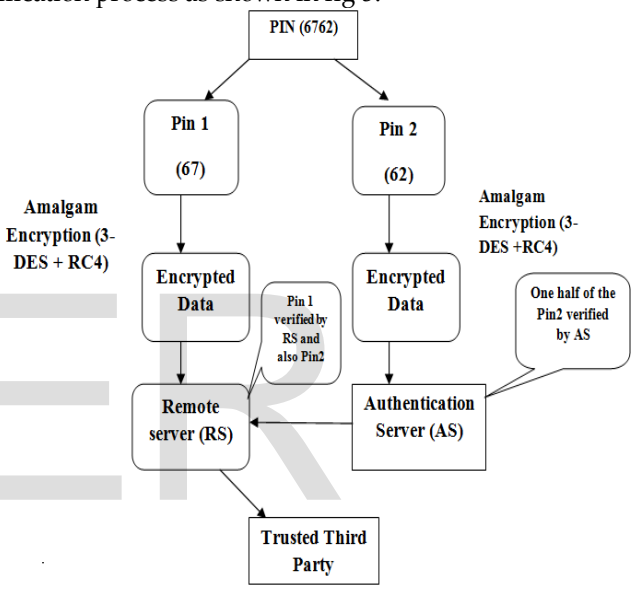

Fig 5: Pin verification process

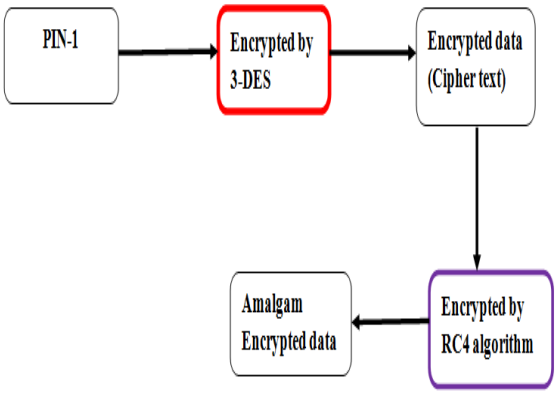

Fig 6: Encryption process

One half (PIN1) of the PIN is encrypted by using 3-DES algorithm and get the cipher text of 3-DES encryption. This

cipher text is again encrypted by using RC4 algorithm and get the amalgam (Hybrid) encrypted data. This amalgam encrypted data is send to the remote server for verification. Another half (PIN-2) of the PIN is encrypted by using similar way as shown in fig 6.

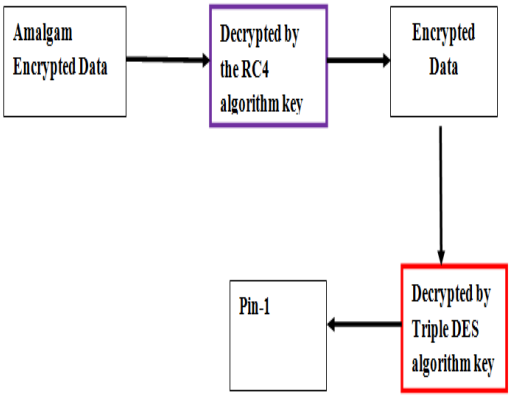

Fig 7: Decryption process

Amalgam encrypted data is decrypted by using RC4 algorithm and get partial plaintext. This Plain text is again decrypted by using 3-DES algorithm and got the one half of the PIN l. This amalgam encrypted data is decrypted by the remote server and verify the correct one half of the PIN. Another half(PIN-2) of the PIN is Decrypted by using similar way as shown in fig 7.Another Half of the PIN is verified by Authentication server and send to the remote server. Remote server is verified the whole Original PIN number given by user. Finally, PIN number is send to the Third party in verification is successful case. Otherwise, process is rejected.In this amalgam encryption process Hybrid -1 (3-DES+RC4) combination process is better than Hybrid-2(AES+RC4) combination process [13] as shown in table 3 and fig 8.Increasing the more Secrecy only by triple DES and RC4 combination[13].

