A Pragmatic Study on Hybrid-Crypto-Coding Schemes for Secure Data Access

T. J. Jeyaprabha[1], G. Sumathi[2]

[1] Department of ECE, Sri Venkateswara College of Engineering, India
[2] Department of Information Technology, Sri Venkateswara College of Engineering, India
jprabha@svce.ac.in, gsumathi@svce.ac.in

Abstract

Cloud technology is a fast developing computing technology through which resources are shared via the internet. Though it is growing fast, the hurdle to its growth is security. In general, sophisticated encryption algorithms are using the locking key, to prevent unauthorized access of data placed in the cloud. If the unlocking key is placed along with the data in the cloud then attack is very easy. To increase the toughness in accessing the data some additional security mechanism will help to save the data in the cloud. In this paper, a hybrid encryption algorithm with channel coding scheme and additional interleaver is proposed. Computational complexity is analyzed based on time complexity for the proposed algorithm. The hybrid cryptography schemes chosen for analysis are AES-ElGamal, DES-RSA, and TDES-Rabin. These hybrid cryptography schemes along with Turbo coding ensure joint-defense on security and reliability. This work concentrates on applying the Hybrid-Crypto-Coding scheme (HCC) for enhancing security at distributed data storage centers. Simulated outputs show that the proposed system provides better security and reliability when compared to conventional schemes. Among the three hybrid cryptography schemes, the AES-ElGamal pair outperforms the rest.

Keywords: Cryptography, Hybrid-Crypto-Coding, Reliability, Security

1 Introduction

A network of intelligent devices that gather and swap data among themselves is known as the Internet of things. Big data is a huge and complex data set generated by all the smart devices. Cloud computing gives a centralized platform for accessing these data. The extraction of big data is possible when the user machine is linked via the internet. Big data can be captured easily with IOT. The collected data can be stored and processed using cloud computing. Cloud computing has come out from grid computing, parallel computing, utility computing, and virtualization [1-3].

National Institute of Standards and Technology (NIST) has defined, cloud computing as a system to access shared computing resources like storage, networks, servers, applications, and services which can be provided swiftly and freed by the customers with few management efforts and/or interaction with the service provider through any access network.

Cloud computing can be defined by describing three service models, five essential characteristics, and four basic models [2-3]. The main features are self-service when requested, broad access of network, pooling of resource, measured service, and quick elasticity. The basic models are private cloud, public cloud, community cloud, and hybrid cloud models. The three service models are Platform-based service model, Software-based service model, and Infrastructure-based service model.

Cloud computing has given way for accessing the data with reduced infrastructure cost, time and maintenance. Though it has several advantages, security threats are challenging in the cloud domain [4-6]. The three security concerns are 'availability', which ensures to access the data when needed, 'integrity', which ensures to protect the data from getting altered by unauthorized unit and 'confidentiality', which allows accredited users to read the protected data. The public cloud is the one that is most affected as the customer is not aware of where the information is placed, how it is processed.

The non-profit organization Cloud Security Alliance (CSA) has mentioned vital threats on security in cloud computing [1, 7-9]. There may be a violation of data due to human error or insufficient security practices, bad actors claiming as the genuine entity using false identity, credential, and access management, unsecured interfaces, vulnerabilities of systems, account or service stealing, mischievous insiders, Advanced Persistent Threats (APTs) or targeted cyber attack, data loss due to accident or physical catastrophe, insufficient due diligence, misuse and dreadful use of cloud services, attack with denial of service and shared technology vulnerabilities. Security issues in a cloud

[*] Corresponding Author: T. J. Jeyaprabha; E-mail: jprabha@svce.ac.in

DOI: 10.3966/160792642021032202012

domain are displayed in Figure 1. The security types are data storage security, data transmission security, application security, and resources of third party [3, 10-13].

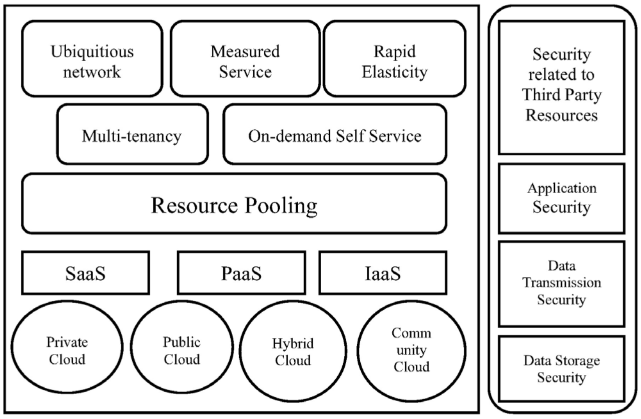


Figure 1. Security Issues in Cloud Environment
Image Courtesy: www.sciencedirect.com

Conventional systems use cryptography for protecting cloud information [3, 14-16]. Cryptography is utilized for hiding the data from unauthorized users. When data is in transit through unsecured channels, cryptographic algorithms and protocols are required to keep the data secure.

In Cloud computing, the major problems are related to data security, backups, network traffic, file system, and security of hosts [4, 9-10]. Cryptography can resolve these issues to some extent. All the encryption techniques are sensitive to noise when the encrypted data travels through the unreliable channel [11, 17-18]. Even small errors in the encrypted data may give a different decrypted plaintext. To recover from these errors additional channel coding schemes must be added with encryption to protect the data. Both the encryption and channel coding techniques function independently. If the encryption process is combined with channel coding schemes like Low-Density Parity Check (LDPC) codes and Turbo codes [17-19], the system performance can be enhanced in terms of security and reliability. A survey has been made on best practices to secure data in the cloud [20-21] and it is summarized in Table 1. In the proposed work, the cryptographic protocol is taken for comparison. The results have been simulated for different data sizes and tabulated in Section 6.

Table 1. Best Security Practices for Cloud Data

S.No.	Security Algorithm Used	Method used	Disadvantages	Advantages
1.	Erasure coding	Peer-to-Peer (P2P) Method	It requires huge storage and additional network overhead	High probability of retrieving files under severe peer failure conditions
2.	Cryptographic protocol	Public/ Private key distribution and digital signature	1. Protocol is its vulnerability 2. Theft of the central keys 3. Reliability of data not guaranteed	Confidentiality and trust worthiness of data
3.	Privacy preserving, auditing and extraction of digital contents	Initialization, audit, and extraction	Protocols do not safe guard from DoS attacks	Eliminates the burden of verification from the customer
4.	Principles of (Redundant Array of Independent Discs) RAID Codes	High Availability and Integrity Layer (HAIL) architecture	HAIL provide guarantee for static files	Efficiency, security, and modeling improvement in terms of availability
5.	Predicate Logic	This is obtained by using predicates over encrypted data	1. Computational complexity 2. Storage increased	Ability to verify without revealing unencrypted data
6.	Homomorphic Encryption	Conversion of one data set into another while maintaining relationships between elements in both sets	1. Computational complexity 2. Time consuming 3. Increase in cost	1. Allows companies to store encrypted data in public cloud 2. Allows processing on enciphered data without deciphering
7.	Split-Key Encryption	Safety locker technique which uses two keys, master key with client and second key with Cloud Service Provider (CSP)	Both Client and CSP keys are required for handling the data; if one key is lost then data cannot be handled	The data is not revealed to CSP at any cost
8.	Honeypots	Infiltration finding and reaction mechanism	It cannot prevent the attack	Exploratory snooping technique to study more about the attacker

Table 1. Best Security Practices for Cloud Data (continue)

S.No.	Security Algorithm Used	Method used	Disadvantages	Advantages
9.	Sandboxing	Virtualization between the software and code executed from the Operating Systems (OS)	Clever social engineering, a bad user interface can defeat any sandbox	Adds layer of security between the applications running within a guest Virtual Machine (VM) and the hypervisor
10.	Data Sanitization	Segregating sensitive data from insensitive data	1. Different levels of masking for different end users 2. Different masking techniques for different data types	Data is hidden from unauthorized access

The proposed scheme combines both cryptography and channel coding schemes. Channel coding is done for reliability and cryptography is done for security in terms of confidentiality. A Hybrid-Crypto-Coding scheme adds additional security in terms of authentication for securing the shared secret key.

1.1 Symmetric and Asymmetric Cryptographic Schemes

Cryptographic techniques can be classified as two major groups as private key cryptography that uses one key for encryption as well as decryption and public key cryptography that uses different keys to encrypt and decrypt. In both cases, intelligible text called plaintext is converted to an unintelligible text called ciphertext using an encryption algorithm. The popular cryptographic algorithms are AES, DES, Triple DES, RSA, cryptography using Elliptic Curve, and ElGamal. The first is symmetric key cryptography and the rest is asymmetric key cryptography.

