International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN: 2350-0557, Volume-9, Issue-2, April 2022
https://doi.org/10.55524/ijirem.2022.9.2.7
Article ID IJIR-1188, Pages 50-58
www.ijirem.org

Analysis of Possible Attacks on Data and Possible Solutions with Comparative Analysis of Various Encryption Algorithms and Evaluation

Chandrashekhar B[1], and Dr. Mohamed Abdul Waheed[2]

[1]Assistant Professor, Department of MCA, Visvesvaraya Technological University(VTU), Belagavi, India
[2]Associate Professor, Department of MCA, Visvesvaraya Technological University(VTU), PG Centre, Kalaburgi, India

Correspondence should be addressed to Chandrashekhar B; chandrashekharb@vtu.ac.in

ABSTRACT- Today's fast-growing technology, "Cloud computing," is widely employed in various industries because to its low-cost services, such as pay-per-use mode, which allows users to access resources via an Internet connection. Cloud storage is a service offered by cloud service providers that allows users to store their data on a remote server. Although cloud service providers ensure that data kept in the cloud will be safe and secure, there are a number of issues that must be addressed. For user data in the cloud, data integrity and security must be assured. The integrity of the data must be unmistakable. There are some security dangers associated with storing sensitive data with cloud storage companies. The lack of data integrity is a big worry in the cloud environment. Encryption computations are used to provide complete security of data being sent from one source to another, as well as to prevent private data from being exposed to unauthorized parties. Encryption computations are mostly useful for obtaining and protecting information being sent from one end to the next from any type of flaw. Some of these computations have been adopted by scientists to ensure data security in banking, healthcare, and the military. When used for information security, a fraction of these computations are varied in terms of effectiveness, exactness, dependability, and reaction time. We considered Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES), BLOWFISH, and Data Encryption Standard (DES) calculations in order to conduct a relative evaluation. Because there is scepticism about which of the computations is more reliable, trustworthy, and practical when considering the highlights that depicted their variety. As a result, this work aims to conduct a close examination of each encryption calculation in order to determine the optimal method for employing the specified measures. Python was used to implement modify BLOWFISH's algorithm. When the results are compared to other algorithms results, it is discovered that BLOWFISH takes the shortest time to encrypt, while RSA and AES take the longest. In addition, based on the measurements used in the evaluation, the BLOWFISH calculation is regarded as the most proficient of the three calculations. In this study, only a few of the obtained results are discussed.

KEYWORDS- Cloud Computing, Security, Algorithms

I. INTRODUCTION

The search for the best solution to offer the necessary protection against data thieves' attacks while also providing these services in a timely manner has become one of the most active subjects in the security related communities as the importance and value of data exchanged over the Internet or other media types has increased **[**1]. This document attempts to provide an objective assessment of the most widely used data encryption techniques. The offered comparison takes into account the behavior and performance of the algorithm when different data loads are employed, as this is our primary goal. The globe has faced a major challenge in the realm of information and communication technologies in recent years. Every day, computer networks and online services grow in number, and our lives have changed as a result of several internet applications: the expansion of e-commerce, e-banking, e-government, bill payment, and other applications that necessitate a safe environment in both the public and private sectors [2]. The large number of transactions and applications that run over public wired or wireless networks cannot be left unchecked, secure, or vulnerable to breaches, so these transactions and applications must require secure and comprehensive communications that protect the network management and monitoring process to ensure data authentication, data integrity, confidentiality, and integrity [3]. There are various facets and applications of security when transferring data over the Internet or any public network [4], ranging from safe commerce and payments to private communications and password protection. Encryption is an important technique for protecting sensitive data and is one of the most secure features of encryption. The information. Encryption is used to ensure data security during transmission. Encryption comes to play with the sole point of fostering a strategy for security instrument to forestall, safeguard illicit admittance to information and records. The requirement for more perplexing ways of encoding and decode with calculations jumped up with different approaches to encoding documents, information, secret key substance which ranges across sound, video, pictures and messages

Data security relies heavily on encryption methods. Asymmetric (private) key and symmetric (public) key encryption algorithms are two types of encryption algorithms. The message's public key was used to encrypt it, while the message's private key was used to decode it. Today, there is a pressing need to employ cryptography to connect the world through open networks, in which networks are used to electronically transfer information between regular individuals or private, public, military, and civil entities. There has to be a way to keep the data private. Government agencies and secret services all over the world employ cryptography to turn information into incomprehensible codes, allowing for safe online and offline message delivery.

