IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. IV (May-Jun. 2014), PP 80-85
www.iosrjournals.org

Enhanced Security Algorithm using Hybrid Encryption and ECC

A. P Shaikh[1], V. kaul[2]
(I.T, Thakur College of Engineering & Technology /Mumbai University, India)

Abstract: *The AES and ECC are the best two algorithms of symmetric encryption technology and asymmetric encryption technology. The paper presents a hybrid model which uses a combination of two symmetric algorithms enhanced AES and Blowfish for data confidentiality, Message Digest-5 for data integrity, Elliptic Curve Diffie Hellman algorithm-ECDHA for key exchange and Elliptic Curve Digital signature algorithm-ECDSA is used for digital signature. AES is enhanced by modifying the S-boxes columns, and then combination of enhanced AES and blowfish is used for data confidentiality. Performance of this system is evaluated on different configurations on the basis of encryption/decryption time, throughput and memory usage for different data formats like text file, image file, audio file and video file.*

Keywords: *AES, Blowfish(BF), enhanced AES, Elliptic Curve Cryptography, ECDH, ECDSA andMD5.*

I. Introduction

Cryptanalyst are expert in how to break the encryption techniques. We need to safe our programs and documents from cryptanalyst. Security of information means protecting data from unauthorized access in transmission network.

There are many techniques to achieve the security of information from unauthorized access. There are two cryptographic techniques used for data encryption which are Symmetric and Asymmetric techniques.

Symmetric techniques like DES, IDEA, Blowfish, RC4, RC5, RC2, Triple DES, and AES. DES algorithm use feistel network, the key size is 56bit. Due to small key size DES is insecure and has weaknesses. Triple DES which is an enhancement to DES, the original DES algorithm was applied thrice to increase the security. But it was found to be very slow. Blowfish algorithm runs faster than other symmetric algorithms[1][2]. The AES is recommended symmetrical based encryption standard by NIST [3] [4].AES algorithm is the best encryption algorithm. The blowfish algorithm is fastest as compare to other algorithms but it has less security than the AES. To overcome these weaknesses, we use combinational model implementation which is AES with Blowfish algorithm.

Asymmetric key algorithms used like RSA, Rabin Cryptosystem, ElGamal Cryptosystem and Elliptic Curve Cryptosystem. RSA give better security because of its factoring large key number but drawback of RSA is to factorize the large number which increases the computational overhead. ECC give equal security in small key as compare to the RSA algorithm[5]. RSA with key size 1024 bit give the security equivalent to the ECC with key size 160 bits[6]. ECC is fast for digital signature creation and faster digital signature verification as compare to RSA [7]. NIST recommend Elliptic Curves for Government use [8].

ECC is an emerging alternative for traditional Public-Key Cryptosystem like RSA, DSA and DH.ECC with ECDH is called ECDHA (Elliptic curve Diffie Hellman Algorithm) for key exchange. ECDHA can use in WAN for secure hypertext information transmission [9].

AES and ECC are the best two algorithms of symmetric encryption technology and asymmetric encryption technology.

There are different cryptographic hashing algorithms used for message authentication some are like MD2, MD4, MD5, MD6, SHA-1, SHA-224, SHA-256, SHA-512, Whirlpool etc.

NSA publicly announced Suite B Cryptography [10] which was built on National Policy on the use of the AES to Protect National Security Systems and National Security Information (CNSSP-15).

Here mixing of AES and ECC encryption algorithm has been done. This algorithm enhances the speed of data encryption and decryption[11]. Here, using Message Digest 5(MD5) for integrity. The key exchange is done by the ECDHA. The ECDSA is used for digital signature. The ECDSA is the elliptic curve analogue of the DSA [12].

II. Cryptographic Techniques

The goal of Information security is to achieve confidentiality by cryptography, integrity by hashing, and availability by access control. Information security use cryptography when transferring information such that information is unable to unauthorized parties. There are two cryptographic techniques are Symmetric and Asymmetric techniques are shown in Fig 1.