1.2 Crypto-Coding Scheme

All the types of encryption are reactive to noise when transmitted through unreliable channel hence channel coding schemes ought to be used after encryption. Both these functions work separately. If the process of encryption is combined with channel coding scheme, the system performance can be improved in terms of reliability and security [1, 17, 22].

The major augmentations of this research paper are given as follows:

1. Analysis of three pairs of hybrid cryptography techniques namely, AES-ElGamal, DES-RSA, and TDES-Rabin in terms of providing security to the data.

2. Additional interleaver after encryption and before turbo coder to make the data more secure.

3. Performance analysis considering when only encryption, only channel coding are done, including and excluding the additional interleaver, encrypting the data before and after interleaving, various modulation schemes, and varying channel conditions namely AWGN and Rayleigh channels.

The remaining portion is structured as given below. Section 2 outlines the encryption-decryption algorithms, and channel coding scheme. Section 3 explains the proposed Hybrid-Crypto-Coding (HCC) model. Section 4 highlights the results of the simulation using MATLAB. BER performance and security enhancements are considered in this section. In Section 5, the implementation and testing results in AWS are shown. In Section 6 a comparative analysis of proposed schemes is shown. The conclusion and scope for the future are highlighted in Section 7.

2 Outline of Cryptographic Techniques and Channel Coding

A great number of researchers have analyzed various techniques of cryptography based on performance metrics like key size, complexity, time taken to break the cipher, and number of rounds. Here, a study is made to analyze the performance of three combinations of hybrid cryptography algorithms DES-RSA, AES-ElGamal, TDES-Rabin along with turbo coding, with reference to SNR and BER, brute force attack on each scheme.

2.1 Review of Cryptographic Techniques

Cryptography is a hot research area. Cryptography ensures information and data security in terms of secrecy, authenticity and/or integrity by constructing protocols and algorithms. It is classified into private-key and public-key algorithms. Alternatively it can be classified as block ciphers and stream ciphers. Block ciphers exhibit error propagation effect which can prove highly valuable in authentication. Among many cryptographic systems Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Triple DES (T-DES) are popular private-key algorithms and Rivest-Shamir-Adleman (RSA), ElGamal and Rabin algorithms are popular public-key algorithms. In private-key algorithms one single key is maintained secret between transmitter and receiver whereas public-key algorithms split key into two parts, one maintained secret and other key is public. In the latter system, it is computationally infeasible to recover the secret text from the encrypted text [23]. Cryptographic algorithms find applications in SIM and SMART cards, network devices like routers, MODEMs, and many wireless applications.

2.2 Review of Turbo Codes

In information theory and coding, turbo codes are considered as high-performance forward error correction (FEC) codes which were introduced between 1990-91 (but first published in 1993) were the first realizable codes to nearly reach the maximum theoretical limit on Shannon's channel capacity and also provide reliable communication for a fixed noise level [19, 24-25].

In this paper, an analysis of the behavior of turbo codes for various modulation types, modulation order, and repetition of iterations is made. The simulation in MATLAB is carried out for varied noise levels and the characteristic graph is plotted against SNR and BER. The analyses prove that it is very much suitable for achieving reliability and enhancing security.

2.2.1 Turbo Encoder

Figure 2 shows the construction of turbo encoder [1, 26]. The encoder is constructed using two -component encoders (Recursive Systematic Convolutional encoders) coupled in parallel and partitioned using an interleaver or permuter. The structure of encoder is called parallel connection as both encoders work on an identical set of input values.

$$G(D) = \frac{g_1(D)}{g_0(D)} \quad \textbf{(1)}$$

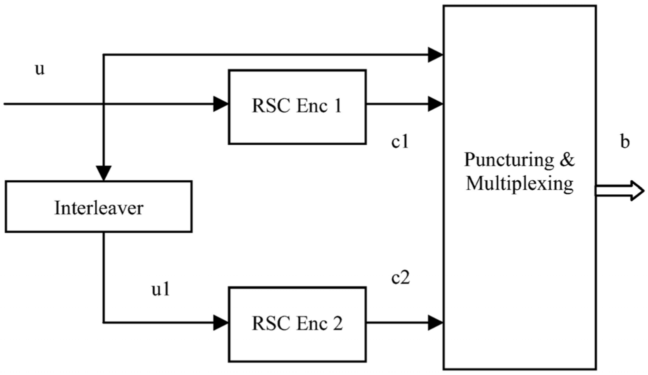


Figure 2. Structure of a Turbo Encoder

The rate ½ component encoders' generator matrices are expressed as in equation 1 where $g_0(D)$ and $g_1(D)$ are generator polynomials. In the turbo coder, an identical data sequence is encoded two times except in a varied order. The first encoder works on the data bits of length N. The second encoder works on identical bits permuted in a varied order. The data is turbo encoded before sending it into the channel and after the reception the data from the channel, it is turbo decoded. The special characteristic of turbo codes is that a better performance i.e. lower error rate achieved at lower SNR values. The binary input sequence u of finite duration is fed to the first component encoder to get the redundant sequence c_1 of the same finite duration as the input sequence. The permuted sequence u1 in parallel is put into the second component encoder to produce an output redundant sequence c_2. The redundant sequences c_1 and c_2 along with u is sometimes punctured and then multiplexed for generating the output sequence b.

The memory of the encoder is M and constraint length is K=M+1. An input at any time instant t is u_t and its equivalent binary output is represented as X_t and Y_t.

$$X_t = \sum_{i=0}^{Y} (g_{1i} u_{t-i})$$

$$g_{1i} = [1\ 1\ 1] \quad \textbf{(2)}$$

$$Y_t = \sum_{i=0}^{v} (g_{2i} u_{t-i})$$

$$g_{2i} = [1\ 0\ 1] \quad \textbf{(3)}$$

where g_{1i} and g_{2i} are the two encoder generators.

The input sequence of N input bits or symbols to the turbo encoder is,

$$u = \{u_1, ..., u_N\}$$

The a priori probability distributions associated to the sequence of input bits are,

$$p(u; I) = (p_t(u_t; I))\ t \in T \quad \textbf{(4)}$$

$$c = \{c_1, ..., c_N\}$$

The associated a priori probability distributions for the output sequence are represented as:

$$p(c; I) = (p_t(c_t; I))\ t \in T \quad \textbf{(5)}$$

2.2.2 Turbo Decoder

Parallel concatenation of convolutional decoders is used in the Turbo-decoder for decoding the input signal as shown in Figure 3. Two a posteriori probability (APP) decoders are used in the iterative decoder as the constituent decoders (shown as SISO modules) along with an interleaver and a de-interleaver [25-26].

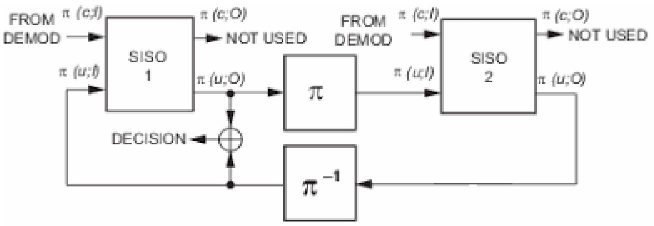


Figure 3. Structure of a Turbo Decoder

Log-likelihood values of the encoder input bits, π (u; O) are produced by the decoders to generate a sequence. This generated sequence arrives from the received log-likelihood sequence of the channel parameter and its coded bits π (c; l). The decoder updates the likelihood values after a set of iterations and then regenerates the decision bits. The interleaver (π) that is used by the turbo decoder is similar to that of the one used by the turbo encoder at the transmitter side. The reverse operation of interleaver is done by deinterleaver (π^{-1}). The decoder does not assume the tail bits and is excluded during iterations.

