Research Article

Performance Analysis of Cascaded Hybrid Symmetric Encryption Models

Pravin Soni[1], Rahul Malik[2]

[1]Research Scholar, Department of Computer Science and Engineering,
Lovely Professional University, Punjab, India
[2]Asst. Professor, Department of Computer Science and Engineering,
Lovely Professional University, Punjab, India

Article History: Received: 10 November 2020; Revised: 12 January 2021; Accepted: 27 January 2021; Published online: 05 April 2021

Abstract: Over a few years, there is rapid increase of exchange of data over the net has brought data confidentiality and its privacy to the fore front. Data confidentiality can be achieved by implementing cryptography algorithms during transmission of data which confirms that data remains secure and protected over an insecure network channel. In order to ensure data confidentiality and privacy, cryptography service encryption is used which makes data in unreadable form while the reverse process rearranges data in readable form and known as decryption. All encryption algorithms are intended to provide confidentiality to data, but their performance varies depending on many variables such as key size, type, number of rounds, complexity and data size used. In addition, although some encryption algorithms outperform others, they have been found to be prone to particular attacks. This paper reviews and summarizes the various common hybrid cascaded n-tier encryption models. Additionally, this paper compares and analyzes the performance of common hybrid cascaded 2-tier and 3-tier encryption models obtained during simulation based on encryption/decryption time, avalanche effect and throughput. The models compared with AES are 2-tier models (AES-TWOFISH, AES-BLOWFISH, TWOFISH-AES, BLOWFISH-AES, AES-SERPENT and SERPENT-TWOFISH) and 3-tier models (DES-BLOWFISH-AES, AES-TWOFISH-SERPENT and SERPENT-TWOFISH-AES). The hybrid cascaded model like AES-TWOFISH, AES-BLOWFISH and SERPENT-TWOFISH-AES are better hybrid models with respect to throughput and avalanche effect.

Keywords: Cascaded encryption, Hybrid cryptographic model, Multiple encryption, Symmetric encryption algorithm

1. Introduction

Now days, we are in the information overflow over internet, where we are producing, storing and distributing a variety of digital data every day. A lot of data is stored on a computer and transmitted to the internet in the form of files. For valuable, personal or private information or file, it must be secured from infringement by using cryptographic method encryption.

It is essential to protect data from cyber attacks with the growing use of data sharing and connectivity through the Internet. Nowadays, the provision of data confidentiality and privacy has posed a huge problem for computer security analysts and practitioners. Confidentiality of data entails securing data from unwanted disclosure or fraud. It can be accomplished by data encryption and decryption with the aid of cryptography. Cryptography helps to protect sensitive data or records on a hard disc or as it is sent by an unreliable medium of communication. Encryption is the art of protecting information by translating them to secret texts, while decryption is called the opposite way of extracting original texts from secret texts. Without knowing the secret key used during encryption, every encryption algorithm aims to make the decryption process almost impossible (Alenezi et al., 2020).

The hybrid model involving cascaded encryption (multiple ciphers) can enhance the security of a cryptographic system, especially if the different algorithms along with different keys are autonomously chosen and used. Fig. 1 demonstrates the general concept of n-tier hybrid cascaded encryption model i.e. with n stages. During decryption process of hybrid model, obviously reverse order of the algorithms and its associated keys will be used (Marinakis, 2019).

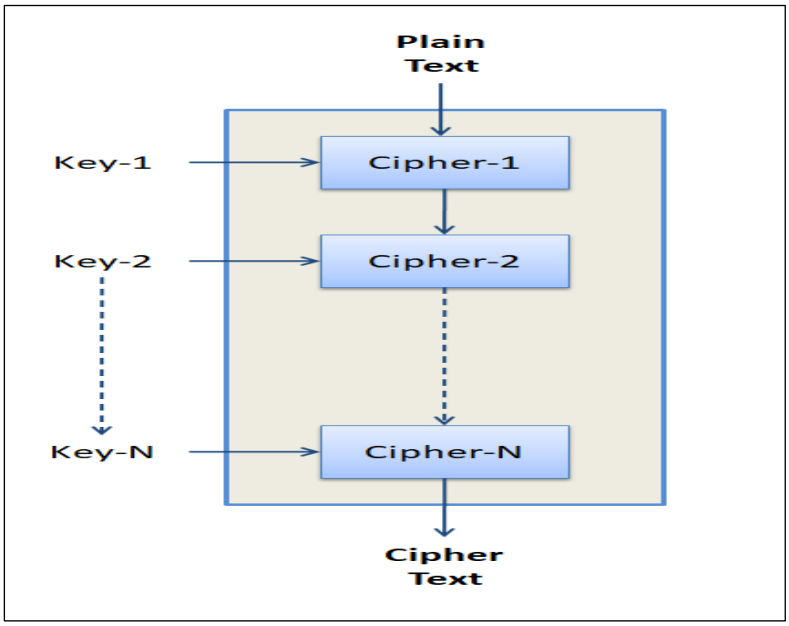

Figure 1. Hybrid cascaded encryption model (n-tier)

The paper provides performance analysis of cascaded hybrid cryptographic model developed by the amalgamation of conventional cipher like DES, AES, BLOWFISH, TWOFISH and SEPRENT. The cascading of conventional ciphers is used to form a strong cascaded hybrid cryptographic model which enhances the security level. A hybrid model puts the best of each together and also minimizes the weaknesses that occur in each uniquely used algorithm (Timilsina & Gautam, 2019). Undoubtedly it's going to surely take some more time however hybrid model will not be ruptured over some finite life years (Onyesolu & Nnabugwu, 2018).