A revolution in technology and computing has resulted in the creation of a new computer service known as Cloud Computing. Traditional data centres will undergo evolutionary changes as a result of this new era of Cloud Computing. Cloud computing is becoming the future of many IT enterprises and organizations [5]. They choose this current computing method, in which their financial deposits are reduced by utilizing the enormous number of Cloud resources available in the Payasperuse approach. Services are provided in response to demand and the needs of the entire company or a single user. There are numerous Cloud companies who can supply those services Cloud storage is currently in a modern and emerging phase, in which data is outsourced on a regular basis by data users, and the cloud provider has responsibility for its availability and reliability. The Cloud Service Provider (CSP) should keeps track of and manage these data. In a private cloud, the infrastructure is owned and managed by the individual organization. In other words, access to the data rests with this organization and is granted only to trusted parties. In a public cloud, the infrastructure is owned and operated by a cloud service provider and resides on remote servers. This means that customer data is beyond their control and may even be passed on to untrusted third parties. The two major services that the cloud should give are secrecy and integrity. Confidentiality means that the cloud storage provider does not have access to any information about the customer data, and integrity means that the customer data must not be modified by a supplier [6]. Usage of Cloud have become popular in recent years the transactions which has large data transactions such as banking, business, and stock trading, are carried out over a remote or link network, necessitating a profitable and dependable start-to-finish relationship. And there's more. To ensure accessibility, honesty, and classification of data sharing across the network, the connection from one end to the other should be strictly protected. Encryption comes into play with the sole purpose of creating a security plan to prevent and safeguard unauthorized access to information and data. With numerous approaches to encoding documents, information, secret key substance that ranges over music, video, photographs, and messages, the demand for more complex ways of encoding and decoding with computations has risen. Clouds various storage services and attacks are shown in figure 1.

There are basically three entities in the cloud environment.

- **User of Information:** One that keeps data in the cloud and entrusts security to the cloud service provider
- **Provider of Cloud Services:** The person in charge of user data held on cloud servers.
- **Third Parties You Can Trust:** By replying to their request, you'll be able to gain access to and investigate the risk of cloud storage on your behalf.

II. INTERGRITY OF DATA IN CLOUD STORAGE

A. Data Reliability

In general, data integrity is defined as data that is undamaged (that is, data that has not been altered without the users' knowledge). When assaults or data outages happen, the customer is the one who suffers, and their vital information is gone. When a customer's data is compromised, they will lose faith in the service provider. As a result, it is the provider's job to assume responsibility for the information kept. Protecting private and sensitive information, such as a customer’s credit card information or personal details data, from unscrupulous attackers or insiders is critical. Users must have access to the integrity and security of their data [16].

B. Attack Stopping Data Integrity

During this duration of online storage, various intruders, nameless customers, and providers may distort the virtual statistics. If an attacker gains access to the garage server, he can change the statistics of the clients. He might change the content of the statistics, causing a significant loss to the customer and halting the growth of the Cloud service provider. As a result, this issue is a major setback for Clouds' reputation. Figure 2 depicts the evaluation of Cloud garage offerings and the assault on statistical integrity. There are more chances of inflicting significant losses to statistics that can be saved remotely in Provider's statistics facilities, where customers have less control over their saved information. Within the cloud context, there are several forms of assaults [8], resulting in a loss of Data Integrity saved on far-flung servers. Many internal and external attacks [9] are common, corrupting the data stored on the provider provider's cloud servers. The attacks on the cloud garage's mission statistics integrity.

