KeAi
CHINESE ROOTS
GLOBAL IMPACT

Journal of Digital Economy

PERFORMANCE ANALYSIS OF HYBRID ENCRYPTION ALGORITHM FOR DATA SECURITY IN CLOUD SYSTEMS

Ms. Mamta Joshi[1], Dr. Manish Prateek[2]

1. Research Scholar, G D Goenka University, Sohna, Haryana-India
2. Professor and Pro Vice Chancellor, DBS Global University

Abstract

Cloud computing emerged as a new tool for pooling and offering numerous computing resources in ICT industry. Most of organizations are adopting cloud computing now a days because of availability of massive cloud facilities with minimal cost like Paytm in India. Data security is a big concern as the user data always stored on off-site cloud locations . The data owners are using firewalls, VPN (Virtual Private Network) to ensure the data security at there end , data security is a serious concern when data owner stores their sensitive data on remote servers on cloud and users access required data from these remote cloud machines. Data security in cloud is a very popular research areas for cloud data protection. Encryption algorithms are most widely used approach for ensuring the data security in today's rapidly evolving cloud computing environment
. For this research paper, we have analyzed and compared the effectiveness of some widely used symmetric key encryption algorithms, Advanced Encryption Standards (AES), Elliptic-curve cryptography (ECC)and Blowfish, based on throughput, power consumption, and encryption speed. While tested by simulation we found that AES outperforms on Blowfish when security flaws are put into consideration however AES requires more processing power compare to ECC .After analyzing all the results we have proposed MKP as efficient hybrid security algorithm thatwillcombinethebenefitsofbothapproachestoprovidebetterdatasecurityincloudbasedsystems.
Our performance analysis test proved that the proposed hybrid approach named MKP will be an excellent solution for encrypting and decrypting files in cloud environment even on large block sizes and longer key with very high level of security .

Keywords. CSA,AES,ECC,LCKS, CBC , Blowfish, Encryption, Multiple Key Passing

1. Introduction

Cloud computing emerged as a new tool for pooling and offering numerous computing

resources in ICT industry . Most of organizations are adopting cloud computing now a days because of availability of massive cloud facilities with minimal cost like Paytm in India . Data security and privacy are emerging as big concerns in cloud supported services. To addresstheseconcerns,theNationalInstituteofStandardsandTechnology(NIST)hasestablishedcomprehensiveguidelinesforensuringcloudservicesecurity,providingproviderswitharoadmapforprotectingtheirclient'sdata [1,2].Cloud Security Alliance (CSA)has also reiterated the importance .of authentications,

secrecy, integrity, as well, availability. Encryption algorithms are most widely used approach for ensuring the data security in today's rapidly evolving cloud computing environment . For this research paper, we have analyzed and compared the effectiveness of some widely used symmetric key encryption algorithms, Advanced Encryption Standards (AES), Elliptic-curve cryptography(ECC)and Blowfish, based on throughput, power consumption, and encryption speed. While tested by simulation we found that AES outperforms on Blowfish when security flaws are put into consideration however AES requires more processing power compare to ECC. After analyzing all the results we have proposed MKP as efficient hybrid security algorithm that will combine the benefits of both approaches to provide better data security in cloud based systems. Our performance analysis test proved that the proposed hybrid approach named MKP will be an excellent solution for encrypting and decrypting files in cloud environment even on large block sizes and longer key with very high level of security .

2. Literature Review

Cloud computing offers advantages to users by allowing them to use infrastructure, platforms and software by cloud providers at low cost and elastically in an on-demand fashion. Cloud computing provides remote users , large data storage and fast processing services in clouds, obviating the need to have a powerful device configuration of CPU speed, memory and storage capacity.[3,4]

BesidesthatCloudComputingalsoprovidenumerousbenefits,likecostsavings,security,privacy,dependability,increasedprocessingpower,storage,flexibility,scalability,andlowerITinfrastructure overhead costs [4,5]. Various implementation models, such as public, private, communal, and hybrid cloud, provide organizations with a variety of options for leveraging cloud services[6].