2. Literature Review

Symmetric encryption is a kind of encryption algorithm that depends upon single master key used for encryption/decryption process of digital information. The entities speaking through symmetric encryption ought to make some alternative arrangement for sharing key in order that it could be used for the decryption process. Symmetric encryption algorithm complexity or security mainly depends upon factors like key size, number of rounds, round function and generation of round key (Stallings, 2010).

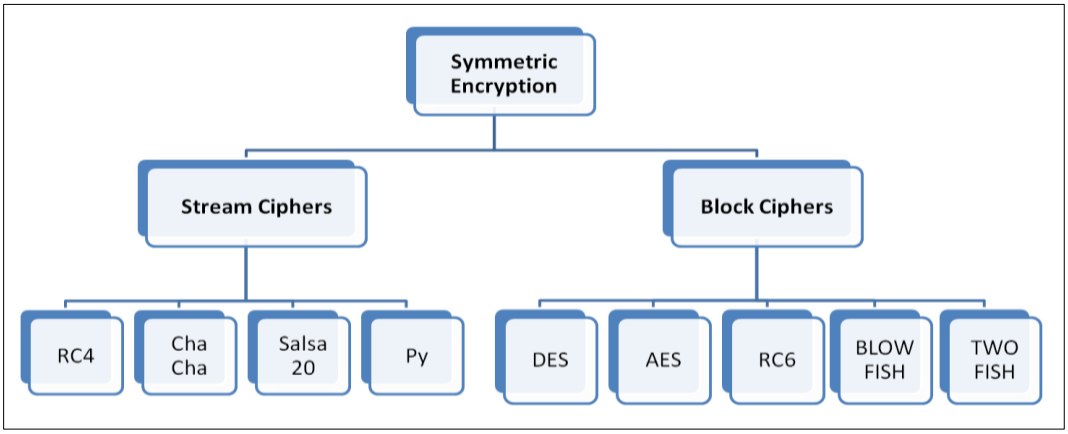

Figure 2. Categorization of symmetric encryption algorithm with example

Modern symmetric encryption key ciphers can be categorized broadly as Stream ciphers and Block Cipher as shown in fig. 2. The stream cipher encrypts message as digit or character one at time using pseudo-random sequence generate based upon key generates one output at time whereas the block ciphers requires complete message to be available for processing which is divided in some fixed size of block and generates fixed size of ciphertext per block which is concatenated as final ciphertext.

The modern block symmetric encryption performance depends on parameters like key size in bits (Jiang et al., 2003), no of rounds (Jiang et al., 2003), no. of sub block (Nechvatal et al., 1999) , block size in bits (Jiang et

al., 2003), key setup speed (B Schneier & Whiting, 2000; Bruce Schneier, 1996) and RCPF throughput(Jiang et al., 2003). The brief overview of some popular block cipher algorithms is shown in fig. 3 based on features like year of design, block size, key size and number of rounds.

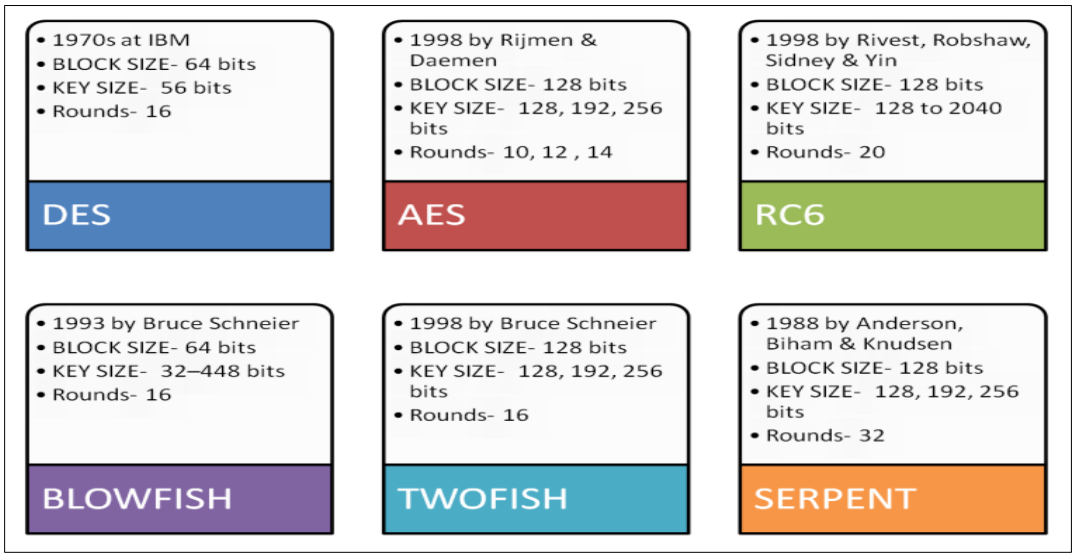

Figure 3. Overview of some popular symmetric encryption algorithms

3. Existing Hybrid Models

Neha, 2019 have developed cascaded hybrid model using AES and TWOFISH symmetric encryption algorithm. The file is encrypted first by AES then followed by TWOFISH using single secret or symmetric key generated using ECDH algorithm. They have used various parameters like encryption, decryption time, throughput for comparing with hybrid cascaded model based on AES and BLOWFISH. They concluded that TWOFISH algorithm is superior then BLOWFISH in terms of encryption decryption processing time and throughput.