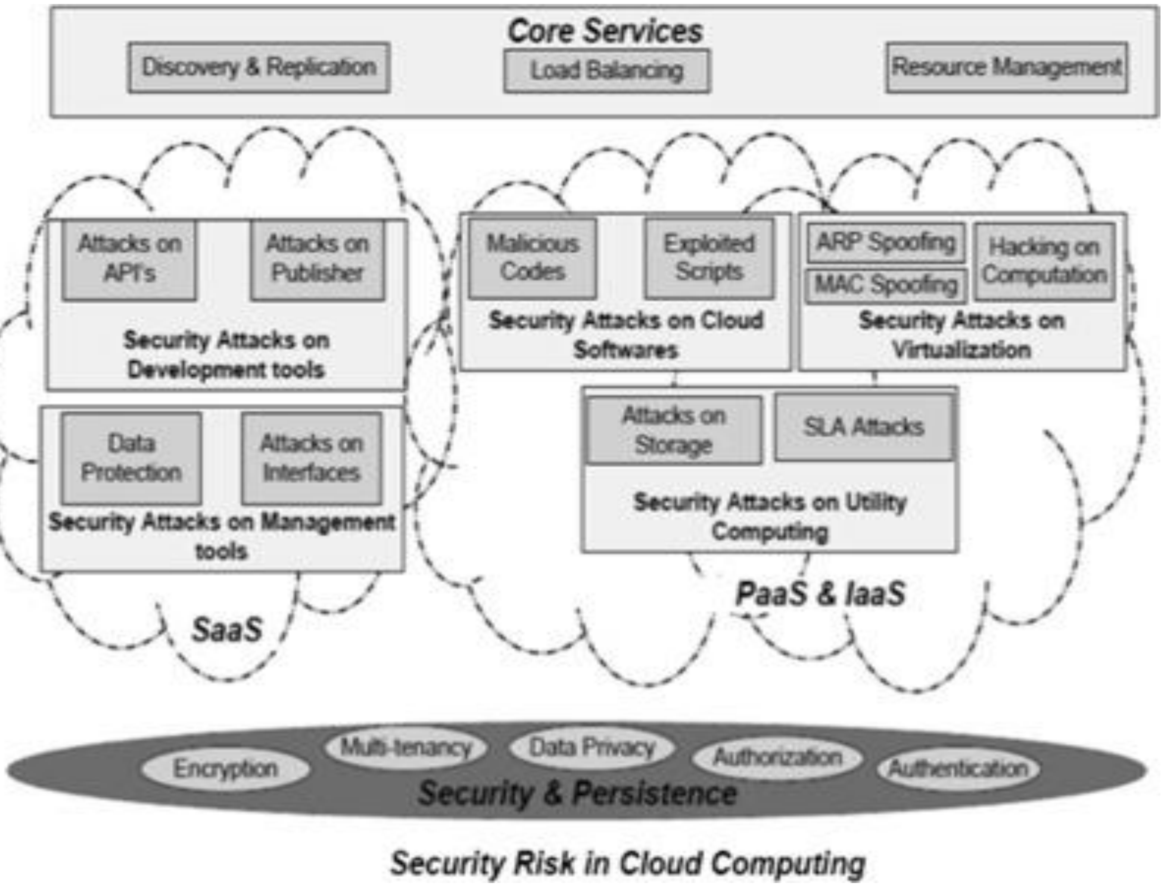

Figure 1: Cloud Storage services and Attacks [7]

1) A Data Alteration Assault

A data modification attack alters data saved on a remote storage medium. An attacker can modify data or a server fault can cause it to be modified. An attacker can update this for a variety of reasons, including harming another company's reputation or disclosing information for personal gain. The loss of data integrity in Cloud Storage is caused by a server breakdown owing to probable corruption [9].

2) Data Leakage and Tag forgery Attack

An intruder can readily access data stored by executing or intercepting possible verification communication during the auditing and verifying process, which is known as a data leakage attack. A Tag Forgery Attack is one in which a dishonest or untrustworthy service provider defrauds clients by employing forged data tags [10]. These two concerns may increase the danger of ownership fraud and data leakage. Furthermore, these assaults can jeopardize data integrity and compromise the security of a distributed cloud system more quickly than a single cloud system.

3) Attack on Replay and Timeliness

A replay attack is a type of network assault in which a lawful data transaction is repeated or delayed deliberately or fraudulently [11]. This can be done by the initiator or by an attacker who intercepts and retransmits the data. When considering the Timeliness attack the protocol does not know when the phase is completed without a deadline, which can cause issues. To ensure fairness, each party has a set amount of time to stop the execution.