The constituent decoder module shown as SISO has four I/O ports [25-26]. The probability distributions of input sequences are p(c; I) & p(u; I) which are given as inputs and output sequences are generated with probability distributions p(c; O) & p(u; O) for corresponding inputs and trellis information. The time index set t is assumed to be finite, i.e., t = {1, ..., n}. The SISO operation is explained in two steps for finding the output distribution. The first step,

(1) For any time t, the probability distributions of output are computed as

$$p_t(c; O) = N_c \Sigma_{e:c(e)=c} a_{t-1} [m^M(e)]\, p_t [u(e); I]\, p_t [c(e); I]\, b_t [m^E(e)] \quad \textbf{(6)}$$

$$p_t(u; O) = N_u \Sigma_{e:u(e)=u} a_{t-1} [m^M(e)]\, p_t [u(e); I]\, p_t [c(e); I]\, b_t [m^E(e)] \quad \textbf{(7)}$$

(2) $a_t(\cdot)$ and $b_t(\cdot)$ values are found through the forward and backward recursive functions, respectively, as

$$a_t(m) = \Sigma_{e:m^E(e)=m}\, a_{t-1} [m^M(e)]\, p_t [u(e); I]\, p_t [c(e); I] \quad k = 1 ,..., n \quad \textbf{(8)}$$

$$b_t(m) = \Sigma_{e:m^M(e)=m}\, b_{t+1}[m^E(e)]\, p_{t+1}[u(e); I]\, p_{t+1}[c(e); I] \quad t = n - 1,..., 0 \quad \textbf{(9)}$$

with initial values

$$a_0(m) = 1 \text{ at } m = M_0 \quad \textbf{(10)}$$

$$b_n(m) = 1 \text{ at } m = M_n \quad \textbf{(11)}$$

The variables N_c, N_u are normalization constants defined as follows:

$$N_c \rightarrow \Sigma_c P_k(c; O) = 1$$
$$N_u \rightarrow \Sigma_u P_k(u; O) = 1$$

3 Proposed Hybrid-Crypto-Coding Cloud Security Model

3.1 Hybrid-Crypto-Coding Scheme

In any communication system, a cryptographic application is usually implemented at a layer above the physical layer and assumes that the channel is noise-free. However, in any real-time applications, the channels for friendly users and passive eavesdroppers are not error-free. Channel coding is very much necessary for noisy channels. Tapper may listen to any confidential information secretly without the knowledge of friendly users. Modern cryptography uses pseudorandom generators (PRGs) to transform a set of small beginning set of bits into a long series of bits which appear to be random. PRGs use Linear-feedback shift registers (LFSRs) as they have good statistical and periodicity properties. By increasing the computational complexity of unmasking the secret key, a tapper can be made to undergo difficulty in breaking an LFSR-based cryptographic system. Traditional communication systems have implemented cryptographic techniques for handling security, channel coding for handling reliability.

Channel coding can be combined with cryptography for providing confidentiality and reliability for discrete sources [17, 22]. Hybrid encryption schemes are chosen for enhancing security [27-31]. The proposed Hybrid-Crypto-Coding (HCC) model helps distributed data to defend on attacks against confidentiality, authentication, and reliability. The main advantage of going for this hybrid-crypto-coding scheme is to achieve security without requiring a large key size. The block diagram of secured and reliable data access from the distributed data center is shown in Figure 4.

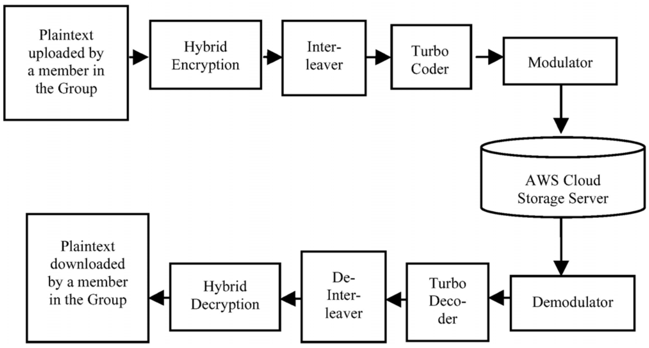


Figure 4. Block Diagram of Proposed Hybrid crypto-coded Security Model

When encrypted information is transmitted over an unsecured channel it will result in an error propagation effect, which degrades the bit error rate (BER) performance of the system. The error propagation effect is due to noisy and unsecured channels. With standard encryption algorithms alone for security, there is a loss in BER performance in the order of 1 to 5 dB with respect to un-encrypted and uncoded data. To compensate for this loss channel coding is performed. If the length of the key is made large then there may be a substantial improvement in the BER performance. Hybrid-Crypto-coding scheme shown in Figure 5 is proposed to guarantee both security and reliability. The information which is to be placed in a distributed data storage environment can be a text, audio, image, or video file. For security, the information has to be encrypted before placing in the cloud, while placing the data in the cloud, information has to be transmitted through an unreliable channel hence channel coding is necessary. For hiding data and the key hybrid-crypto-coding scheme is used. Here, the message is encrypted using any one symmetric key encryption technique (DES/AES/TDES), and the symmetric key itself is encrypted using any one public key encryption technique (RSA/ElGamal/Rabin). An interleaver is added to the block before the Turbo coder to provide additional security and to minimize the burst error. Turbo code is used for channel coding. When encryption and error control coding like turbo codes are performed the loss is less but adds strong security. This can also strongly reduce the BER degradation effect at lower SNR value. The encoded data is then modulated and transmitted through the channel. The modulation schemes chosen are 8PAM, 8PSK, and 16QAM. The channel types analyzed are AWGN and Rayleigh. The encrypted data then passes through the channel and placed in the cloud storage server.

Actual flow of HCC Scheme:

At Transmitter side:

1. The information (text/image/audio/video) is encrypted using the symmetric key algorithm (AES/DES/TDES), to get the encrypted data.

2. The secret key of symmetric key algorithm is encrypted using public key of asymmetric key algorithm (ElGamal/RSA/Rabin).

3. The encrypted data along with the encrypted secret key are sent through an additional interleaver before channel coding.

4. The interleaved data is channel coded using turbo encoder.

5. The crypto coded data and encrypted secret key are modulated and sent through AWGN/Rayleigh channel to be stored in distributed data storage.

At Receiver side:

6. The reverse operation is done at the receiver side. On requisition from member of a group the crypto-coded data and encrypted secret key in the cloud storage are demodulated, turbo decoded and de-interleaved.

7. Before performing symmetric key algorithm decryption, the secret key of symmetric key algorithm is retrieved from encrypted secret key using asymmetric key algorithm's private key.

8. Now the retrieved secret key is used for decrypting the encrypted data to get the original information.

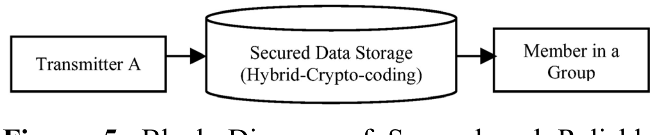


Figure 5. Block Diagram of Secured and Reliable Model for Distributed Data Access

Cloud Computing can provide storage requirements for storing the company's data. The data proprietor stores the information in the cloud for access by the users in the authorized group. The service provider does not assure the whole data security. Data access and its security remain as a great challenge and research is ongoing in cloud security, because the users are outsourcing their sensitive data in the cloud storage provided by the cloud service provider [3, 9, 12-13]. The current techniques use cryptographic algorithms to solve security issues but find difficulty in distributing the secret key.

In the proposed scheme the sensitive data to be placed in the distributed server is crypto-coded then sent via the channel for placing in the storage server. We have proposed to combine both symmetric and asymmetric key algorithms along with channel coding scheme and bring this as Hybrid-Crypto-Coding (HCC) Encoder. The block diagram of the transmitter is shown in Figure 6. This research work aims in handling security issues using the hybrid-crypto-coding technique that ensures access to outsourced data by authorized users only. This work also proposes an enhanced security technique by keeping the secret key in an encrypted format along with the data in the cloud and unlocking the key using the public key for accessing the data by the members in the group. The combined security mechanism is incorporated along with the turbo coder. The simulation run and analysis are demonstrated to prove that the proposed approach is highly reliable and secure.

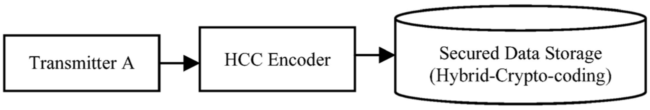


Figure 6. Secured and Reliable HCC framework for Transmitter

Figure 7 shows the HCC framework for the receiver. At the receiver side, when any member in the group has to access the stored data in the distributed storage server, he has to use his private key for unlocking the secret key. The crypto-coded data is retrieved from the storage server. The secret (symmetric) key is used by the HCC decoder for decoding the corrupted crypto-coded data. If the data has been changed in between due to noise, the channel decoding technique helps to minimize the bit error and the decryption algorithm protects the data from being accessed by unauthorized users.

The public key of the recipient helps in locking the authorization key, this provides authentication. Hence, the overall system guarantees security and reliability with additional cost, hardware, and time complexity when compared to traditional schemes that use either channel encoder or encryption.

4 Results and Discussion

Hybrid-Crypto-Coding (HCC) scheme provides data security and reliability than traditional schemes (encoding or encryption only).

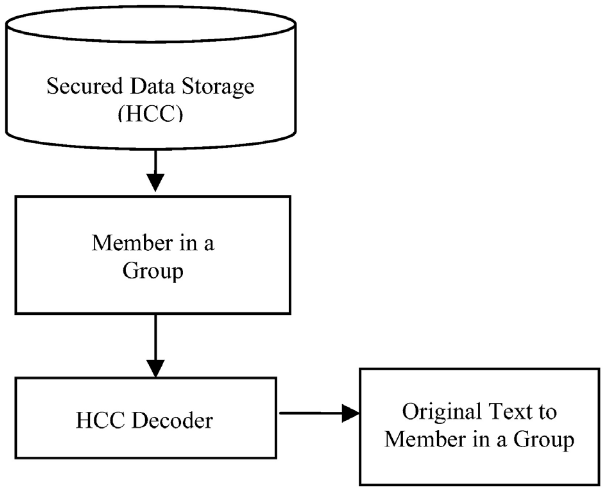


Figure 7. Secured and Reliable HCC framework for Receivers from Distributed Data Storage

The results were simulated using MATLAB version R2015b with computer specifications Intel ® Core ™ i7 – 6500U CPU @ 2.5 GHz, 8GB RAM, and 64- bit operating system. Three different hybrid-crypto-coding schemes DES-RSA, AES-ElGamal, and TDES-Rabin HCC were analyzed for simulation parameters listed in Table 2.