Kaushik & Patel, 2019 have designed two different hybrid model based upon symmetric encryption algorithm AES-TWOFISH and AES-BLOWFISH for cloud security. They concluded that hybrid encryption model increases the computational cost of brute force attack by enriching the complexity of ciphertext. As per their result analysis, AES-TWOFISH hybrid model provides better performance then AES-BLOWFISH with respect to encryption decryption processing time.

Priyanka & Lal, 2019 have developed dynamic cascaded 3 tier hybrid model based on AES, BLOWFISH and DES algorithms. They have concluded that hybridizing the cryptographic algorithms like AES, DES and blowfish can enhance the security of data because it increases the complexity. They have specified that the model with DES, BLOWFISH and AES i.e. 3 tier cascaded hybrid model provides high level of security.

Albahar et al., 2018 have developed novel hybrid cryptographic model based upon symmetric (AES, TWOFISH) and asymmetric (RSA) encryption algorithm in Bluetooth. The RSA algorithm is used to transmit the symmetric key securely to recipient during transit. The data is dual encrypted using the secret key of 128 bit by AES then again by TWOFISH before transmitting to recipient. They have observed that hybrid model enhanced the level of security in Bluetooth transmission. Their process of sharing the data remains secure during transit due to amalgamation of 3 algorithms.

Hybrid model have been designed by combining BLOWFISH and AES algorithm to provide enhanced security to cloud data at rest. Their model uses double encryption in fixed order. The data is encrypting by BLOWFISH at first and then AES is applied to generate final output to be stored in cloud. Nothing much is mentioned about generation of secret key used for data security (Gupta et al., 2018). Christnatalis et al., 2019 have designed cascaded hybrid model using AES and BLOWFISH symmetric encryption algorithm for key exchange utilized in digital signature process. Also Purwinarko & Hardyanto, 2018 have used same set of algorithms for developing hybrid model but BLOWFISH is used for encrypting key and AES is used for data encryption.

Othman, 2017 have implemented hybrid model using asymmetric algorithm (RSA) and symmetric algorithm (TWOFISH, AES) for securing robot commands. The hybrid model provides better security features for small commands used in robotic commands. They have used asymmetric algorithm for encrypting robotic command due to its small size.

Oishi et al., 2016 have designed cascaded hybrid algorithm of BLOWFISH and Rivest Cipher 6 (RC6) for Wi-Fi security. They have observed that proposed algorithm takes provides better efficiency like BLOWFISH with respect to encryption decryption processing time and also secured as AES.

Rajan & James, 2013 have designed 3-tier hybrid model using AES-TWOFISH-SERPENT for hiding encrypted text files in image using steganography. Hybrid model developed by Vashishtha & Chouksey, 2019 applies different algorithm for different type of data i.e. for text type of data model uses enhanced version of RC6 and BLOWFISH encryption algorithm applied on image file. Roellgen, 2013 have developed hybrid model by cascading eight different symmetric algorithms. Algorithm sequenced and executed in order based on key.

Table 1 shows the brief overview of various hybrid model used for data security enhancement. These models mainly perform cascaded encryption using different algorithms to increase the complexity in generating ciphertext.

Table 1. Overview of Various Hybrid Models Used for Data Security

Study	Algorithms Used	Model	Gist
Neha, 2019	AES–TWOFISH	2 Tier	• Dual encryption in fixed order using two different Symmetric algorithms. • Common key is used generated using ECDH. • AES–TWOFISH model is better
	AES–BLOWFISH	2 Tier	
Kaushik & Patel, 2019	AES–TWOFISH	2 Tier	• Dual encryption in fixed order • Model increases the computational cost of brute force attack • AES–TWOFISH model is better
	AES–BLOWFISH	2 Tier	
Priyanka & Lal, 2019	AES, BLOWFISH and DES	2 or 3 Tier	• Double or Triple encryption using mentioned algorithms. • Dynamic order increases complexity • 3 tier cascaded hybrid model provides higher level of security than 2 tier.
Albahar et al., 2018	AES–TWOFISH-RSA	2 Tier	• Dual encryption in fixed order. • Key of 128 bit is used for both algorithms. • RSA is used to share key securely over network.
Gupta et al., 2018	BLOWFISH-AES	2 Tier	• Dual encryption in fixed order. • Properties of secret key are not mentioned. • Used for securing cloud data at rest
Christnatalis et al., 2019	AES-BLOWFISH	2 Tier	• Dual encryption in fixed order. • Used for sharing secret key instead of public key algorithms
Othman, 2017	RSA–TWOFISH-AES	3 Tier	• Triple encryption using mentioned algorithms in fixed order. • Used for securely transmit commands of robot to interface. • Used for securing small size messages (2 or 3 char maximum)
Oishi et al., 2016	BLOWFISH - RC6	2 Tier	• Dual encryption in fixed order. • Used for enhancing Wi-Fi security. • Model Performance is similar like BLOWFISH.
Mata et al., 2017	AES-BLOWFISH	2 Tier	• Dual encryption in fixed order. • Used for enhancing data security in cloud. • Hybrid model performance is slower than individual ones but provide high security.