4) Collusion Attack and Rollback Attack

In technical words, Rollback is the rolling of data information towards the backside, as the name suggests. When the data owner updates a new set of data blocks, the dishonest service provider continues to deliver the previous version to users who download the data. It's tough for inexperienced users to notice. As a result, data owners may experience data loss, resulting in a tarnished reputation among data consumers. When a new version of data is updated, this rollback can also occur without sufficient deletion assurance of the users' old data [12][13].

5) The Byzantine Assault

It is a type of in which the fail of the system happens in a variety of ways, including basically stopping, crashing, requests are wrongly processed, corrupting their local state, and/or producing inaccurate or inconsistent results. It’s an assault in which the adversary has complete control of a legitimate device and can use it to disrupt the system by acting irrationally [9][19]

C. Data Integrity Attacks in the Cloud are Prevented Using following Mechanisms

As previously stated, there are several flaws and risks that prevent information honesty. Cloud data is stored on remote servers with limited capacity, and clients have no way of knowing whether the data is accurate. The document director saves the first information or scrambled information to the distributed storage servers when a client transmits it to the record server. Malicious clients or information owners, distributed storage providers, or untrustworthy outsiders can all be aggressors. Juels et al. [14] describe the recovery test design (POR) as a way to ensure information integrity in remote areas where this technique only works with encoded data. We can use a few sentinels to validate the accuracy of the data, but the sentinels you employ can't be used again for more verification. In the cloud environment, many ideas have been offered for information security, information honesty, and information possession. The "Provable Data Possession" (PDP) plot is shown, which verifies the integrity and ownership of client data stored on remote servers or in untrustworthy stockpiles. In this case, an open key is used in conjunction with homographic labels to review information documents [15]. In this case, an open key is used to inspect information documents in light of homographic labels. Instead of using the public key, symmetric key cryptography [20], [21] is offered, which allows for block refreshing, cancellation, and addition. It uses a homomorphic straight authenticator based on the RSA approach to verify the re-appropriated information, but there is a drawback in that there is a risk of information spillage to outside verifiers [23]. Many proposals were offered in relation to ensuring information trustworthiness and ownership in the Cloud environment.

D. Tag Forgery and Data Leakage Attacks Mitigation

The innocent user is harmed as the service provider tries to deceive the client by utilizing misleading data tags. Cooperative Provable Data Possession (CPDP) scheme was proposed ny scYun Zhu et al., which combines two tactics (Hash Index order and Homomorphic Verifiable Response) to provide robust security and clear confirmation. For information accessibility, many distributed storage administrations are explored rather than solitary stockpile administrations. This CPDP plot is used to verify the trustworthiness and accessibility of the stored data. Clients create a test tag before providing information to Cloud Service Providers, which they then forward to CSPs. They put the CSP to the test by using TTP to investigate information integrity and accessibility. The Hash Index progressive system process is proposed, which is used to combine the results from different Cloud Service Providers into a single reaction value.

Another technique, known as homomorphic undeniable reaction, provides competent agreement safe hashing capability. This strategy is based on a multi-prover zero-information evidence framework with information adequacy. The client can use the culmination property to challenge the cloud server to check the information's honesty and veracity. The information and mark labels are secure because to the Zero information attribute. The reaction from the specialist co-op, where the verifier has no idea what the number is, is remembered for the irregular whole number. As a result, this is a defense against data leakage.

E. Reducing Replay and Timeliness Attacks

The organization assault can be carried out by postponing or rehashing the information while it is being transmitted. Jun Feng.et.al] present an NR (Non renouncement) convention for ensuring information trustworthiness, in which the capacity rightness and honesty flaws are overcome. In both the transferring and downloading meetings, the accuracy of the data is reviewed For the purpose of bridging these two meetings, an Integrity interface is being designed [11]. This practice is useful since it allows the client to stop an execution if the other party does not respond. All of the parties involved, such as the information's originator and recipient, provide confirmations. For information classification, the source encodes the proof using the beneficiary's public key. A succession number with the source's mark is included, and an irregular number is provided to avoid the Replay assault. While an interloper can modify the grouping number in the plain message if they block and replay, they cannot change the Encrypted Hash value, which is protected by the source's private key. Furthermore, Timestamp is incorporated in this convention, where this time limit evades the practicality assault, i.e., the interaction cannot be done after as far as feasible. To avoid ambiguity, this plan is being used for web-based re-energizing of portable equilibrium and other trade purposes.

