HYBRID CRYPTOGRAPHY-BASED SECURE AND EFFECTIVE DATA CONFIDENTIALITY, VALIDATION, AND RELIABILITY SYSTEMS

[1]V.Ranjini, [2]S.G.Reethigaa, [3]. Mrs..M.Geetha
[1] II MCA, Paavai Engineering College, Namakkal
[2] II MCA, Paavai Engineering College, Namakkal
[3] Professor, Department of MCA, Paavai Engineering College, Namakkal

Abstract : In today's world, information security is one of the most important and pressing issues. Numerous cryptographic algorithms are used today to safeguard information transmission across unreliable channels. But both symmetric and asymmetric encryption methods now in use have a large number of possibilities. The key exchange is the main issue with symmetric encryption methods, however encryption has always had this issue. Even though key exchange is straightforward, extended encryption times and asymmetric algorithms pose serious issues. Now, to overcome these flaws, a hybrid model is given in this research that uses a combination of symmetric and asymmetric cryptographic approaches to provide extra security with reduced key maintenance and encryption time. In this hybrid model, a digital envelope is also included that incorporates all of this to transfer them securely over the network and achieve the embryonic security services of integrity, confidentiality, and authentication by encompassing message digest, symmetric encryption, and digital signature, respectively.

Keywords : Cypher Text, Encryption,Decryption,Public key and Private Key

1. INTRODUCTION

A hybrid paradigm, which combines symmetric and asymmetric cryptographic algorithms with digital signatures, is used in this proposed work. This model's improved hybrid cryptographic approach provides a safe environment with fewer resource consumption.

Mixed-mode cryptosystem This cryptosystem is a hybrid of symmetric and asymmetric algorithms that offers extreme security with minimal key maintenance.

strategies for encrypting data that combine the benefits of cryptography with its drawbacks. Sharing of the secret key is a difficulty that comes with symmetric cryptography despite the fact that it is faster than asymmetric encryption.

Message Digest: A message digest is a type of cryptographic hash algorithm that utilises one-way hashing to generate a string of alphanumeric characters. In order to perceive alterations to any part of a message, message digests try to maintain the integrity of the message. A certain data volume is assigned a distinct message digest. These numbers come from algorithms.

Asymmetric encrypted hash numbers are used to create a digital signature. It is used to authenticate messages and documents since it is the digital counterpart of a handwritten signature. The hash numbers are encrypted using a private key to form the digital signature

Only the advantages of symmetric and asymmetric cryptography are included in this hybrid architecture. The sender's side user's private key is used in symmetric key encryption to give the hybrid system confidentiality and effective performance. All other outdated public key cryptographic encryption techniques are significantly slower than symmetric key encryption. One-way hashing is used to produce a message digest of the input message, which must correspond with the message digest of the recovered message from the receiver's side of the decryption process, in order to reduce the integrity of the input message. If the message digests do not match, it indicates that the integrity of the channel was broken when the initial message was interrupted. A digital

signature that authenticates the intended receiver is produced by encrypting the hash value of the input message using the private key of the public key cryptography technique. A digital envelope is used to obtain assurance over the channel and includes a digital signature, an encrypted input message, and the symmetric key technique's double-encrypted private key.

2. LITERATURE SEARCH

In the earlier search, depiction of understanding on some exploration papers of various cryptographic methodologies is utilized for getting the data from the dishonest organizations.

This clever strategy enciphers the picture and embeds the advanced mark into the picture. A computerized mark is a strategy used to achieve respectability of information, advanced records, programming and underwrite the genuineness. Pictures are all around respected to cover objects utilized in steganography which is likewise an encryption technique. Here, the Java philosophy is wanted to prove the presentation of the proposed model in conditions of key length, scrambled message length, message length, encryption time and decoding time [1].

This paper points on security upgrading by working fair and square of encryption in channel. This study's principal objective is to uncover the meaning of safety in net-work and give the upgraded encryption procedure to by and by carried out encryption techniques. In this examination, the creator has extended a blend of MD5, RSA and DSA as a combination connect for remote gadgets and furthermore determined a contextual investigation for MANET networks reasonable to propose the calculation's applications [2].

In this paper, another security convention is intended to work on the strength of safety calculations for online exchange utilizing gathering of both symmetric and unbalanced cryptographic procedures and offers three cryptographic administrations like confiden¬tiality, honesty and validation. These administrations are vanquished by utilizing elliptic bend cryptography (ECC) (for encryption), message digest (MD5) (for uprightness) and double RSA cryptographic technique (for validation) [3].