IDRIX VeraCrypt v1.24 Oct-2019	AES-TWOFISH	2 Tier	• Dual encryption in fixed order. • Each block of 128-bit encrypted with Twofish then with AES in XTS Mode.
	AES-Serpent	2 Tier	• Dual encryption in fixed order. • Each block of 128-bit encrypted with AES then with Serpent in XTS Mode.
	Serpent-Twofish	2 Tier	• Dual encryption in fixed order. • Each block of 128-bit encrypted with Serpent then with Twofish in XTS Mode.
	AES-Twofish-Serpent	3 Tier	• Triple encryption in fixed order. • Each block of 128-bit encrypted with AES, Twofish and Serpent in XTS Mode.
	Serpent-Twofish-AES	3 Tier	• Triple encryption in fixed order. • Each block of 128-bit encrypted with Serpent, Twofish and AES in XTS Mode.

4. Experimental Setup and Performance Analysis

The models we have designed are hybrid cascaded 2-tier models (AES-TWOFISH, AES-BLOWFISH, TWOFISH-AES, BLOWFISH-AES, AES-SERPENT, SERPENT-TWOFISH) and hybrid cascaded 3-tier models (DES-BLOWFISH-AES, AES-TWOFISH-SERPENT, SERPENT-TWOFISH-AES) using default key size space of each individual algorithm and compared with AES (Rijndael). For simulation purpose the key and IV of each individual algorithm generated using SHA-256 and assigned to each algorithm based on key size and IV size as shown in table 2.

Table 2. Key and IV Values in HEX Format for Key Size and IV Size

	Size	**Value in HEX Format**
Secret Key	8 byte	280A724CFD7B6DC0
	16 byte	280A724CFD7B6DC07771732E6799568D
IV	8 byte	E72A3BC28C8E1A84
	16 byte	E72A3BC28C8E1A843E0499524C914CB0

Development and programming of above hybrid models are carried out on Visual Studio 2013 in C++ language and compiled with Visual C++ Compiler. We have used famous developed cryptographic library provided by CryptoPP (version 8.2.0) (Dai, n.d.). The computer specification on which simulation carried out consists of WINDOWS 10 Home Single Language OS 64 bit architecture with 8 GB RAM and processor as Intel® Core TM i3-3217U CPU @ 1.8 GHz. The hybrid cascaded 2-tier or 3-tier encryption model performance compared based on encryption/decryption processing time, avalanche effect and throughput.

a) Encryption Processing Time : Time taken by model to generate Ciphertext file from Plaintext file in milliseconds

(1)

Encryption Processing Time (in ms) = End - Start Time of Encryption Process

The fig. 4 shows the processing time required for encrypting files of different sizes by AES and various model of hybrid cascaded model 2-tier and 3-tier. Time required by any model is directly proportional to file size. AES takes minimum time for encrypting input file compared to other hybrids. AES-TWOFISH takes lowest encryption time in hybrid cascaded model.

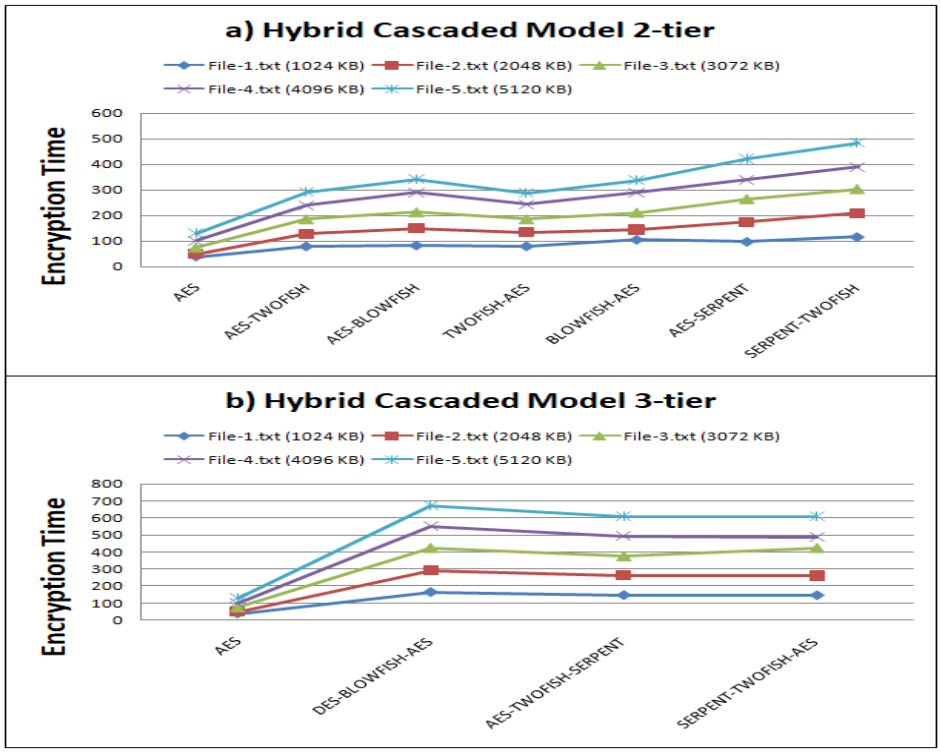

Figure 4. Encryption Processing Time

b) Decryption Processing Time : Time taken by model to recover Plaintext file from Ciphertext file in milliseconds

Decryption Processing Time (in ms)= End - Start Time of Decryption Process (2)

The fig. 5 shows the result of decryption time required for decrypting files of different sizes by AES and various model of hybrid cascaded model 2-tier and 3-tier. Time required by any cryptographic model gradually increases with its file size. AES-TWOFISH requires minimum decryption time for decrypting file in hybrid cascaded model.