F. Resolving the Issue of Roll-back and Collusion Attacks

Ordinary encryption schemes are used when storing data in a local system, but when the data is stored in a distributed storage system, strong security schemes are required to ensure data confidentiality and integrity. When information is stored by outsider stockpiling suppliers, the nefarious aggressor may alter the content, delete a new record, and then 'roll-back' the document by providing the obsolete substance to the blameless customers. There is a loss of information integrity. "Roll-back assault" approach was proposed by Q. Wang.et.al, but distributed storage system cannot use it. As a result, provided a method for avoiding the cloud's 'roll-back' occurrence using the Merkle Hash tree concept. When another piece of data is changed, the counter value and tag of the data obstructs are updated as well. As a result, if an intruder tries to alter the data, the counter value changes, indicating that the data is correct. The basic principle behind this method is that the root counter's trust is transferred to its children by checking the tag's uprightness as well as the information blocks meanwhile, decency and addressing are accomplished. . This plan is additionally suitable for deflecting agreement assaults with the utilization of the

G. Multi Party Non-Repudiation (MPNR)

show. The information proprietor partitions the information into a few squares and encodes every one with a different key, then, at that point, makes a ticket for every client that contains the strategies for differentiating keys and opens squares. By scrambling the ticket with the client's public key, information and the hash tree are shipped to the cloud. By utilizing the Group encryption approach, the proprietor allows all clients admittance to the hash's root esteem. Accepting that the client of that get-together gets the hash regard, he can decipher and acquire the information and really look at the respectability. Tezuka.et.al propose the methodology

H. Assured Deletion and VErfiable Structure Control (ADEC)

which uses a two-phase appended key encryption design to protect data against rollback attacks. The data is separated into protuberances and blended. The keys that are used to scramble the metadata of the encrypted knots are stored in a key escrow system. The hysteresis mark is utilized for data authenticity insistence, which prevents aggressors from performing rollback or reordering of client data variations [12] [13] [21] [18] [9].

I. Solving Byzantine Failure and Malicious Data Modification Attacks

High Availability and Integrity Layer protocol (HAIL) is a cryptography system suggested by Bowers et al. ensures that client data is kept safe and accessible across a network of servers. For file distribution, erasure correcting coding is employed to provide redundancy and availability against misbehaving hosts. This proposed paradigm defends against both Byzantine and active adversary attacks. This is data loss resistant; however it only works with static data.To enable safe arrangement of disseminated stockpile management, an eradication coding method that is coordinated alongside an intermediary re-encryption plan is proposed. This plan also allows the client to distribute his information to other clients without having to recover it from the capacity servers. Homomorphic tokens and communicated eradication coded information are offered to overcome the Byzantine disappointment.

At the point when any blunder is distinguished while checking the honesty of the information, similar information can be recovered from different servers and afterward the bombed server can be refreshed with the first information. This plot have likewise been proposed and improved with the information elements property, where the client can refresh, erase, affix or addition information squares to his information. This arrangement system enormously decreases the correspondence and calculation upward, alongside solid information uprightness is given. The Reed Solomon deletion coding method is used to distribute the data, as well as overt repetitiveness equality parts, to multiple servers. This dispersion is done to reduce information loss due to an attack or failure on the server that stores the client's information. Furthermore, pre-computed homomorphic tokens are created for checking the specialist organizations prior to stealing the information to various servers. This cycle detects the trouble server and quickly completes information mishap limitation. Utilizing the similar homographic token and spread elimination coded information Cong et al. also advocated to defeat the Data adjustment assault. The testing approach he proposes, which focuses on a few columns rather than all lines, reduces the server's processing load. These strategies considerably reduce the issue of Byzantine disappointment and data modification.

J. Security Services

Recommendation ITU-T X.800 has six administrations linked to security aims and assaults have been identified as shown in figure 2.

K. Information Privacy

Information classification is intended to ensure the security of the information by ensuring that no one enters to acquire or know these facts, or by providing a specific service through which it is prevented from knowing the substance of the data on all supporters except those who have been granted permission to know and have this data. This means it was designed to prevent people from eluding traffic checks and assaults.

L. Integrity of Information

Information integrity aims to protect data from unauthorized changes (delete, add, or amend). It could protect the entire communication or just a portion of it.