Triple Data Encryption Standard(3DES)was the first project that was first anticipatedbyIBMin1998 and was standardized in ANSI X9.17 and ISO 8732. This algorithm is based on the three main options that were introduced from the Feistel architecture. The key is 168 bits long allowed in 16 sub keys with 8 s blocks and is 48 bits long[7] .Due to the need for high protection and performance, the NIST launched a call for cipher candidates to introduce a new encryption standard in 1997, it is time to replace the current DES and 3DES encryption algorithm with new AES encryption algorithms. depend on The Feistel layout of the AES symmetric block cipher means that the AES algorithm accepts a 128-bit block size

and a set of three 128, 192, 256 key lengths permitted for10,12,and14 rounds using the same key for both encryption and decryption. The vector design of Rijndael give sit considerable protection and the main scale of upto 256 gives it resistance to possible attacks[8]. A symmetric cipher with a variable key length is a blowfish depend on A Feistel structure. It has a block size of 64-bits, and the key ranges from 32 to 448bits. It uses 16 rounds and has a wide box that relies on the key. In the Blowfish algorithm, there are four S boxes, and the same algorithm is used for decryption in reverse [9]. Elliptic curve cryptography transforms a mathematical problem into an applicable computer algorithm. Intractable problems are the center of public key cryptography and bring computationally demanding operations into a cryptosystem. ECC is based upon the algebraic structure of elliptic curves over finite field [10].

3. Proposed hybrid algorithm for cloud data security

The proposed hybrid algorithm based cloud data security model will use classification system with three levels of categorization. To protect data, we have proposed different encryption techniques at each level. Level 1 data is non-sensitive and available to the public, whereas level 2data, such as personal and transactional data , is encrypted with AES-256. Level 3 data, which is critical, is encrypted using ECC and Blowfish with a two-cipher cascade process and Multi key passing(MKP) on each level.

The proposed hybrid algorithm based cloud data security model is depicted graphically in Fig. 1, which shows the categorization and encryption techniques used at each level. The diagram highlights the client-side encryption and decryption procedures at all three levels (Level 1, Level2,and Level 3).

