International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 01, January 2022)

An Improved Method for Securing Data on Network

Jagpal Singh[1], Manoj Saini[2]

[1,2]*Department of Master of Computer Application, Compucom Institute of Information Technology and Mangement, Jaipur, India*

***Abstract*-- Technology is now advancing quickly. Although technology has greatly improved our daily lives, it has also resulted in certain undesirable side effects and crimes. Cybercrimes are one of such heinous crimes. However, because of the enormous safety holes brought forth by the internet's and the web's quick development, cybercrime now exists everywhere. Cybersecurity offers tools for defending the user against a variety of dangers with the right algorithms. In this research, we propose a novel HDES (Hybrid Encryption Algorithm) to improve the security of user data by combining the advantages of the two most widely used encryption algorithms, AES (advanced encryption standard) and DES (data encryption standard). The recently proposed technique is complicated, making it more difficult for hackers to decipher the code. Using the proper decryption procedure, the code can only be cracked by the intended user.**

I. INTRODUCTION

Inrecent years, many applications based on internet are developed such as on-line shopping, internet banking and electronic bill payment etc. To provide data authentication, accountability, privacy, integrity, and availability during such transactions via wired or wireless public networks, end-to-end secure connections are required [2]. Most people today use computers, the internet, smartphones, or other modern electronics, but not everyone is aware of cyber security. The most important aspect of employing any technological equipment is safeguarding the network against cyberattack. The user's data is protected thanks to a variety of effective algorithms.

In order to increase the security of user data like text, audio, and video, we combine the advantages of the AES and DES algorithms in this study and propose a new method called HDES.Cybercrimeaffectstechnology, digitalinformation and finances a lot in the present. Numerous people, businesses, or banks sustain significant losses as a result of cyber assaults. In terms of business, the cloud computing (CC) technology's secure data transmission characteristic is particularly significant. The goal of the DES (Data Encryption Standard) algorithm is to offer a uniform approach to safeguarding confidential and sensitive commercial data. The Advanced Encryption Standard (AES) method offers excellent speed in addition to security[10, 12]. In this study, we present the HDES algorithm, a more effective method that combines the strengths of both the DES and AES algorithms.

II. CRYPTOGRAPHY

Cryptography is a method of protecting information and communications through the use of codes. The concepts and procedures involved in changing an understandable communication into an unintelligible one (encryption) and then returning that message to its original form (decryption) using a secret code known as keys. So that only the intended audience for the material may read and process it [1]. Encryption algorithms areclassified into two groups: Symmetric key (also called secret-key) and Asymmetric-key (calledpublickey) encryption [2].

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 01, January 2022)