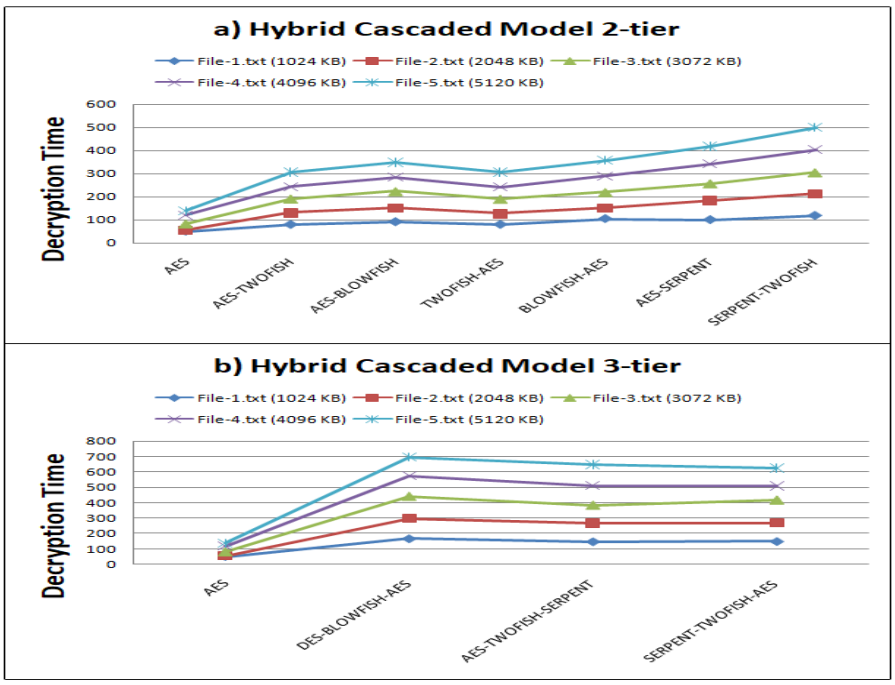

Figure 5. Decryption Processing Time

c) Throughput: It denotes processing speed for encryption process (in Bytes/ms) and calculated as

$$\text{Throughput} = \frac{\text{Size of Ciphertext (in Bytes)}}{\text{Encryption Time (in ms)}} \quad (3)$$

The fig. 6 shows the result of throughput required by AES and various hybrid cascaded models of 2-tier and 3 tier. Throughput of most models is constant and does not increase with increase in input size. Fig. 6 depicts that processing speed of model remains constant and does not vary due to input size. From fig. 4, fig. 5 and fig. 6 one can conclude that AES performance is better due to fact that the hybrid model uses multiple encryptions but provides high security. In hybrid cascaded 2-tier model, AES-TWOFISH or TWOFISH-AES performance is better than other models whereas in hybrid cascaded 3-tier model, AES-TWOFISH-SERPENT or SERPENT-TWOFISH-AES model performance are almost similar and least in their type.