Table 2. Simulation Parameters

Parameter	Value
Input Block size	64, 128, 256, 512
Key size	56, 128, 168
Channel Coding	Turbo Coding
Modulation Techniques	PAM,PSK,QAM
Modulation Order	8PAM,8PSK,16QAM
No. of Iterations in Turbo Decoder	10,15,20
Transmission Channels	AWGN, Rayleigh

4.1 Varying the Input Block Size and Iterations of the Turbo Coder

Figure 8 illustrates BER performance comparison of AES-ElGamal HCC Scheme for different input block sizes and the varied number of iterations in turbo decoder. For 128- bit input block size and number of iterations is 10, BER is 10^{-1} when E_b/N_0 is 10dB. As the number of iterations increases from 10 to 15, BER decreases to 10^{-2} for the same E_b/N_0. There is approximately 1 dB improvement in performance for different input sizes and the number of iterations.

Figure 9 and Figure 10 illustrates BER performance comparison of DES-RSA HCC and TDES-Rabin HCC Schemes respectively for different input block sizes and the varied number of iterations in turbo decoder. The plot with 256 bit and iteration 15 shows better performance compared to other cases. At 10dB BER, in this case, is 10^{-2} than that for 64- bit block size for which BER is 10^{-1}.

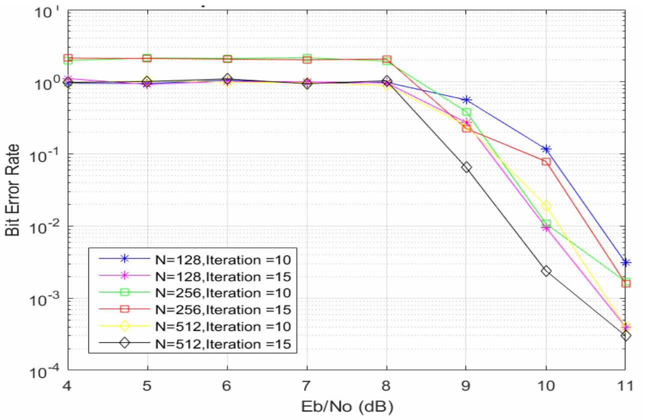


Figure 8. BER Comparison of AES-ElGamal Hybrid-Crypto-Coding Scheme for different input block size and iterations in turbo decoder

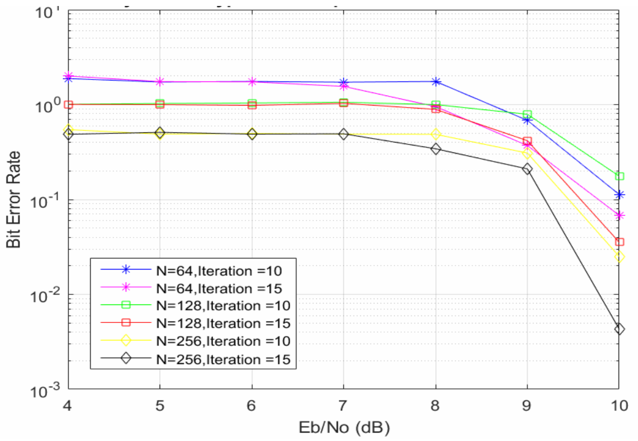


Figure 9. BER Comparison of DES-RSA Hybrid-Crypto-Coding Scheme for different input block size and iterations in turbo decoder

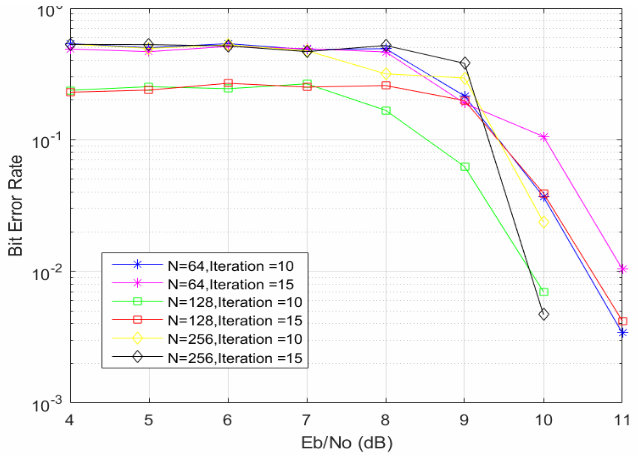


Figure 10. BER Comparison of TDES-Rabin Hybrid-Crypto-Coding Scheme for different input block size and iterations in turbo decoder

4.2 Interleaving the Input Block Before Encryption and After Encryption

In all the three HCC cases, the BER Vs SNR plots Figure 11, Figure 12 and Figure 13, show considerable variation in values due to the impact of HCC techniques. It is observed that interleaving after encryption shows a reduction in BER values compared to encryption after interleaving. In DES-RSA and TDES-Rabin schemes, for E_b/N_0 11dB, BER is approximately 10^{-2} when interleaving is done before encryption and BER is approximately 10^{-3} when interleaving is done after encryption.

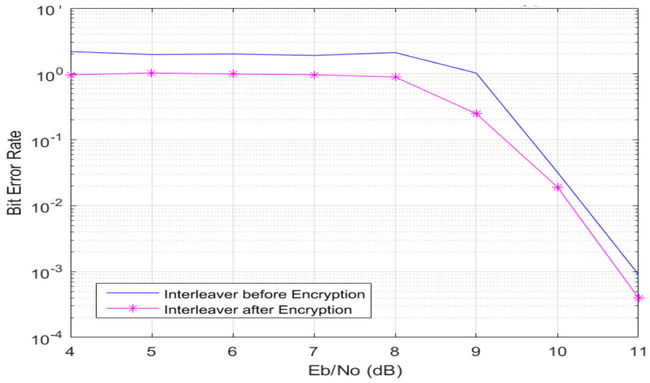


Figure 11. BER Comparison of AES-ElGamal Hybrid-Crypto-Coding Scheme interleaving input block before and after encryption

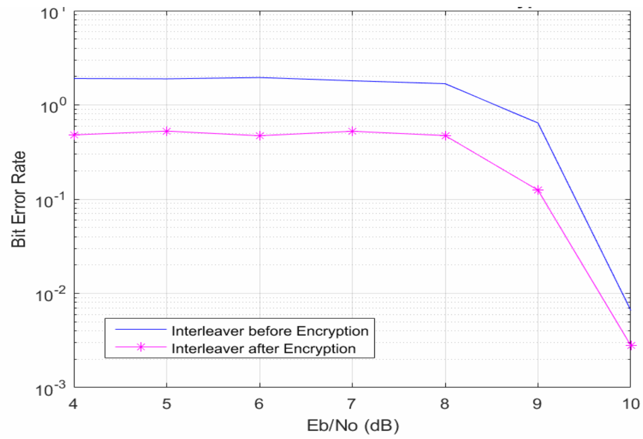


Figure 12. BER Comparison of DES-RSA Hybrid-Crypto-Coding Scheme interleaving input block before and after encryption

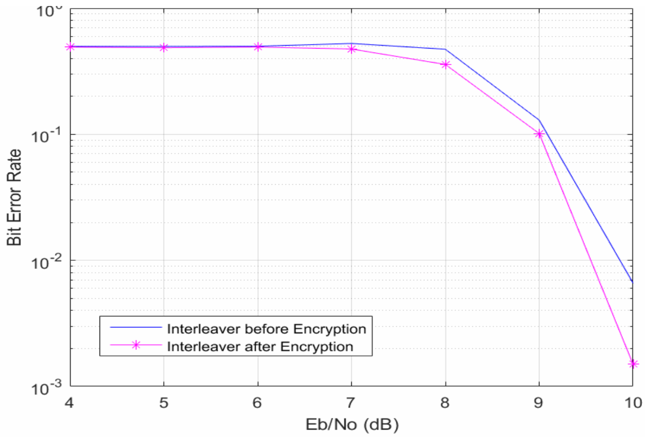


Figure 13. BER Comparison of TDES-Rabin Hybrid-Crypto-Coding Scheme interleaving input block before and after encryption

4.3 Transmission of Input Data with Encryption and Without Encryption

Error propagation effects are analyzed in the plots shown in Figure 14, Figure 15, and Figure 16. When hybrid encryption schemes alone are applied the BER value is larger than the case when no encryption scheme is applied. This is due to the fact that when encryption schemes are applied, error in few initial bits affects the rest of the transmitted bits which imply error propagation. In all the three cases, to avoid error propagation, channel coding has to be done along with encryption to provide security and reliability. Figure 15 and Figure 16 show that there is a need for 0.8 dB excess SNR for achieving the same BER of 10^{-2}.