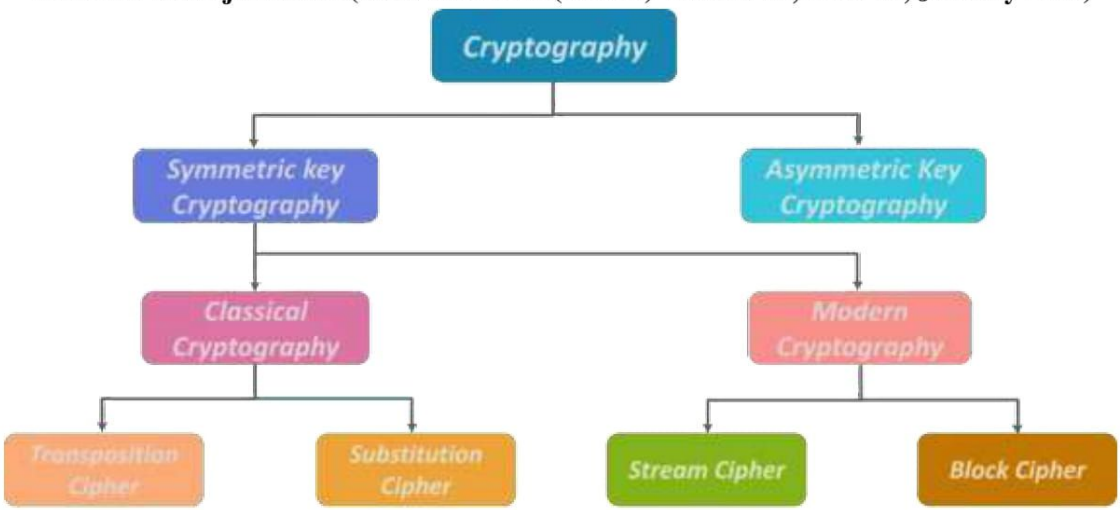

Fig1:Classification of Cryptography

As we've already mentioned, encryption is the process of encrypting data or information to guard against unauthorised access. Different kinds of cryptographic techniques are available.Eachoneofthemservingdifferenttopologyandallprovidesecuretransmitted data throughnetworklinksandensureauthenticationandconfidentiality.All of these end-to-end encryption and decryption algorithms must be implemented in the computer application's physical layer and security layer. The protocol that will be used to transport the traffic must also be taken into account at the same time as specific IP configurations. The graphic above shows us the two models of cypher security classes, known as classical and modern classes.Themostcommonandusedisthemodernclassduetothe dynamicandstaticcryptographytechniques that thistechniquewas deployedwith.Itisknownalsobyits types;

III. PROPOSED ALGORITHM

A hybrid HDES algorithm is used to transmit data securely. We have combined the benefits of the DES and AES algorithms in one algorithm. Block cypher algorithms include the AES and DES. AES and DES are less secure than the HDES algorithm.

The probability of an algebraic assault on the hybrid model is decreased and the diffusion of the hybrid model is improved.

Data encryption using the proposed HDES method is effective and trustworthy. The hybrid algorithm HDES, which uses a feistal structure and is a block cypher algorithm like the AES and DES, is also a block cypher algorithm. Block by block, the raw text is processed.

Implementation of Proposed Algorithm:

Step1: The plain text is arranged in thegiventranspositionorderspecifiedbytheAESalgorithm.

Step2: Theplaintext isdividedintotwo equalhalvesthe leftandrighthalvesrespectively

*Step3:*Theroundfunctionisperformed and 4 keys are used in each round

*Step4:*Thenumberofrounds is16 and4sub keysareusedineachround

*Step5:*Afterthecompletion oftheentirerounds32bit swapisperformed.

Step6: After the swap inverse permutation is applied, the cipher text to the given plain text isobtained

In below table the featuresof AES,DES and HDES are compared [9,10].

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 01, January 2022)

Table1:
Comparison of AES, DES and HDES

CHARACTERISTICS	AES	DES	HDES
Blocksize	128bit	64 bit	128bit
Keysize	128bit	56bit	128
No.OfRounds	10	16	16
No.OfSubkeys	44	16	64
SubkeySize	32 bit	48 bit	32 bit
Speed	Fast	Slow	Medium
Security	ExcellentSecurity	NotSecureEnough	High security