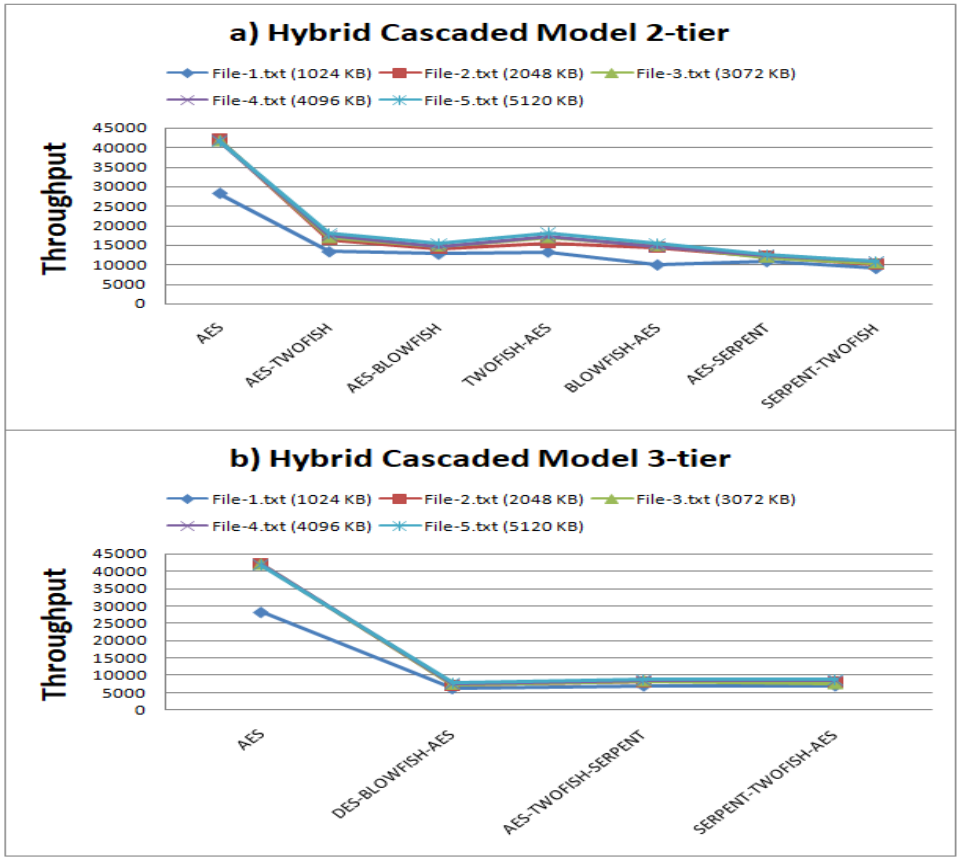

Figure 6. Throughput Analysis

d) Avalanche Effect (in %):: percentage of number of bits flipped or changed in new Ciphertext from Reference Ciphertext by changing single bit in plaintext with respect to number bits in Reference Ciphertext.

$$\text{Avalanche Effect} = \frac{\text{Number of bits flipped or changed in new Ciphertext from Reference Ciphertext}}{\text{Number bits in Reference Ciphertext}} \% \quad (4)$$

Table 3 shows the reference ciphertext generated along with its size (in bits) of different cryptographic models using some fixed plaintext. Table 4 shows the avalanche effect result of various cryptographic models calculated using table 3 and changing one bit in reference plaintext at different position.

The fig. 7 shows the comparative avalanche effect of AES and various model of hybrid cascaded 2-tier and 3 tier cryptographic model. The avalanche effect should be minimum 50% for considering model as highly secure i.e. probability of change for each bit in output is ½ with single bit change in input or key (Yusuf et al., 2019). AES-BLOWFISH hybrid cascaded model provide the highest security and its avalanche effect ranges from 49.5 – 53.65 % whereas the famous AES (Rijndael) has avalanche effect ranging from 46.1 – 51.6 %. The hybrid cascaded model AES-TWOFISH and SERPENT-TWOFISH-AES also have good avalanche effect.

Table 3. Reference Ciphertext Values and its Size

Name	Reference Plaintext	Reference Ciphertext (in HEX Format)	Ciphertext size in bits
AES	4142434445464748494A4B4C4D4E4F	E9F91503C797B6B8B5425655EB16D972	128
AES-TWOFISH		E11BB1D7805D87952DA77C2CE8AF033E194A9AAF910F1AA7F2E732DBDC8D838A	256
AES-BLOWFISH		BCA2DEE99FEE45C68F2E5950AE8DF50C76373F4BBDC38E50	192
TWOFISH-AES		740B7BBB6F1368A007916DE865921D4154B6FF599F577EF47D10F608B2A08641	256
BLOWFISH-AES		0BEE33BC67A66918108C83944B33460E8678C76B22391470EC81E79C73699038	256
AES-SERPENT		7BDB6B15480148F94179504F4B4AD8248A401FE26322856F5796445C6E08DAEC	256
SERPENT-TWOFISH		5A0BA9827B19A3250AAB918456C262C8FF1EE9975EDD78E6055986F5FA487A5D	256
DES-BLOWFISH-AES		22E3F5547498FAFA20796BE63C8AC1F897F7C4B8BE76D79FADFB630975372C8E	256
AES-TWOFISH-SERPENT		5CADED049780828EA692A0F8E0F15F2FDB516AADF37CCBF82F6765F60CDD41CFCF5DCDB6C35F4E06AE7EDA75C525766E	384
SERPENT-TWOFISH-AES		82B72258BDB341439873BEC5C3BA6FCEBC9EE62103ABAD3430990E8FA14BD6BA6DBE735928A7B14E18D8876A22C00CE4	384

Table 4. Avalanche Effect Result for Input Bits Changed at Different Position in Reference Plaintext

Cryptographic Model	Avalanche Effect		
	Single bit change in First Byte of Plaintext (**42**424344454647484 94A4B4C4D4E4F)	**Single bit change in Middle Byte of Plaintext** (4142434445464**749**494A4B4C4D4E4F)	**Single bit change in Last Byte of Plaintext** (4142434445464748494A4B4C4D4E**50)**
AES	66 bits changed (51.56%)	59 bits changed (46.09%)	59 bits changed (46.09%)
AES-TWOFISH	120 bits changed (46.88%)	126 bits changed (49.22%)	127 bits changed (49.61%)
AES-BLOWFISH	103 bits changed (53.65%)	95 bits changed (49.48%)	97 bits changed (50.52%)
TWOFISH-AES	108 bits changed (42.19%)	118 bits changed (46.09%)	114 bits changed (44.53%)
BLOWFISH-AES	125 bits changed (48.83%)	115 bits changed (44.92%)	128 bits changed (50.00%)
AES-SERPENT	148 bits changed (57.81%)	121 bits changed (47.27%)	122 bits changed (47.66%)
SERPENT-TWOFISH	117 bits changed (45.7%)	142 bits changed (55.47%)	122 bits changed (47.66%)
DES-BLOWFISH-AES	133 bits changed (51.95%)	130 bits changed (50.78%)	114 bits changed (44.53%)
AES-TWOFISH-SERPENT	201 bits changed (52.34%)	179 bits changed (46.61%)	198 bits changed (51.56%)
SERPENT-TWOFISH-AES	186 bits changed (48.44%)	199 bits changed (51.82%)	205 bits changed (53.39%)