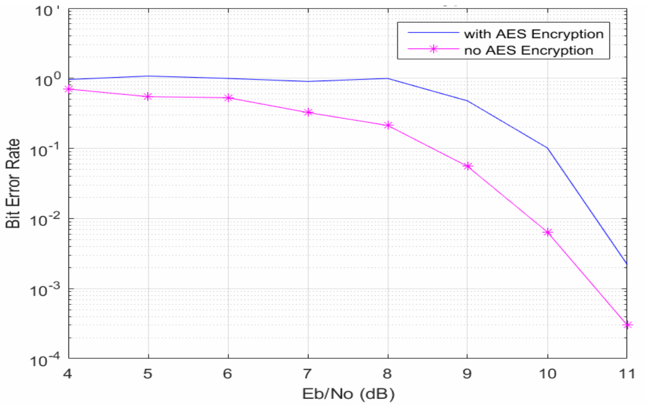


Figure 14. BER Comparison of AES-ElGamal Hybrid Encryption Scheme

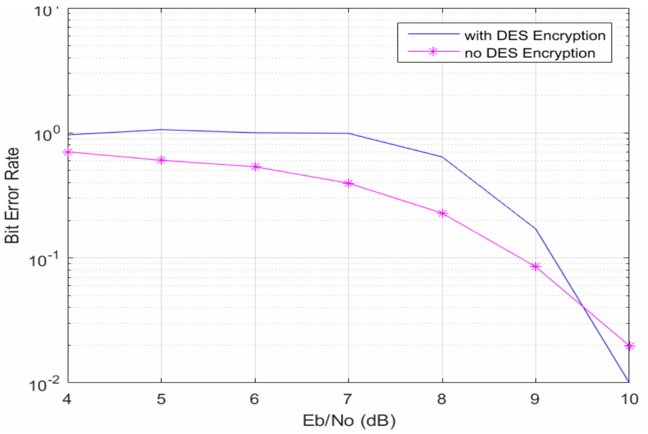


Figure 15. BER Comparison of DES-RSA Hybrid Encryption Scheme

4.4 Transmitting the Input Data with and Without Interleaving

When data is transmitted through a noisy channel there is always large BER. When an additional interleaving is done after encryption and before channel coding, additional security can be provided but BER increases from 10^{-2} to 10^{-1} for SNR 11dB. Figure 17, Figure 18 and Figure 19 show that by increasing 1 dB of SNR, security can be increased with almost the same BER for all the three schemes.

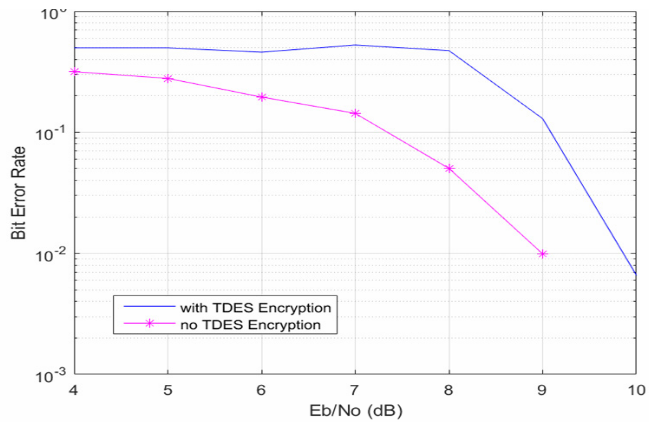


Figure 16. BER Comparison of TDES-Rabin Hybrid Encryption Scheme

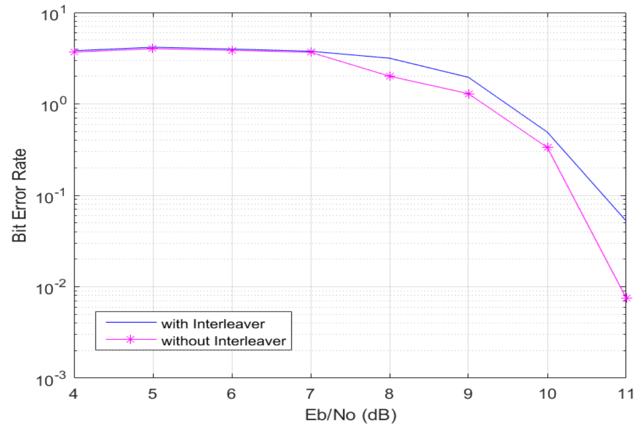


Figure 17. BER Comparison of AES-ElGamal Hybrid Scheme with and without Interleaver

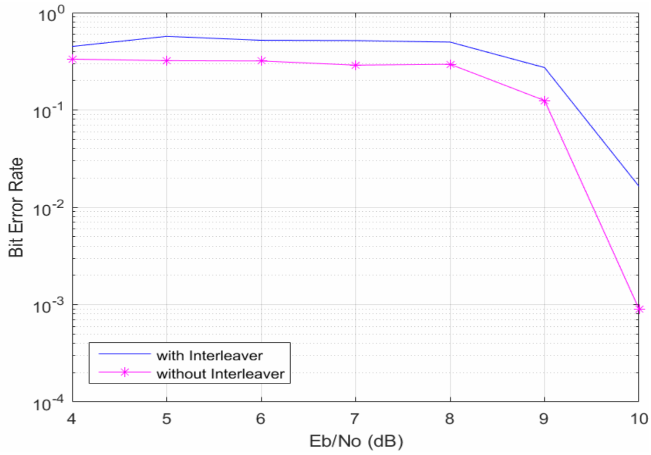


Figure 18. BER Comparison of DES-RSA Hybrid Encryption Scheme with and without Interleaver

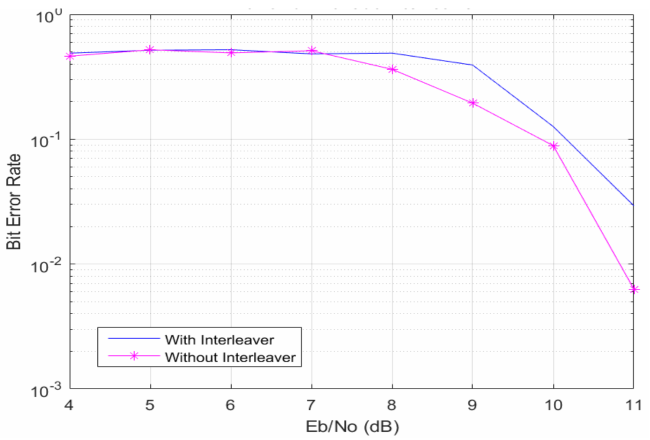


Figure 19. BER Comparison of TDES-Rabin Hybrid Encryption Scheme with and without Interleaver

4.5 Transmitting the Input Data with and Without Encryption and Turbo Coding

When data is transmitted through an unreliable and unsecured channel there is always large BER. The plots are shown in Figure 20, Figure 21 and Figure 22 indicate that BER is 10^{-1} for SNR 10dB and it decreases to 10^{-2} when the data is coded and encrypted for all three schemes.