This study alludes to a few parts of cryptographic strategies and many issues connected with cryptography. The proposed work is screening a portion of the pivotal issues of cryptography alongside their answers. DES cryptographic strategy is utilized for encryption reasons, and RSA is utilized for symmetric and hilter kilter cryptography procedures; additionally, hash technique (SH1) is utilized in this paper [4].

In this paper suggest figure conspire that propels the Diffie — Hellman key exchange by involving shortened polynomial in discrete logarithm issue to rises the intricacy of this plan over the perilous channel, additionally adding the MD5 hashing calculation, the AES symmetric key procedure and the Modification of Diffie — Hellman (MDH) uneven key strategy [5].

Diffie — Hellman is revised to offer verification and evade antiquated root generation stage to accomplish speed and confirmation to escape key trade with an unauthenticated administrator. In this paper, half breed cryptography game plan is proposed to achieve secret message trade. RSA utilizes any superb figures P and Q which increased a get esteem N is shared to the collector side [6].

This paper concentrated as the data security can be deciphered into three key natives: trustworthiness, accessibility, and information wellbeing. In this work, present their productivity by looking at the few sorts of cryptographic calculations and by showing their defects and resources. To upgrade the benefits of the crypto strategies, we propose a half-breed strategy that chains three cryptographic methodologies [7].

Secure Electronic Medical Records (SEMR), which aspirations of conveying a few offices which will offer safeguarded and skilful access of the EMRs to specialists, experts and patients. In this desk work, the creator proposes an execution of a half-breed model that joins the MD5 hashing calculation, AES symmetric key calculation and HECC deviated key calculation in the computerized envelope. The result exhibits the best substitute computerized envelope half and half cryptographic-based framework for EMR [8]. Due to the existence of great computing stimuli processors which is building varied circumstances for secret key encryption with the smaller size of the key since dispersed computation methods can break smaller size of key simple. The exchange of keys in the secret key encryption method across

an unsafe network presents even another challenge. The use of an asymmetrical method has the drawback of a slow encryption process. All widely used symmetric encryption methods are considerably slower than any secret key encryption method. When there is a lot of information, public key cryptography is not practical. To address these issues, numerous hybrid prototypes are created.

3. METHODOLOGY

The archaic cryptography system essentially involves two parties agreeing to exchange a secret key and keep it privately between them. If they are spread out, they will need to rely on a dispatcher or other secure means of communication to prevent the transmission of the secret key. Anyone who intercepts the key while it is being used to encrypt or authenticate information can later read or modify it.

The challenge with cryptographic systems is that they cannot solve the whole issue at once, unlike confidentiality, integrity, and authentication. Because of the need for increased protection, an intruder can easily infiltrate a system, and brute force attacks can happen with ease.

The suggested model's primary objective is to achieve the fundamental objectives of cryptography, namely authentication, integrity, and confidentiality. Utilizing a combination of cryptographic techniques to improve the functionality of antiquated cryptographic security procedures, a reliable, secure hybrid model will be put into practise. In the suggested paradigm, the message data is symmetrically encrypted (achieving confidentiality), digital signatures serve as authentication, comparing the hash values serves as integrity, and a digital envelope offers further network protection.

Encryption

1. To create cypher text, symmetric key (Ksym) encryption is performed on plain text (PT) (CT).
2. A one-way hashing algorithm (mathematical hash function) is used to create a message digest (fixed length numbers), which is then encrypted with the sender's private key (Kpri(s)) to create a digital signature (DS).
3. To create a doubly encrypted symmetric key, symmetric key (Ksym) is first encrypted using the sender's private key (Kpri(S)), and then this encrypted symmetric key (ESK) is encrypted using the receiver's public key (Kpub(R)) (DESK).
4. To transport three CT, DS, and DESK through the channel, a digital envelope (DE) is created.