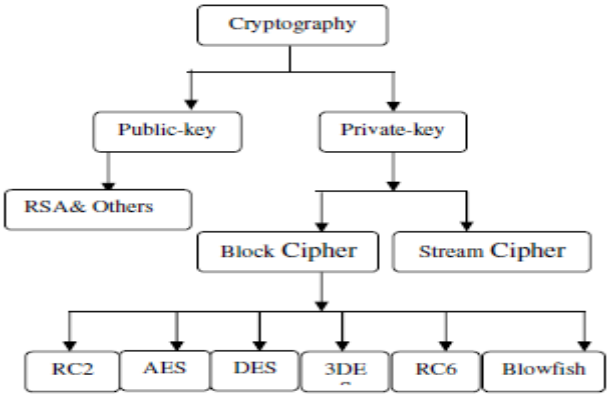

Figure.1Classification of Cryptography technique

Encryption protects secret digital data from unauthorized users. Data encryption improves database security and achieve confidentiality security goal. Integrity can achieve by different hashing techniques and authentication by digital signature.

III. Proposed System Architecture

The encryption and decryption of a data is done by combination of AES and Blowfish algorithms. Key management and authentication is done by using the concept of Elliptic Curve Cryptography. For key management and key exchange, Key is generated by the ECC key generator and then Key agreement can be done by Diffie-Hellman. Combining the concept of ECC and DH is called Elliptic Curve Diffie-Hellman (ECDH) key exchange. Authentication should be done by Using ECDSA.-

3.1Hybrid Symmetric and Symmetric Algorithm

First we use two symmetric encryption algorithms AES and Blowfish. Combining these two algorithms, will increases the run time for encryption/decryption. The total time required for hybrid algorithms will be the addition of both the algorithm's run time (processing time). Blowfish requires less time as compared to others algorithms, Blowfish algorithm adds the additional time for processing but it will enhance the overall security. The combination of enhanced AES and Blowfish is as shown in Fig. 2

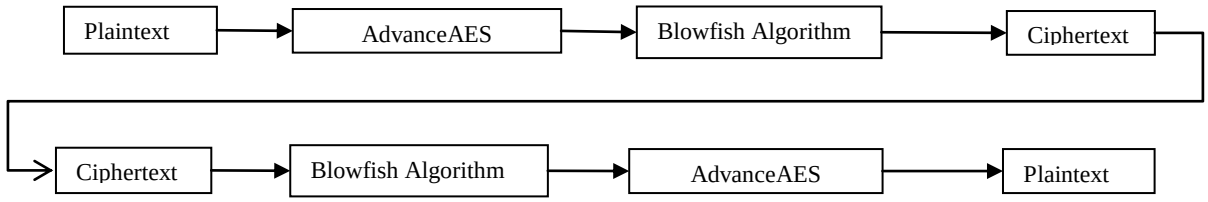

Figure 2Hybrid AES and Blowfish data encryption and decryption

3.2 Sender's System Steps are as follows

In sender system we are encrypting the data with AES and Blowfish with the seed value key (Initial vector) entered by the sender at the time of encryption. The encryption key is again encrypted by the ECC concept and finally tis key send to the channel using key management algorithm that is ECDHA.

1. Take plain text or any file as input.
2. Applying MD 5hashing function plain text and gives128bit of Message Digest value.
3. Generate private and public key by ECC generator[13].
4. Apply Blowfish with AES on plain text by using key to generate cipher text.
5. Apply Digital Signature to Hashed Result by using private key.
6. Step 5 will generate a Signature Block.
7. Apply ECC encryption to AES key using public key (key) that will result AES key block.
8. Apply digital signature on encrypted file.
9. Now, Send encrypted file along with encrypted AES key to destination.

Sender's system sends the three file 1) Encrypted data, 2) Encrypted key, and 3) Digital signature.
The Sender's System Architecture is shown in Fig. 3.