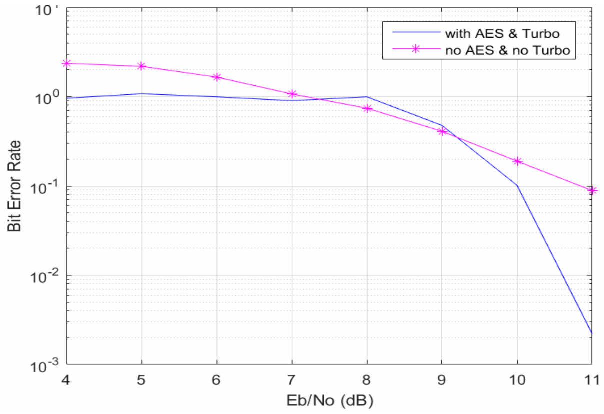


Figure 20. BER Comparison of unencrypted uncoded data with AES Encryption Scheme

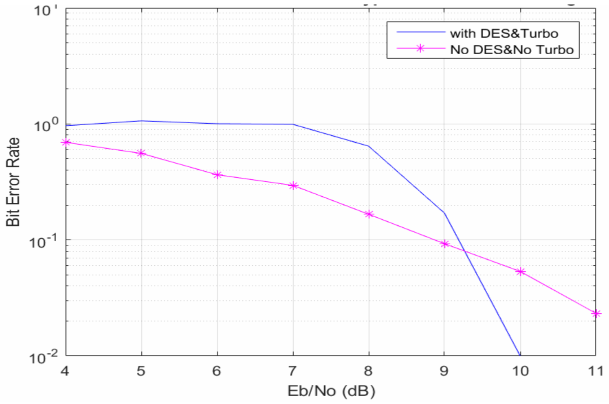


Figure 21. BER Comparison of unencrypted uncoded data with DES Encryption Scheme

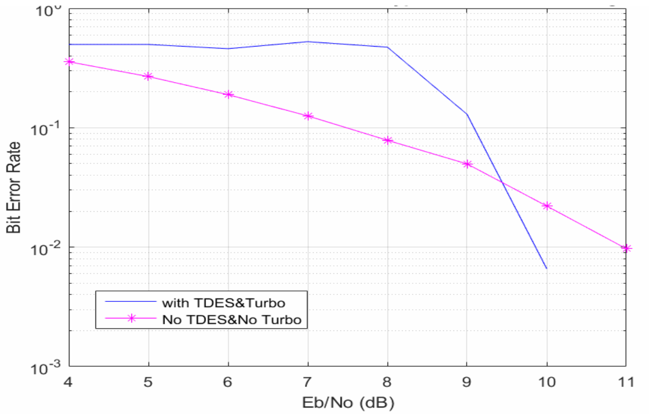


Figure 22. BER Comparison of unencrypted uncoded data with TDES Encryption Scheme

4.6 BER Comparison of HCC Schemes for Different Modulation Techniques

BER performance on different digital modulation techniques 8 PAM, 8 PSK, 16 QAM, and input block lengths N= 128 and N=256 were studied for the three pairs of HCC schemes. The simulation graphs Figure 23, Figure 24 and Figure 25 show that 16 QAM with input block size N=256 bits has the lowest BER of 10^{-3} at SNR 11dB.

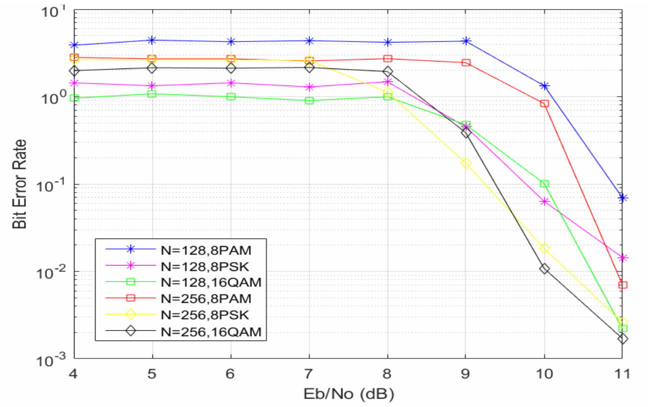


Figure 23. BER Comparison of AES-ElGamal HCC Scheme for different modulation techniques

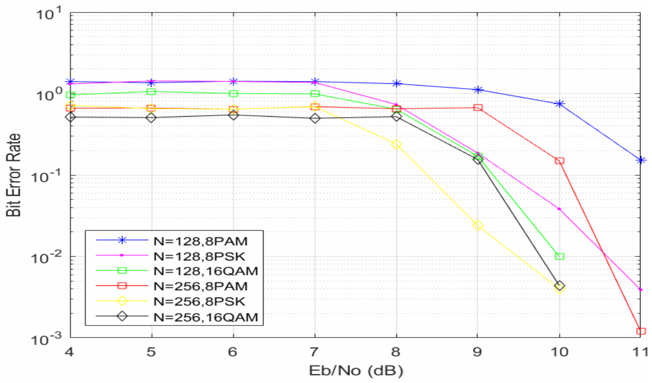


Figure 24. BER Comparison of DES-RSA HCC Scheme for different modulation techniques

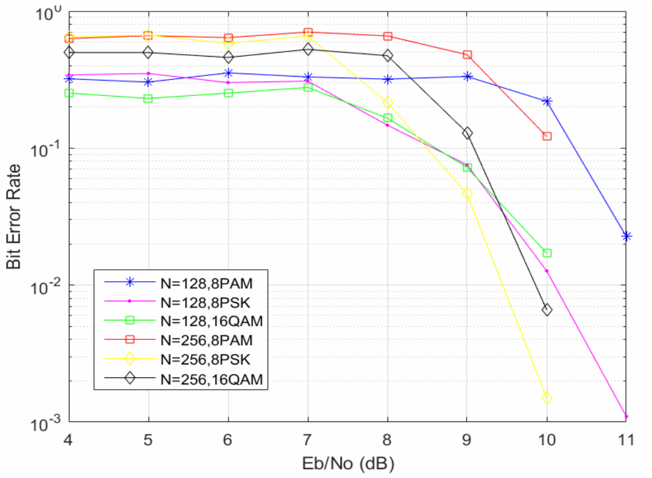


Figure 25. BER Comparison of TDES-Rabin HCC Scheme for different modulation techniques

This suggests that by using higher levels of modulation too, lower BER and security can be achieved for all the three HCC schemes.

4.7 BER Comparison of HCC Schemes for Different Channel Conditions

The simulation was tested for a secured and reliable transmission of data in the Additive White Gaussian Channel (AWGN) channel and Rayleigh channel. The results in Figure 26, Figure 27 and Figure 28 show that the transmissions through the Rayleigh channel prove to be comparatively poor in performance than that of the AWGN channel. The channel performance was studied with modulation technique 8 PSK.

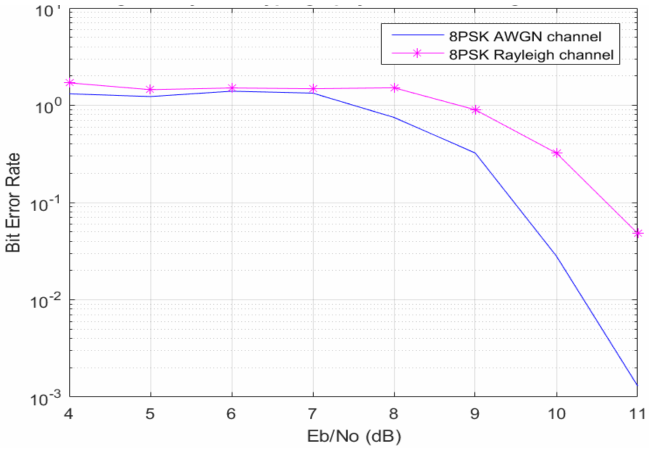


Figure 26. BER Comparison of AES-ElGamal HCC Scheme for different channel conditions

5 Implementation and Testing

The dataset was tested in the machine with the specifications, Intel® Core™ i5-4460 CPU @ 3.20GHz × 4; GPU: GeForce GTX 750 Ti/PCIe/SSE2; 64-bit operating system, 1TB memory space. Figure 29 shows the block diagram of the implementation model.

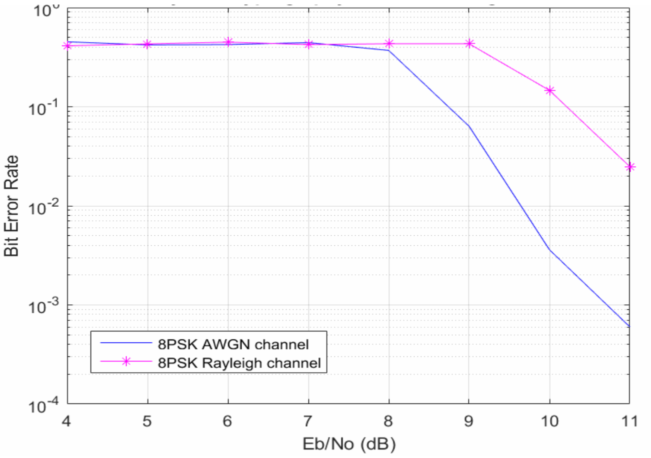


Figure 27. BER Comparison of DES-RSA HCC Scheme for different channel conditions

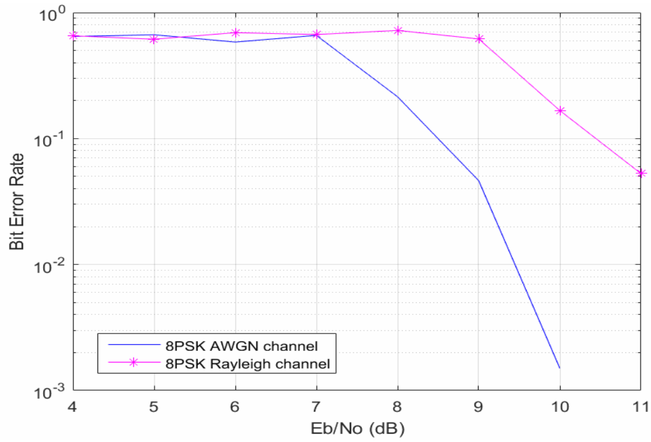


Figure 28. BER Comparison of TDES-Rabin HCC Scheme for different channel conditions