M. Validation

A service or capability related to the verification of recognizable proof, or a strategy for confirming a client's character. The asset framework is expected to be verified.

N. Non-Repudiation

The non-renouncement administration defends against disavowal by the source or beneficiary of the information and proof ensures that no arrangement or activity will be denied in the not-too-distant future. The source of information can afterwards show that the information was passed on to the intended recipient, such as an advanced mark.

O. Access Control

Techniques for limiting access to an asset framework or a physical location. Unauthorized access to scrambled frameworks is prevented through access control.

P. Accessibility

Infers that the information can be accessed at any time, without interruption. An accessibility administration protects a system in order to ensure its accessibility. The security problems posed by denial of-administration assaults are addressed by this help. It is dependent on proper administration and control of framework assets, as well as access control administration and other security administrations.

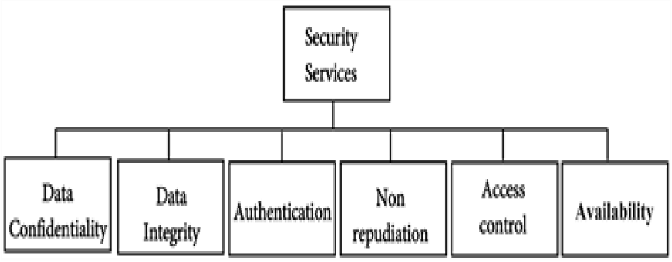

Figure 2: Cloud Security services

Q. Contrasts among Symmetric and Asymmetric Encryption Algorithms

With a similar key, symmetric encryption calculations encrypt and decrypt data. The primary advantages of symmetric encryption computations are their security and speed. With different keys, deviated encryption computations scramble and unscramble. A public key is used to scramble data, and a private key is used to decode it as shown in figure 3. To achieve a similar level of security as a 128-bit symmetric calculation, hilter kilter encryption computations (also known as public-key calculations) require a 3000-piece key. Topsy-turvy calculations are extraordinarily slow, and using them to encode a large amount of data is unfeasible. Symmetric encryption calculations are, for the most part, far faster to perform on a computer than deviated encryption calculations. In practice, they're frequently used combined, with a public-key calculation being used to encode a hastily generated encryption key and an arbitrary key being used to scramble the genuine message using an erroneous computation. This is sometimes referred to as half-breed encryption [17].

R. Block Ciphers and Stream Ciphers

The form of the input data they work on is one of the most prevalent categorization approaches for encryption systems. Block Cipher and Stream Cipher are the two types. This section compares the security and performance of the two types, as well as their main characteristics and operation modes. If facts are in the form of blocks, this approach encrypts and decrypts them. In its most basic mode, you divide the visible textual content into blocks, which are then fed into the cipher machine to generate cipher textual content blocks. If facts are stored in the form of blocks, this technique encrypts and decrypts them. We divide the seeming textual material into blocks, which are subsequently fed into the cipher machine to give blocks of cipher textual content in its simplest mode.

S. Data Encryption Standard (DES)

The Information Encryption Standard (DES) was developed by IBM in 1975 and published by the American National Standards Institute (ANSI) in 1981 as ANSI X3.92, making it one of the most widely recognized symmetric key standards today. DES uses a 56-bit key to scramble and decode data in 64-digit blocks. It takes a plaintext square of 64 digits as input and outputs a 64-cycle square of encrypted text. Because it works with squares of similar size and requires both alterations and replacements in the calculation. The principle calculation is rehashed numerous times to form the encrypted text in DES [24], which includes 16 rounds. It has been discovered that the number of rounds used is directly proportional to the amount of time required to observe a key using a savage power assault. As the number of rounds increases, the calculation's security improves considerably.