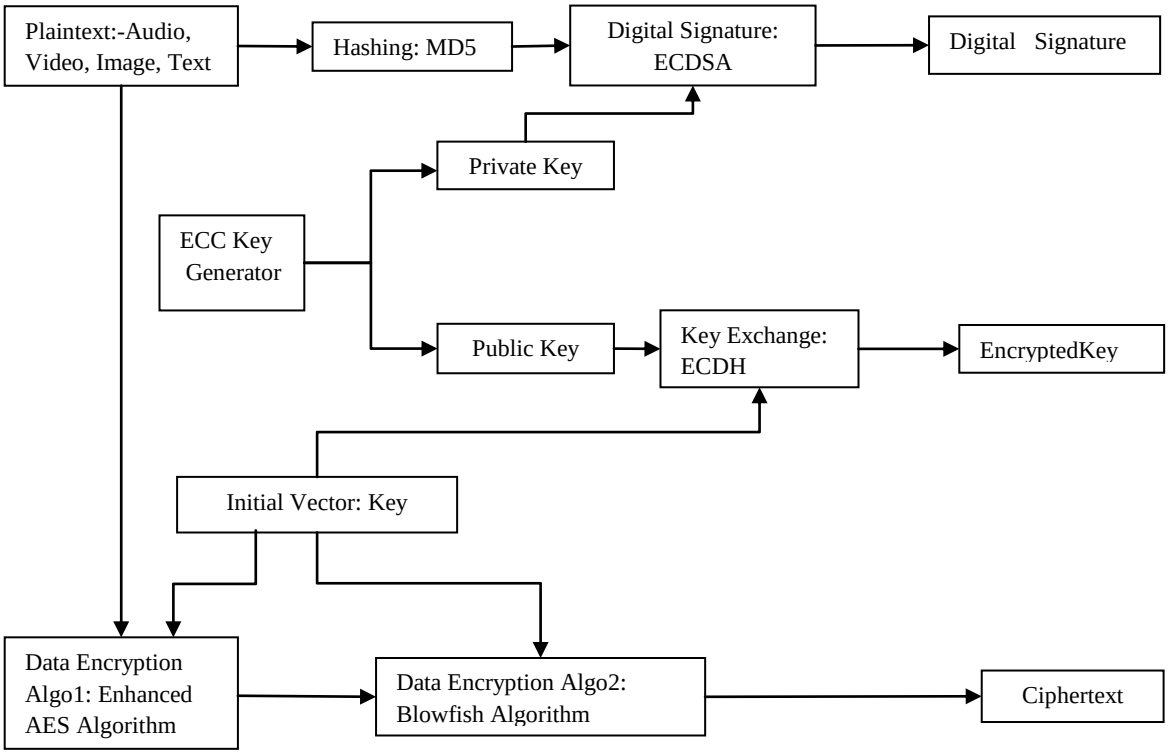

Figure 3Sender's System Architecture

3.3 Receiver's System Steps are as follows

The receiver system decrypts the received encrypted data by two decryption algorithms AES and Blowfish. Key to encrypt the data gets from the applying decryption of ECC algorithm (ECDH). That is private key of sender and public key receiver. Result gives the plain text. Apply the message digest algorithm on this plaintext data. The message digest that we get from plain text at receiver and received message digest of size 128 bit are compare with each other to validate. If both the message digest are same the data get accepted else if the both are differ then the received data get discarded.

Receiver system receives three files 1) Encrypted Key, 2) Encrypted data, and Digital signature. Digital signature authenticates the sender and gives the message digest.

1. Receive encrypted file along with key and perform cryptanalysis on it.
2. Then we will be having 3 blocks.

a. Cipher text block
b. AES key block
c. Signature block

3. Apply Private Key of receiver on AES key block it will provide AES key.
4. Apply public key on Signature block for authentication which will generate Abstract result.
5. Apply AES key on cipher text block which will give plain text and then abstract result.
6. Compare both step 4 output and step 5 outputs.

a. If the comparison is found consistent then

i. Grant access

b. Otherwise

ii. Failure

The Receiver's System Architecture is shown in Fig. 4.