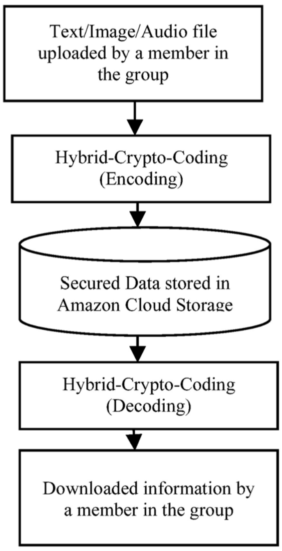
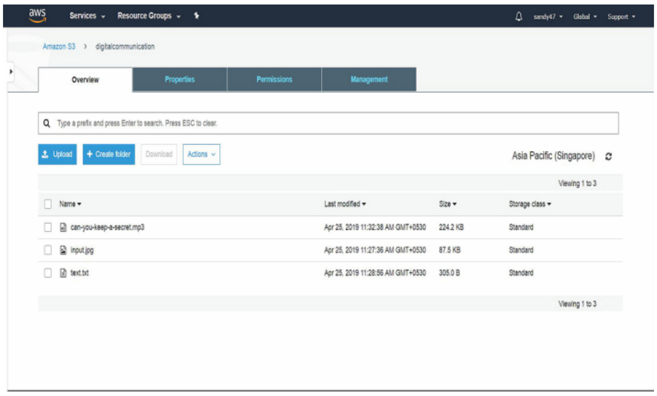

Text/Image/Audio file uploaded by a member in the group
Hybrid-Crypto-Coding (Encoding)
Secured Data stored in Amazon Cloud Storage
Hybrid-Crypto-Coding (Decoding)
Downloaded information by a member in the group

Figure 29. Testing Model in AWS Storage

The crypto-coding scheme was implemented and tested in AWS cloud storage, Python programming was used to perform hybrid-crypto-coding scheme. The data were tested for three different data types – text, image, and audio files. The sample test data are shown below. The screenshot of the testing environment is shown in Figure 30.



Name	Last modified	Size	Storage class
can-you-keep-a-secret.mp3	Apr 25, 2019 11:32:38 AM GMT+0530	224.2 KB	Standard
input.jpg	Apr 25, 2019 11:27:36 AM GMT+0530	87.5 KB	Standard
text.txt	Apr 25, 2019 11:28:56 AM GMT+0530	305.0 B	Standard

Figure 30. Testing in AWS Storage

The tested result for text in the AWS cloud storage is as shown in the following:

Text:

Input Text: Science is a beautiful gift to humanity we should not distort it

Output Text: Science is a feautiful gift to humanity we should`nou dhs_ort i

Image:

Figure 31 and Figure 32 show the uploaded and downloaded images to and from the AWS cloud storage.

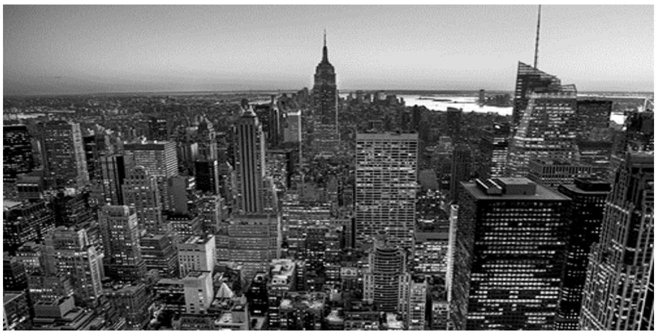


Figure 31. Input image to AWS Storage Server

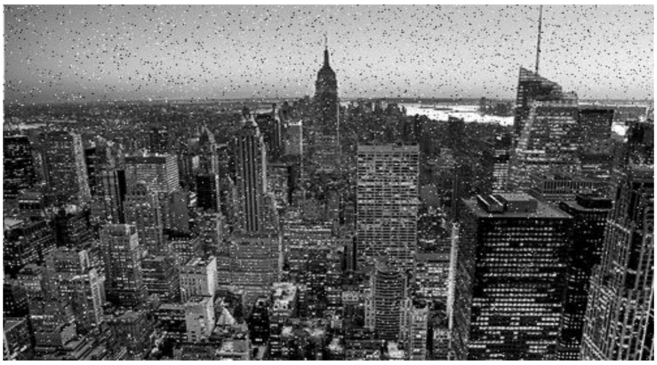


Figure 32. Output image from AWS Storage Server

The distortion in the output is not handled for testing HCC in AWS. Table 3 shows the time taken for uploading and downloading the tested data to and from the cloud.

Table 3. Uploading & Downloading time to/from the cloud

Input Type	Time in channel and sending to cloud in seconds	Time to download data from cloud in seconds
Image	454	1.48
Text	0.1312	1.38
Song	1600.022	1.78

6 Comparison of HCC Techniques

The computational complexity of all three proposed schemes is compared based on time complexity. The results are simulated in MATLAB R2015b and tabulated in Table 4. Figure 33 proves that the AES-ElGamal scheme is better than the other two hybrid schemes.

Table 4. Time complexity analysis of HCC schemes

Type of HCC Scheme on Data	Input size in bits	Time in Sec
AES-Elgamal Hybrid-crypto-coding scheme	64	11
	128	20
	256	33
	512	52
DES-RSA Hybrid-crypto-coding scheme	64	16
	128	25
	256	48
	512	83
TDES-Rabin Hybrid-crypto-coding scheme	64	28
	128	43
	256	102
	512	162

Table 5 shows the analysis of time taken for the execution of the algorithm by the three pairs of hybrid-crypto-coding schemes for input size **n=128** when compared to other traditional schemes.

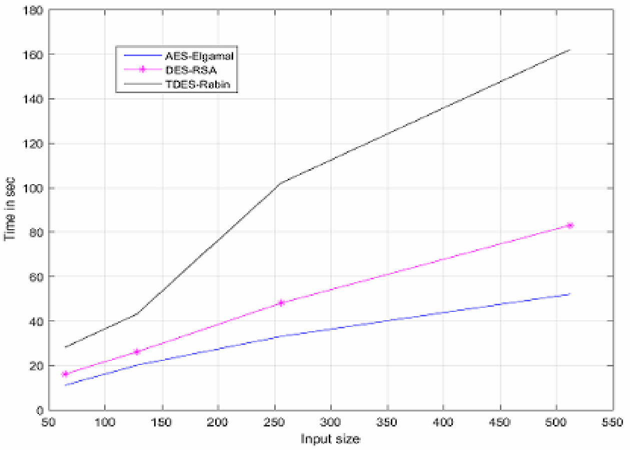


Figure 33. Time Complexity Analysis of HCC schemes

Table 5. Comparison table of HCC schemes with other schemes

Hybrid-crypto-coding pair	Both encryption & encoding done (Time in sec)	Only encryption done (Time in sec)	Only Hybrid Encryption (Time in sec)	Only encoding done (Time in sec)
AES-Elgamal	20	8	12	5.2
DES-RSA	26	14	19	4.8
TDES-Rabin	43	24	36	5.1

From Table 5, we can conclude that only if encryption and encoding are done together the algorithm shows an optimized performance with respect to time for guaranteeing security and reliability.

Table 6 and Table 7 show a brute force attack on all three HCC schemes using MATLAB and Python simulations respectively.

7 Conclusion

The simulated results from Figure 8 to Figure 28 show that hybrid cryptography along with interleaver before channel coder will be a better approach to defend well in an unsecured and noisy channel.

Table 6. Brute force attack on Hybrid-Crypto-Coding Security

Type of Encryption on Data	Time Complexity in terms of number of executions per second	Brute force Attack on Security if key is unknown
Channel Coding only	5.278	0
Secured channel coding with DES only	7.556	2.3 months
Secured channel coding with AES only	7.322	2.3 months
Secured channel coding with Triple DES only	7.317	9.34 century
Secured channel coding with DES and key encrypted with RSA	8.231	2.3 months
Secured channel coding with AES and key encrypted with ElGammal	12.555	2.3 months
Secured channel coding with Triple DES and key encrypted with Rabin	12.549	9.34 century

Table 7. Comparative study of Hybrid-Crypto-Coding Techniques

Symmetric Algorithm for Data Encapsulation	Asymmetric Algorithm for Key Encapsulation	Data Size in bits	Key Size in bits	No. of rounds	Speed in sec	Brute force attack on Security
AES	ElGamal	128	128, 192 or 256	10, 12, 14	High 20.8 (avg.)	Years
DES	RSA	64	56	16	Low 197	Days
TDES	Rabin	192	168	48	Mod-erate 91.2	Centuries

The Hybrid-Crypto-Coding schemes prove to provide strong security when implemented for distributed data centers. The BER against SNR plots of the AES-ElGamal Hybrid Encryption pair shows that it is a better candidate to provide security in wireless communication networks.