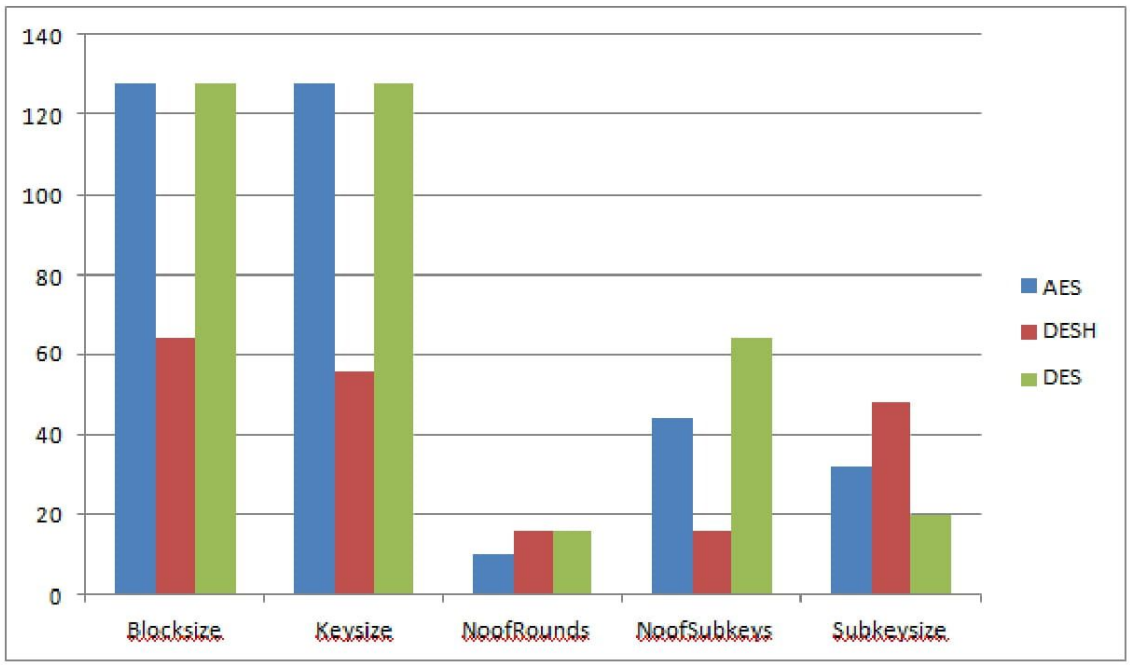

Fig3:Comparison of AES, DES and HDES

Fig 3: Displays the features of HDES comparing with AES and DES algorithms. From theresults, it shown that HDES secured high level security than AES and DES algorithm. FurtherHDESsecurityis enhanced byNo.ofSubkeys used in this algorithm.

IV. CONCLUSION

The final hybrid HDES algorithm is impervious to cracking. We increased the number of rows to 16, and we performed a pre-round computation while keeping the data secure.

The well-known AES and DES algorithms further improve the HDES algorithm. Additionally, the HDES algorithm has good efficiency. As the subkeys are generated simultaneously, the usage of 4 subkeys every 16 rounds improves security. With the right decryption technique, only the intended user will be able to read the cypher text during data transfer. Therefore, it is established that HDES is the best secure algorithm. The same effort can be continued in the future while taking a longer key into consideration.

Another intriguing research area in this regard is the implementation of the suggested HDES algorithm in the areas of WiMAX-based 4G communication and 5G communication, such as the Internet of Things (IOT).

REFERENCES

[1] https://searchsecurity.techtarget.com/definition/cryptography

[2] https://www.edureka.co/blog/what-is-cryptography/

[3] https://www.techopedia.com/definition/16139/public-key

[4] JigneshRPatel,"HybridSecurityAlgorithms forDataTransmissionusingAES-DES".

[5] Panda, P. K., & Chattopadhyay, S., "A hybrid security algorithm for RSA cryptosystem", 2017 4th InternationalConferenceonAdvancedComputingandCommunicationSystems(ICACCS).doi:10.1109/icaccs.2017.8014644

[6] PriyadarshiniP,PrashantN,NarayanDG,MeenaSM,"AComprehensive EvaluationofCryptographicAlgorithms:DES,3DES,AES,RSAandBlowfish",ProcediaComputer Science. 2016;78:617-624.

[7] YogeshK,RajivM,HarshS."Comparisonofsymmetricandasymmetricc ryptographywithexistingvulnerabilitiesandcountermeasures".InternationalJournalofComputerScienceandManagementStudies.2011;11(3): 60-63.

[8] Jeeva AL, Palanisamy V, Kanagaram K." Comparative analysis of performance efficiency and security measuresof some encryption algorithms". International Journal of Engineering Research and Applications. 2012;2(3): 3033-3037.

[9] Alanazi HO, Zaidan BB, Zaidan AA, Jalab HA, Shabbir M, Al-Nabhani Y " New Comparative Study BetweenDES,3DESand AESwithin Nine Factors",JournalofComputing.2010;2(3):152-157.

[10] Ritu T, Sanjay " A. Comparative Study of Symmetric and Asymmetric Cryptography Techniques. InternationalJournalofAdvance Foundationand ResearchinComputer"2014;1(6):68-76.

[11] Mahindrakar MS. "Evaluation of Blowfish Algorithm based on Avalanche Effect" International Journal ofInnovationsinEngineeringandTechnology. 2014;4(1):99-103.

[12] Ritu P, Vikas k "Efficient Implementation of AES" International Journal of Advanced Research in ComputerScienceandSoftware Engineering. 2013;3(7):290-295.