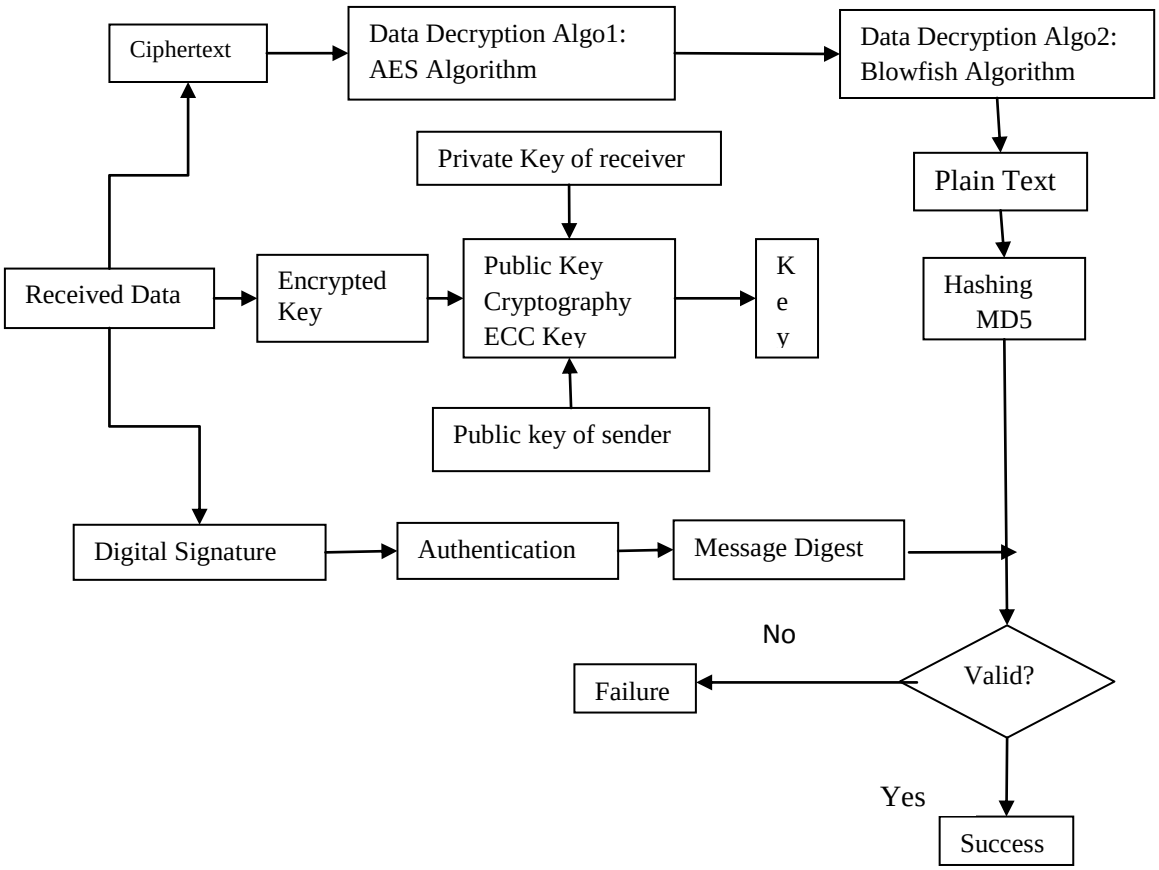

Figure 4Receiver's System Architecture

IV. Evaluation Method

All the algorithms are important of network information security. The performance evaluation of proposed algorithms done based on following parameters:

1 Encryption and Decryption Time (Run Time)

Encryption speed is a runtime of algorithm. The runtime is important for evaluating algorithm performance. Runtime is the algorithm lifecycle phase during which the algorithm executing.