As there are key-synchronization and key sharing problems, at distributed data centers, symmetric key encryption techniques cannot defend alone for providing security, instead hybrid schemes are preferred so as to combine the advantage of symmetric and public key techniques. Asymmetric key encryption techniques are always advantageous than symmetric key encryption techniques as one of the keys can be held secret by the customer and only public keys are maintained in the registry. These public keys are shared with the intended person in the group by the Trusted Third Party.

Acknowledgements

We would like to acknowledge **Sindhumathi Rasappan,** Engineer R & D at Vinwares.com and **Sandeep Kumar**, B.E. (ECE), Sri Venkateswara College of Engineering, for their support in MATLAB and Python Programming.

References

[1] T. J. Jeyaprabha, G. Sumathi, P. Nivedha, Smart and Secure Data Storage using Encrypt-interleaving, *IEEE International Conference on Innovations in Power and Advanced Computing Technologies – iPACT*, Vellore, India, 2017, pp. 1-6.

[2] S. O. Kuyoro, F. Ibikunle, O. Awodele, Cloud Computing Security Issues and Challenges, *International Journal of Computer Networks*, Vol. 3, No. 5, pp. 247-255, 2011.

[3] J. W. Rittinghouse, J. F. Ransome, *Cloud Computing – Implementation, Management, and Security*, CRC Press, 2010.

[4] M. Sharma, H. Bansal, A. K. Sharma, Cloud Computing: Different Approach & Security Challenge, *International Journal of Soft Computing and Engineering (IJSCE)*, Vol. 2, No. 1, pp. 421-424, March, 2012.

[5] P. Arora, R. C. Wadhawan, E. S. P. Ahuja, Cloud Computing Security Issues in Infrastructure as a Service, *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 2, No. 1, pp. 1-7, January, 2012.

[6] M.-S. Kim, J.-K. Lee, J. H. Park, J.-H. Kang, Security Challenges in Recent Internet Threats and Enhanced Security Service Model for Future IT Environments, *Journal of Internet Technology*, Vol. 17, No. 5, pp. 947-955, September, 2016.

[7] S. Subashini, V. Kavitha, A Survey on Security Issues in Service Delivery Models of Cloud Computing, *Journal of Network and Computer Applications*, Vol. 34, No. 1, pp. 1-11, January, 2011.

[8] U. A. Idris, J. Awwalu, B. kamil, Security Threat on Cloud Computing, *International Journal of Computer Trends and Technology*, Vol. 37, No. 1, pp. 18-21, July, 2016.

[9] V. J. R. Winkler, *Securing the Cloud: Cloud Computer Security Techniques and Tactics Syngress*, 2011.

[10] A. S. Parveen, C. R. Suganya, Information Security through Normalization in Cloud Computing, *International Journal of Scientific & Research Publications*, Vol. 2, No. 5, pp. 1-6, May, 2012.

[11] W. A. Jansen, Cloud Hooks: Security and Privacy Issues in Cloud Computing, *Proceedings of the 44th Hawaii International Conference on System Sciences*, Hawaii, HI, USA, 2011, pp. 1-10.

[12] W. Liu, Research on Cloud Computing Security Problem and Strategy, *2nd International Conference on Consumer Electronics, Communications and Networks*, Hubei, China, 2012, pp. 1216-1219.

[13] S. Ramgovind, M. M. P. Eloff, E. Smith, The management of security in Cloud computing, *IEEE Conference on Information Security for South Africa*, Johannesburg, South Africa, 2010, pp. 1-7.

[14] A. Alrehaili, A. Mir, M. Junaid, A Retrospect of Prominent Cloud Security Algorithms, *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, Vol. 9, No. 3, pp 749-755, January, 2020.

[15] D. Arivazhagan, R. Kirubakaramoorthi, Develop Cloud Security In Cryptography Techniques Using DES-3L Algorithm Method In Cloud Computing, *International Journal of Scientific & Technology Research*, Vol. 9, No. 1, pp. 252-255, January, 2020.

[16] S. Balamurugan, S. Pande, Data Security and Cryptography in Cloud Environment, *International Journal of Engineering Research and Technology*, Vol. 4, No. 6, pp. 1012-1018, June, 2015.

[17] A. Payandeh, M. Ahmadian, M. R. Aref, A Secure Error-Resilient Lossless Source Coding Scheme Based on Punctured Turbo Codes, *Iranian Journal of Electrical and Computer Engineering*, Vol. 5, No. 1, pp. 19-23, Winter-Spring, 2006.

[18] T. J. Jeyaprabha, G. Sumathi, Security Enhancements at Distributed Data Centers Using Turbo Codes, *Compusoft Journal*, No. Special Issue, May, 2016.

[19] G. M. Kraidy, On Progressive Edge-Growth Interleavers for Turbo Codes, *IEEE Communications Letters*, Vol. 20, No. 2, pp. 200-203, February, 2016.

[20] T. J. Jeyaprabha, G. Sumathi, Cloud Bottlenecks – A Survey on Security Issues, Challenges and Techniques, *International Journal of Applied Engineering Research*, Vol. 9, No. 23, pp. 21851-21862, 2014.

[21] S. A. Khan, R. K. Aggarwal, S. Kulkarni, Encryption Schemes of Cloud Computing: A Review, *5th IEEE International Conference on Advanced Computing & Communication Systems*, Coimbatore, India, 2019, pp. 1-4.

[22] C. M. Stuart, Nandan S., Deepthi P. P., Low Complex Crypto based Channel Coding with Turbo Code, *International Journal of Computer Applications*, Vol. 61, No.16, pp. 39-44, January, 2013.

[23] K. V. Pradeep, V. Vijayakumar, V. Subramaniyaswamy, An Efficient Framework for Sharing a File in a Secure Manner Using Asymmetric Key Distribution Management in Cloud Environment, *Journal of Computer Networks and Communications*, Vol. 2019, Article ID 9852472, June, 2019.

[24] C. Berrou, A. Glavieux, P. Thitimajshaima, Near Shannon limit Error-correcting Coding and Decoding: Turbo-codes, *in Proc. IEEE International Conference on Communications*, Geneva, Switzerland, 1993, pp. 1064-1070.

[25] S. Benedetto, D. Divsalar, G. Montorsi, F. Pollara, A Soft-Input Soft-Output Maximum *A Posteriori (MAP) Module to Decode Parallel and Serial Concatenated Codes*, TDA Progress Report 42-127, November, 1996.

[26] K. M. Bogawar, S. Mungale, M. Chavan, Implementation of turbo encoder and decoder, *International Journal of Engineering Trends and Technology*, Vol. 8, No. 2, pp. 73-76, February, 2014.

[27] F. Idrizi, I. Ninka, Analyzing the use of combined cryptography for increasing the security of information, *International Journal of Scientific & Engineering Research*, Vol. 4, No. 8, pp. 969-972, August, 2013.

[28] M. U. Bokhari, Q. M. Shallal, Evaluation of Hybrid Encryption Technique to Secure Data during Transmission in Cloud Computing, *International Journal of Computer Applications*, Vol. 166, No. 4, pp. 25-28, May, 2017.

[29] V. Kaur, A. Singh, Review of Various Algorithms used in Hybrid Cryptography, *International Journal of Computer Science and Network*, Vol. 2, No. 6, pp. 157-173, December, 2013.

[30] E. P. Shaikh, S. Patil, Performance Evaluation of Hybrid Cryptography System, *International Journal of Engineering Trends and Technology (IJETT)*, Vol. 54, No. 4, pp. 255-263, December, 2017.

[31] A. K. Koundinya, Abhijith C., Arunraj, Deekshith N., Srinath N. K., J. Abraham, Performance Analysis of Hybrid Cryptographic Algorithm- A^{3}D Algorithm, *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 4, No. 5, pp. 8961-8968, May, 2016.

Biographies

T. J. Jeyaprabha, received her B.E. degree in Electronics and Communication Engineering from Mepco Schlenk Engineering College, Madurai Kamaraj University, Madurai during 1997, M.E. degree in Communication Systems from Sri Venkateswara College of Engineering, Anna University, Chennai during 2006 and currently pursuing PhD in Information & Communication Engineering, Anna University, Chennai since 2013. Her research areas of interest are Wireless Communication, Networks & Security.

G. Sumathi, obtained her B.E. degree in Electronics and Communication from Bharathidasan University, M.E. degree in Computer Science and Engineering and PhD in Computer Science and Engineering from National Institute of Technology, Tiruchirappalli. Her research interest includes Distributed Computing and Computer Networks.