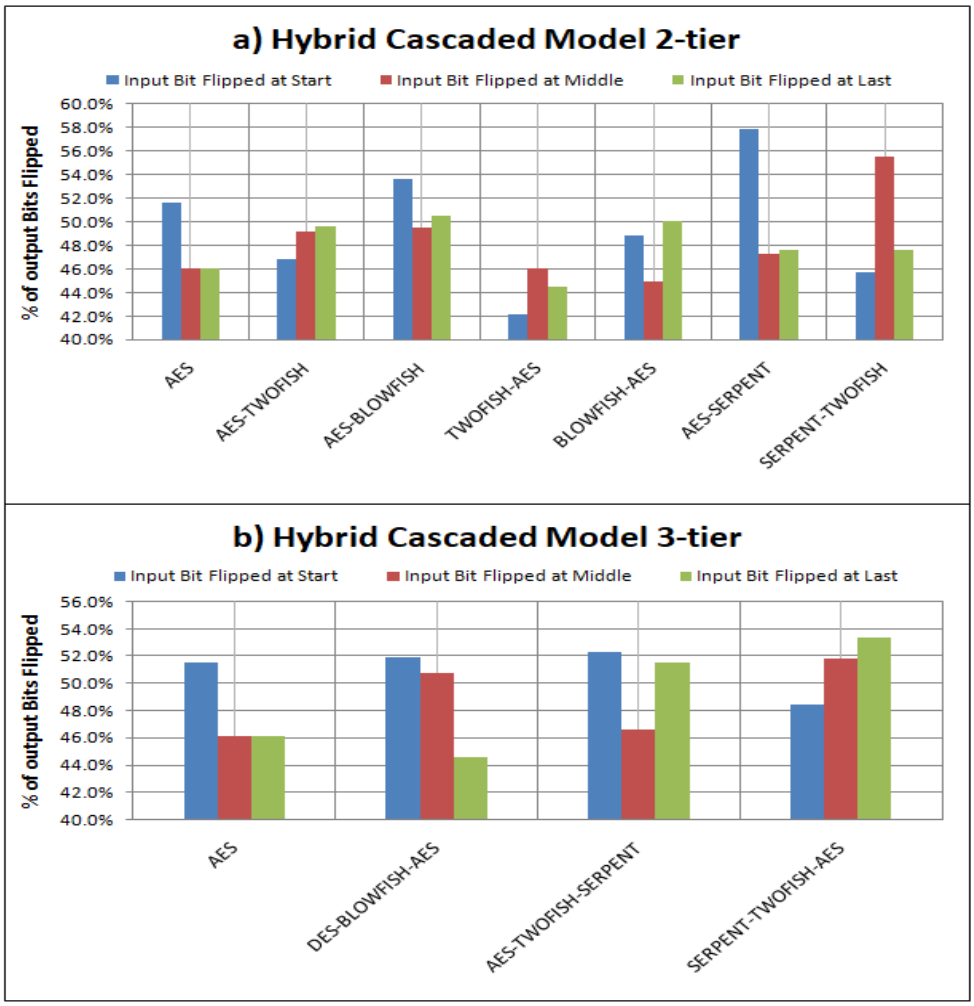

Figure 7. Avalanche Effect in Percentage (%)

5. Conclusion

Everyone wants his/her information should remain confidential during network transit and data stored at cloud or any web-server. The cascading of conventional ciphers is used to form a strong cascaded hybrid cryptographic model which enhances the security level. Undoubtedly it's going to surely take some more time however hybrid model will not be ruptured over some finite life years. The performance of AES i.e. throughput is best when compared with hybrid cascaded 2-tier (AES-TWOFISH, AES-BLOWFISH, TWOFISH-AES, BLOWFISH-AES, AES-SERPENT, SERPENT-TWOFISH) and hybrid cascaded 3-tier models (DES-BLOWFISH-AES, AES-TWOFISH-SERPENT, SERPENT-TWOFISH-AES) but its avalanche effect is less by AES-BLOWFISH 2-tier cascaded model. A hybrid model puts the best of each together and also minimizes the weaknesses that occur in each uniquely used algorithm and enhances the data security level than individual algorithms. From fig. 6 and fig. 7 on can conclude that the hybrid cascaded model like AES-TWOFISH, AES-BLOWFISH and SERPENT-TWOFISH-AES are better hybrid models for data security with respect to throughput and avalanche effect.