2 Throughputs

The throughput of algorithm is sum of data rate that are delivered to all network.

3.2 Experimental Results

Algorithms used

Encryption/Decryption: AES and Blowfish

Key Management: ECDH

Hashing: MD 5

Digital Signature: ECDSA

Computer Configurations used for Testing: AMD FX(tm) – 8120, Eight Core Processor 3.1GHz, RAM 8 GB, 64 bit system.

File Types: Audio, Image, Video and word.

All the algorithms are developed on Net beans7.3.1platformwith JAVA languageon 64 bit operating system.

Table 1 Algorithm characteristics

	AES	**BF**
Block size	128 bits	64 bits
Key size	128 bits	32 bits up to 448bits
Number of rounds	10	16

4.1.2Performance Evaluation in terms of Runtime

Runtime measured in milliseconds. The comparative execution time in CBC mode is shown in Table 2. Graphical representation of encryption runtime is shown in Fig. 5 and decryption runtime show in Fig. 6.

Table 2Comparative runtime (in milliseconds)of encryption and decryption in CBC mode

	Encryption Runtime			Decryption Runtime		
File size in bits	AES	BF	AES + BF	AES	BF	AES + BF
81184	19	5	27	20	6	31
204240	45	10	63	50	15	70
409600	100	20	115	90	30	125
551952	125	27	165	140	35	180
Average Time	72	16	92	75	21	101

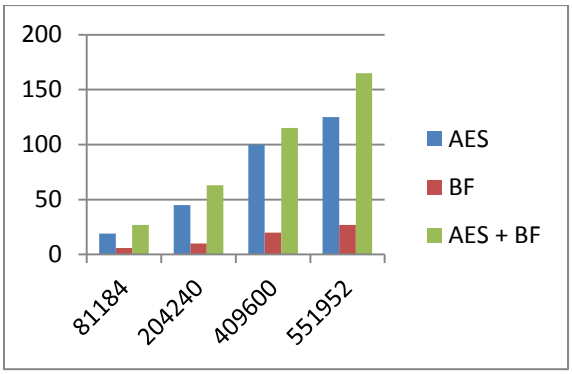

Figure 5 Graphical representation of encryption runtime

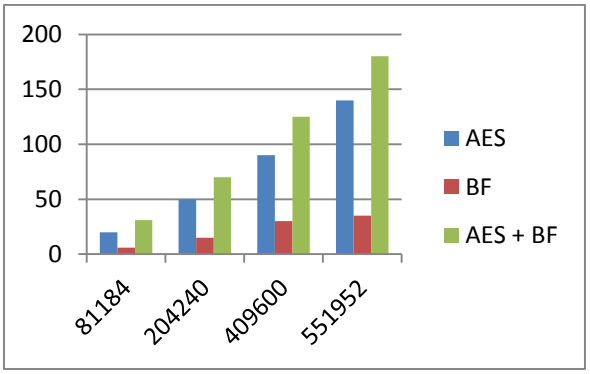

Figure 6 Graphical representation of decryption runtime

Result shows the runtime for blowfish algorithm is less than the runtime for AES algorithm. The runtime for the combined AES and BF algorithm is much higher than the runtime for BF and AES algorithm separately.

4.1.2 Performance Evaluation in terms of Throughput

Throughput measured in Bits per Second. The comparative throughputs of decryption in CBC mode are shown in Table 3.

Table 3Comparativethroughput (bits per second) of encryption and decryption in CBC mode

	Encryption Throughput			Decryption Throughput		
File size in bits	AES	BF	AES + BF	AES	BF	AES + BF
81184	4272842	16236800	3006815	4059200	13530666	2618838
204240	4538666	20424000	3241905	4084800	12014117	2917714
409600	4096000	20480000	3561739	4551111	13653333	3276800
551952	4415616	20442667	3345163	3942514	15613918	3066400
Average TP	4330781	19395867	3288905	4159406	13703009	2969938

The average throughput for Blowfish algorithm is very high than the average throughput for AES and combined AES and BF algorithm and average throughput for AES algorithm is more than the average throughput for combined AES and BF algorithm.