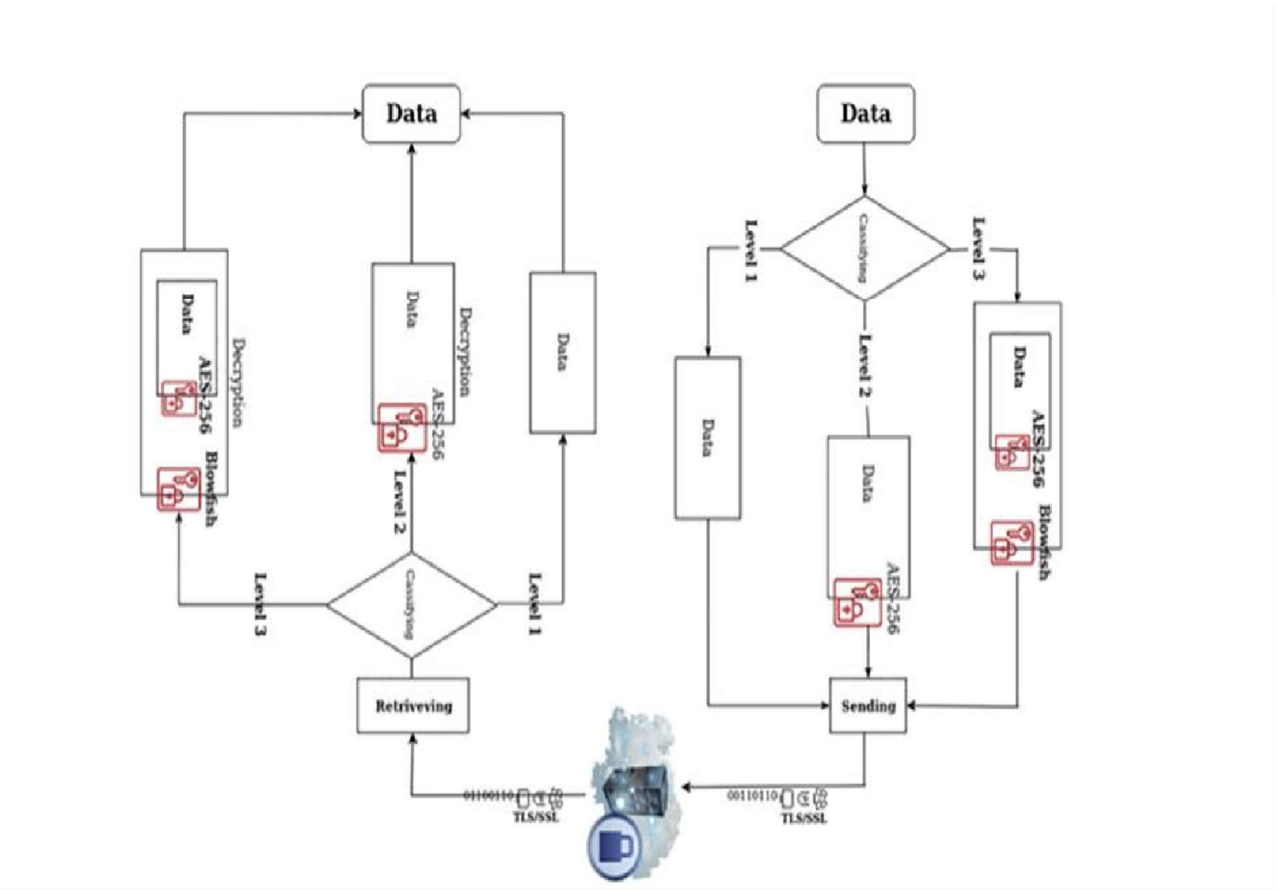

Fig1.proposedhybridalgorithmbasedclouddata security model

Level1 :Client side encryption

Client side encryption is divided into three groups in our proposed model based on data importance and encryption method . Each end user will categorize and encrypt his data before transmitting it to cloud to ensure that data remains secure and inaccessible to the cloud providers or other third parties.

Level2: Cloud storage

During this phase, data is transferred and stored to the cloud storage . The proposed model encrypts data before transmission using AES and Blowfish encryption techniques, eliminating the need for additional encryption by the cloud provider. This ensures that data is protected at all times during transmission and stored securely .

Level3: Server side

Server side decryption, like encryption, applies data categorization to the encrypted data and

uses the encryption keys in reverse order. It is important to note that we have used multiple keys for data encryption and decryption .Blowfish implementation, on the other hand, is key-dependent and employs the Cipher Block Chaining also for added security.

Our proposed hybrid algorithm based cloud data security model improves the security of data stored in the cloud by combining these encryption techniques. It provides a practical solution for protecting critical information during cloud storage from unauthorized access or theft. For multiple key passing , one logical gate exclusive or (XOR) will returns true only when one two keys are true and one key is false.

4.Conclusion

This research paper proposed and tested a hybrid data security method for secure cloud environment. The method achieved a maximum throughput of 88ms for Blow fish and 570ms for AES while using 25 MB of memory in the ECB and CBC models. The AES and BF models produced 425mb with$25x10^4$ms for AES and 429mb with$25x10^4$ms for Blowfish, respectively. In the absence of pipelining, this hybrid method proved to be particularly effective. It is worth noting that the Blowfish method has a security issue with weak keys that AES does not have. As a result, combining AES and Blowfish in a hybrid approach is an excellent solution for encrypting and decrypting files with large block sizes and longer keys, such as 128-bit blocksand128, 192, and 256-bit keys.

References

[1] James, D., &Girish Tere.: Cloud-Computing. The University of Mumbai,(2018).

[2] Keijo, H., Adnan, A., Johan, L., &Tommi, M.: Introduction to Cloud Computing Technologies. TUCS General Publication (2014).https://doi.org/10.13140/2.1.1747.8082

[3] Harold C. Lin, Shivnath Babu, Jeffrey S. Chase, Sujay S. Parekh, ―Automated Control in Cloud Computing: Opportunities and Challenges‖, Proc. of the 1st Workshop on Automated control for data centres and clouds, New York, NY, USA, pp. 13-18, 2009 [4] Gaoyun Chen, Jun Lu and Jian Huang, Zexu Wu,―Saa AS-The Mobile Agent based Service for Cloud Computing

in Internet Environment‖, Sixth International Conference on Natural Computation, ICNC 2010,pp.2935-2939

[4] Hashizume, K., Rosado, D.G., Fernández- Medina,E., &Fernandez, E.B. :AnanalysisofsecurityissuesforcloudcomputingJournalofinternetservicesandApplications,4,1 -13(2013).

[5] Zhang, Q., Cheng, L.,& Boutaba, R.: Cloud computing: state-of-the-art and research challenges. Journal of internet services and Applications, 1,7-18 (2010).

[6] Mell, P., & Grance, T.: The NIST definition of cloud computing(2011)

[7] J.Thakur, N. Kumar, DES, AES and blowfish: symmetric key cryptography algorithms simulation based performance analysis Int. J .Emerg. Technol. Adv. Eng. (2011)

[8] T.NieandT. Zhang, "A study of DES and blowfish encryption algorithm," 2009,doi:10.1109/TENCON.2009.5396115.

[9] S.Manku, K. Vasanth, Blowfish encryption algorithm for information security, ARPNJ. Eng. Appl. Sci. (2015)

[10] Pardeep Malik "Elliptic Curve Cryptography For Security In wireless Networks"Statistics2011 Canada: 5th Canadian Conference in Applied Statistics/ 20th conference of the Forum for Interdisciplinary Mathematics -Interdisciplinary Mathematical Statistical Techniques, July 1-4-2011,ConcordiaUniversity, Montreal, Quebec, Canada.