3.2 Simulation Results:

Table 3: Average Secrecy of Ciphers for variable input data sizes [13]

BIT SIZES	HYBRID 1	HYBRID 2
5	0.2151	0.1645
10	0.2295	0.1405
15	0.2237	0.1548
20	0.2206	0.1576
25	0.2313	0.1530
30	0.2259	0.1633
35	0.2375	0.1482

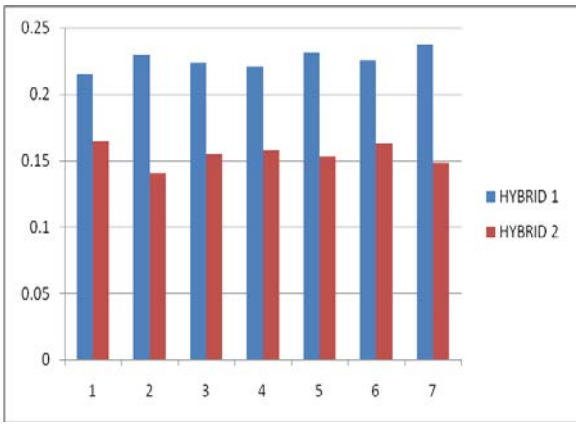

Fig 8: Increasing the Secrecy value using Hybrid scheme

3.3 Benefits of the proposed model:

- ✓ Amalgam encryption is provided more security and increasing the secrecy value compared to the Single block cipher or stream cipher encryption process.

- ✓ Data confidentiality is achieved by using the distributed the PIN. The PIN is divided into two parts and sent. Even if the impostor with the succeeds to trap one half of the PIN, it becomes plentiful to crack the other half of the PIN simultaneously. The cracking of the entire PIN becomes extremely difficult and a tedious process providing enhanced security to this system.

4. CONCLUSION

PIN distributed process is ensured the confidentiality security and Frustration the intruder. The Proposed architecture, it serves to provide a high level security because at each stage a more improved mechanism is introduced to ensure a complete reliable and secure transaction. To add on with this the introduction of a more secure amalgam (Hybrid) Encryption to another key point to ensure the security and reliability of the mobile e-commerce transactions. Secure user and merchant authentication process will explain in next paper.

REFERENCES:

[1] Md. Aminul Islam, Tunku Salha Binti Ahmad, AdoptionOf M-Commerce Services: The Case Of Bangladesh, world journal of management Vol.2 No.1 March 2010, Pp. 37-54.

[2] Punit Ahluwalia,Upkar Varshney, SUPPORTING QUALITY-OF-SERVICE OF MOBILE COMMERCE TRANSACTIONS, Communications of the Association for Information Systems (Volume 16, 2005) 421-434.

[3] JIAN TANG, VAGAN TERZIYAN and JARI VEIJALAINEN, Distributed PIN Verification Scheme for Improving Security of

Mobile Devices, Mobile Networks and Applications 8, 159–175, 2003.

[4] Arunprakash,et.al, improved pin distribution Techniques in m-commerce, Science Direct,GCSE 2011: 28-30 December 2011,Dubai, UAE.

[5] Sivalingham Latchmanan, Dr.Sharmin Parveen, APPLICABILITY OF RC4 ALGORITHM IN BLUETOOTH DATA ENCRYPTION METHOD FOR ACHIEVING BETTER ENERGY EFFICIENCY OF MOBILE DEVICES.

[6] C. Paar, J. Pelzl, Understanding Cryptography, 29 DOI 10.1007/978-3-642-04101-3 2,_c Springer-Verlag Berlin Heidelberg 2010

[7] William Stallings, Cryptography and network security: Principles and practice, Prentice Hall, Upper Saddle River, New Jersey, 2003.

[8] Allam Mousa , Ahmad Hamad , Evaluation of the RC4 Algorithm for Data Encryption

[9] RC4-https://secure.wikimedia.org/wikipedia/en/wiki/RC4, accessed on 2011-09-20.

[10] Naga suman Arepalli,s.srividya,image encryption and decryption based on AES and RC4,IOSR-2012.

[11] T.D.B Weerasinghe, Secrecy and Performance Analysis of Symmetric Key Encryption Algorithms,IJINS, Vol.1, No.2, June 2012, pp. 77~87.

[12] Muazzam Ali Khan Khattak, ENCRYPTION BASED SECURE DATA DELIVERY.

[13] T.D.B Weerasinghe, Secrecy and Performance Analysis of Symmetric Key Encryption Algorithms, International Journal of Information & Network Security (IJINS) Vol.1, No.2, June 2012, pp. 77~87