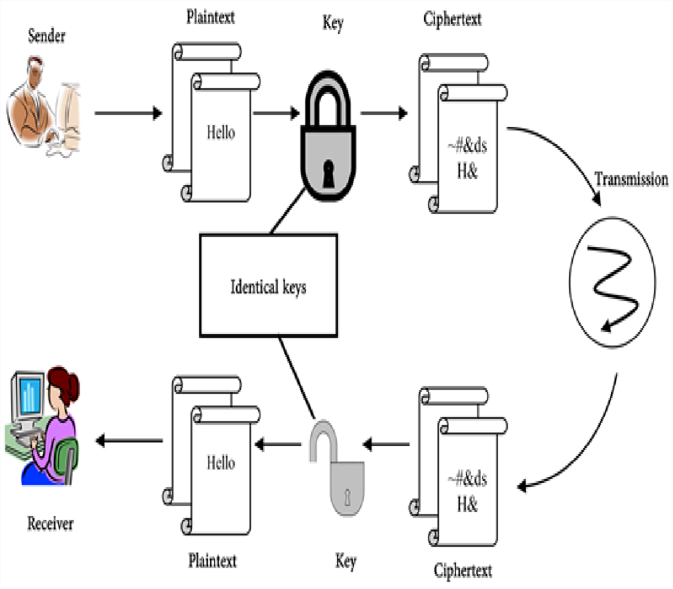

Figure 3: Method describes the work of encryption using a single key

T. Algorithm of the Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a symmetric key encryption algorithm that will eventually replace the widely used Data Encryption Standard (DES). It was the result of the US Government's National Institute of Standards and Technology (NIST) issuing a broad call for encryption computations in 1997, which was completed in 2000.In view of the increasing viability of DES attacks, NIST issued a request for proposals for an authority replacement that meets 21st-century security requirements. The Advanced Encryption Standard (AES) is the name of this replacement. It has fast key arrangement time and low memory requirements; also, its responsibilities are simple to defend against power and timing attacks. The triumphant calculation, Rijndael, was created by two Belgian cryptologists, Vincent Rijmen and Joan Daemen.

Blowfish

Bruce Schneier, one of the world's foremost cryptologists and the founder of Counterpane Systems, a consulting firm focused on cryptography and computer security, has produced one of the most extreme not uncommon public region encryption computations by way of method. Blowfish is a 64-digit block figure with a variable span key. In 1993, the Blowfish set of rules was first communicated. This set of criteria may be streamlined in equipment programmes, but it's not uncommon to see it applied in programming programmes. No attack is seen to be effective, despite the fact that it has defenseless keys.

Table 1: Execution time of various algorithms

Algorithm	Megabytes Processed	Time Taken	MB/Second
Blowfish	512	7.9	64.81
AES	512	8.75	58.51
DES	512	9.87	51.87

As per the Table 1, comparison to other calculations, the results showed that Blowfish had an exceptional overall execution. In addition, it was confirmed that AES has a better overall appearance than and DES. Surprisingly, it also recommends that 3DES has nearly 1/third the throughput of DES, or, in other words, that it takes three times as many samples as DES to send the same amount of data.