The throughput results in AMD eight core, CPU 3.1 GHz:

- The average throughput of AES encryption is 4330781 bps (528.66KBps& 0.5MBps) and decryption is 4159406 bps (507.74KBps& 0.49 MB).
- The average throughput of BF encryption is 19395867 bps (2285.07KBps&2.31MBps) and decryption is 13703009 (1672.73KBps& 1.6MBps).
- The average throughput of combinational AES and BF is 3288905 bps (401.47KBps& 0.39MBps) and decryption is 2969938 bps (362.54KBps& 0.35MBps).

V. Conclusion

Result shows AES is the best algorithm of symmetric encryption technology. AES algorithm is more secure than the Blowfish algorithm, and Blowfish is secured than the other algorithms. Blowfish gives high throughput as compared to AES and other algorithms.

The hybrid of AES and Blowfish algorithm has characteristics of both the algorithms and it makes the algorithm strong against vulnerabilities. This hybrid structure of enhanced AES and Blowfish provides more security by increasing the complexity.

ECC is the best algorithm of asymmetric encryption technology. The ECC is an emerging alternative for traditional Public-Key Cryptosystem like RSA, DSA and DH.

ECC provides the highest strength-per-bit of any cryptosystem known today with smaller key sizes like RSA, resulting in faster computations, lower power consumption and memory. It also provides a methodology for obtaining high-speed, efficient and scalable implementation of protocols for authentication and key agreement.

ECC concept using with DH to solve the problem of key Exchange the algorithm is called ECDHA. ECC is also use for the digital signature is called as an ECDSA algorithm.

Limitation of this system is to decrease the throughput and thus data rate obtained is just compatibly with LTE. But the complexity of the system is increased that of combination of two algorithms.

References

[1]. T. Nie, C. Song and X. Zhi," Performance Evaluation of DES and Blowfish Algorithms, Biomedical Engineering and computer Science International Conference, IEEE, 2010.
[2]. A. Nadeem and M.Y Javed., "A Performance Comparison of Data Encryption Algorithms," IEEE Information and Communication Technologies, 2005. ICICT 2005. First International Conference, 2006, pp. 84- 89.
[3]. J. Daemen and V. Rijmen, "AES submission document on Rijndael, Ver2", September 1999.
[4]. "Announcing the Advance Encryption Standard", FIPS Publication, 2001.
[5]. M.J.B. Robshaw and Y. L. Yin, "Elliptic Curve Cryptosystems", RSA Laboratories Technical Note, 1997.
[6]. V. Gupta, S. Gupta, S. Chang, and Douglas Stebila, "Performance Analysis of Elliptic Curve Cryptography for SSL", ACM, 2002.
[7]. N Jansma, and B Arrendondo, "Performance Comparison of Elliptic Curve and RSA Digital Signatures", "http://www.nicj.net/files/", 2005.
[8]. NIST, "Recommended Elliptic Curves for Government Use", NIST 1999. "www.scrc.nist.gov".
[9]. V. Gupta, S. Gupta, S. Chang, and Douglas Stebila, "Performance Analysis of Elliptic Curve Cryptography for SSL", ACM, 2002.
[10]. NSA Government, SuiteB Cryptography / Cryptographic Interoperability, 2005. "http://www.nsa.gov/ia/programs/suiteb_cryptography/".
[11]. X. Li, J Chen and D. Qin "Research and Realization based on hybrid encryption algorithm of improved AES and ECC", IEEE, 2010.
[12]. Certicom Research, D. Johnson, A. Menezes and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", Certicom Research, 2001.
[13]. H. Brar, "Performance analysis of Point multiplication methods for Elliptic curve cryptography", 2010.