References

1. Albahar, M. A., Olawumi, O., Haataja, K., & Toivanen, P. (2018). Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption. *Journal of Information Security*, *09*(02), 168–176. https://doi.org/10.4236/jis.2018.92012
2. Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. *International Journal of Communication Networks and Information Security*, *12*(2), 256–272.
3. Christnatalis, Husein, A. M., Harahap, M., Dharma, A., & Simarmata, A. M. (2019). Hybrid-AES-Blowfish algorithm: Key exchange using neural network. *2019 International Conference of*

Computer Science and Information Technology, ICoSNIKOM 2019, 4–7. https://doi.org/10.1109/ICoSNIKOM48755.2019.9111500

4. Dai, W. (n.d.). *Crypto++ Library 8.2 | Free C++ Class Library of Cryptographic Schemes*. Retrieved May 22, 2020, from https://www.cryptopp.com/
5. Gupta, U., Saluja, S., & Tiwari, T. (2018). Enhancement of Cloud Security and removal of anti-patterns using multilevel encryption algorithms. *International Journal of Recent Research Aspects*, *5*(1), 55–61.
6. IDRIX. (n.d.). *VeraCrypt - Free Open source disk encryption with strong security for the Paranoid*. Retrieved September 15, 2020, from https://www.veracrypt.fr/en/Home.html
7. Jiang, J., Ni, X., & Zhang, M. (2003). Reconfigurable Cipher Processing Framework and implementation. *In: Zhou X., Xu M., Jähnichen S., Cao J. (Eds) Advanced Parallel Processing Technologies. APPT 2003. Lecture Notes in Computer Science., Springer, Berlin, Heidelberg*, *2834*, 509–519. https://doi.org/10.1007/978-3-540-39425-9_60
8. Kaushik, S., & Patel, A. (2019). Secure Cloud Data Using Hybrid Cryptographic Scheme. *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 1–6.
9. Marinakis, G. (2019). Modification and customization of cryptographic algorithms. *Journal of Applied Mathematics & Bioinformatics*, *9*(1), 1–13.
10. Mata, F., Kimwele, M., & Okeyo, G. (2017). Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish). *International Journal of Science and Research (IJSR)*, *6*(3), 1702–1708. https://doi.org/10.21275/ART20171804
11. Nechvatal, J., Barker, E., Dodson, D., Dworkin, M., Foti, J., & Roback, E. (1999). Report on the development of the Advanced Encryption Standard (AES). *Journal of Research of the National Institute of Standards and Technology*, *104*(5), 435–459. https://doi.org/10.6028/jres.106.023
12. Neha, P. (2019). IMPLEMENTATION OF HYBRID AES AND TWOFISH FOR CLOUD. *Journal of The Gujarat Research Society*, *21*(6), 664–682.
13. Oishi, N. J., Mahamud, M. A., & Asaduzzaman. (2016). Short paper: Enhancing Wi-Fi security using a hybrid algorithm of blowfish and RC6. *Proceedings of 2016 International Conference on Networking Systems and Security, NSysS 2016*. https://doi.org/10.1109/NSysS.2016.7400706
14. Onyesolu, M. O., & Nnabugwu, N. C. (2018). Design and Implementation of a Hybrid Database Encryption Model. *International Journal of Innovative Research in Science, Engineering and Technology*, *7*(3), 2066–2074. https://doi.org/10.15680/IJIRSET.2018.0703015
15. Othman, S. (2017). Securing Robotic Communication using Multiple Security Techniques. *International Journal of Computer Applications*, *178*(1), 1–4. https://doi.org/10.5120/ijca2017915704
16. Priyanka, G., & Lal, A. M. (2019). A hybrid encryption method handling big data vulnerabilities. *International Journal of Cloud Computing*, *8*(3), 207–213. https://doi.org/10.1504/IJCC.2019.103879
17. Purwinarko, A., & Hardyanto, W. (2018). A Hybrid Security Algorithm AES and Blowfish for Authentication in Mobile Applications. *Scientific Journal of Informatics*. https://doi.org/10.15294/sji.v5i1.8151
18. Rajan, M. M., & James, A. (2013). Hiding Encrypted Text Files In Multimedia Files. *International Journal of Engineering Research & Technology (IJERT)*, *2*(3), 1–10.
19. Roellgen, C. B. (2013). The Polymorphic Medley Cipher Version 2 : 128 bit block length , 128 .. 1024 bit key length. *White Paper*, 1–13.
20. Schneier, B, & Whiting, D. (2000). A Performance Comparison of the Five AES Finalists. *Proc 3rd Advanced Encryption Standard AES Candidate Conf*, *3*, 123–135.
21. Schneier, Bruce. (1996). *Applied Cryptography* (Second Edi). John Wiley & Sons, Inc.
22. Stallings, W. (2010). *Network Security Essentials* (Fourth Edi). Prentice Hall Press, USA.
23. Timilsina, S., & Gautam, S. (2019). Analysis of Hybrid Cryptosystem Developed Using Blowfish and ECC with Different Key Size. *Technical Journal*, *1*(1), 10–15. https://doi.org/10.3126/tj.v1i1.27582
24. Vashishtha, M., & Chouksey, P. (2019). A hybrid data security and identification mechanism in cloud computing. *International Journal of Scientific and Technology Research*, *8*(9), 1565–1571.
25. Yusuf, D. M., Setiadi, D. R. I. M., Rachmawanto, E. H., Sari, C. A., & Ali, R. R. (2019). Dual Encryption Method for File Security. *4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, *6*, 222–227.