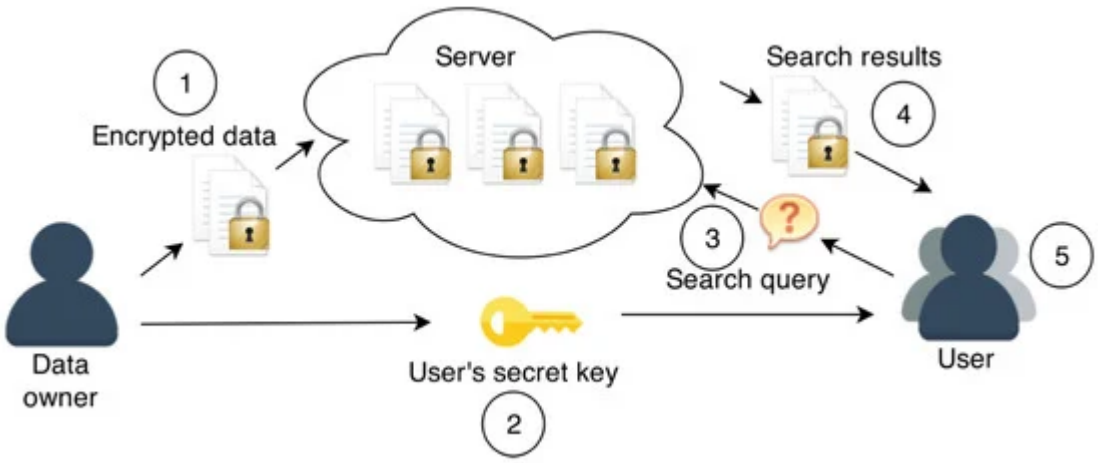

Figure 1 : Encryption and Decryption

Decryption

1. The channel's incoming digital envelope (DE) was composed of CT, DESK, and DS.
2. The final symmetric key is obtained after further encrypting the double encrypted key with the sender's public key and the receiver's private key.
3. The cypher text (CT) is converted to plain text using this symmetric key. Using a hashing method, this plain text (PT) is transformed into a message digest and obtained .
4. To retrieve the message digest, the digital signature is obtained from the digital envelope and decrypted using the sender's public key .
5. Message digest and message digest are compared . Uncorrupted plain text (UPT) is obtained if both are identical, while corrupted plain text (CPT) is acquired if neither are.

Encryption an Decryption model showed in Figure 1.

4. RESULTS AND CONCLUSION

In comparison to systems based on traditional cryptography methods, this hybrid paradigm delivers an effective, intrinsically safe, and excessively performant cryptographic system. Additionally, this methodology will encrypt data more quickly than conventional public key cryptography approaches and provide better key maintenance than other antiquated symmetric key techniques. The key results of this approach are enhanced network confidence as well as crucial security services like confidentiality, integrity, and authentication. The need for efficient, automated, dominant, and risk-reducing ways to manage and protect keys over the course of their lifetime is excessive given today's modest and digitalized environment, which is becoming increasingly threatened by financially motivated hackers and disgruntled employees. As a result, access must be restricted to only authorised users. A strong hybrid cryptosystem, combined with an authentication-based management system, and a safe key encryption-based system, are proposed to ensure the achievement of key security goals.

References

1. S. Sharma, V. Kapoor, A novel approach for improving security by digital signature and image steganography. Int. J. Comput. Appl. **171(8)** (2017)
2. K. Kaur, E. Seema, Hybrid algorithm with DSA, RSA and MD5 encryption algorithm for wireless devices. Int. J. Eng. Res. Appl. (IJERA) 2(5) (2012)
3. S. Subasree, N.K. Sakthivel, Design of a new security protocol using hybrid cryptographic algorithm. IJRRAS 2(2) (2010)
4. D.V. Kapoor, R. Yadav, A hybrid cryptography technique to support cyber security infrastructure. Int. J. Adv. Res. Comput. Eng. Technol. 4(11) (2015)
5. A.M. Rahma, R.N. Farhan, H.J. Mohammad, Hybrid model for securing E-commerse transaction. Int. J. Adv. Eng. Technol. Nov 2011. © IJAET 14 1(5), 14-20
6. S. Deshmukh, R. Patil, Hybrid cryptography technique using modified Diffie-Hellman and RSA. Int. J. Comput. Sci. Inf. Technol. (IJCSIT), 5(6) (2014)
7. G. Mateescu, M. Vladescu, A hybrid approach of system security for small and medium enterprises: combining different cryptography technique, in *Proceedings of the 2013 Federated Conference on Computer Science and Information Systems*
8. M. Gobi, K. Vivekanandan, A new digital envelope approach for secure electronic medical records. UCSNS Int. J. Comput. Sci. Netw. Secur. 9(1) (2009)