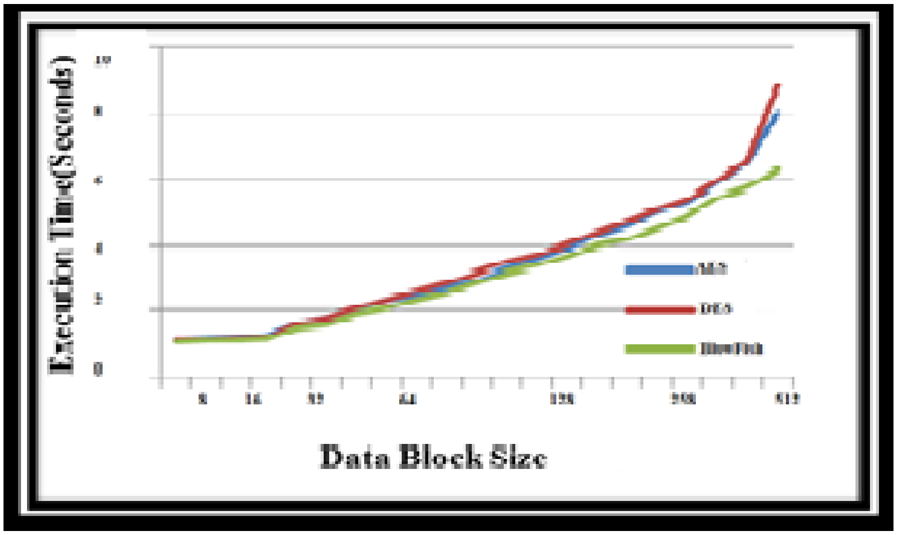

Figure 4: Performance Results with CBC Mode

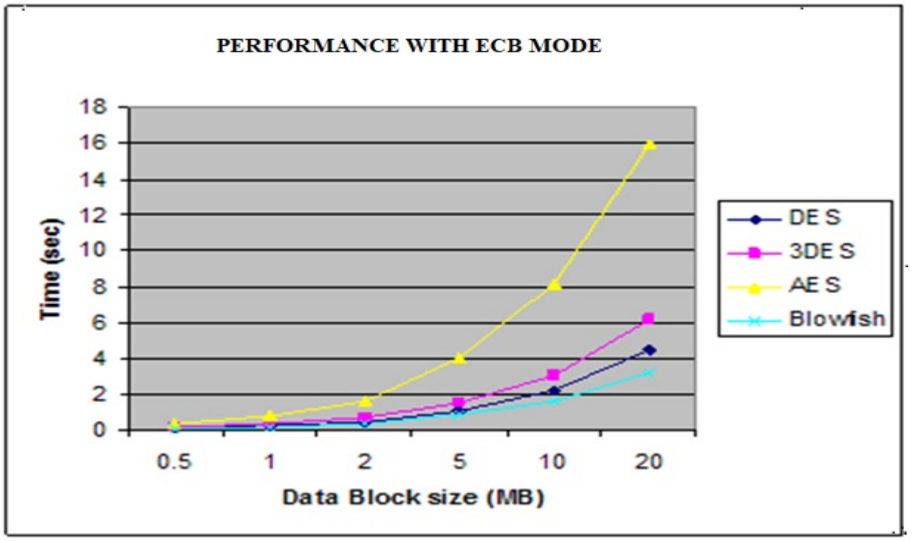

Figure 5: Performance Results with ECB Mode

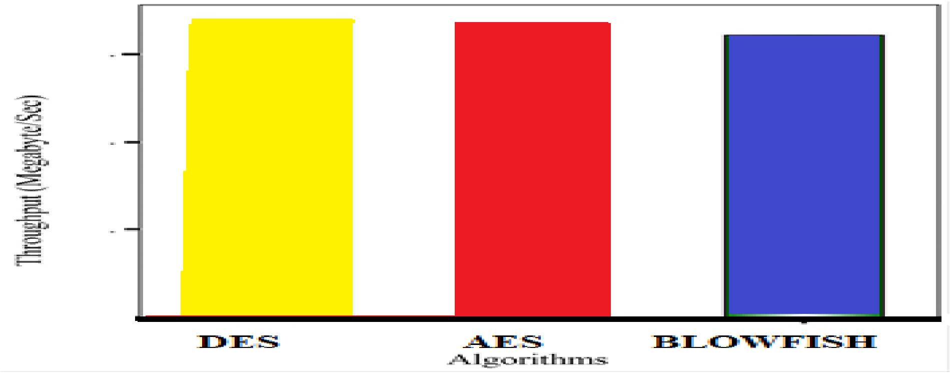

Figure 6: Throughput of Algorithms

III. CONCLUSION

Distributed computing, which is seen as the way of the future by certain IT organizations, currently has a few flaws. Distributed storage is a well-known administration provided by cloud providers for storing client data on a remote server. Despite the fact that Cloud providers claim that the data they store will be secure and pristine, there have been security breaches that have resulted in the loss of data trustworthiness. Many creators presented various mechanisms to mitigate the desecration of information caused by these assaults. These solutions work well and keep clients' information safe. To maintain Cloud's reputation amid adversaries, current techniques and upcoming procedures greatly assist the arising Giant known as Cloud calculating to be effective among Cloud clients. Encryption calculations play an important role in correspondence security, with encryption time, memory usage yielding bytes, and battery consumption being major concerns. For execution evaluation, the chosen encryption algorithms AES, DES, and BlowFish are used. Based on the text records used and the test results, it was deduced that DES calculation consumes the greatest encryption time and AES calculation consumes the least memory, while the difference in encryption time is extremely minimal if AES and DES calculations occur. Blowfish uses the least amount of memory and takes the least amount of time to encrypt. The presented results in figure 4, figure 5 and figure 6 revealed that Blowfish has a better presentation than other commonly used encryption calculations. Since Blowfish has never been discovered to have any security flaws, it's a strong contender to be deemed a standard encryption computation. Because it necessitates considerable handling power [22], AES produced poor showing outcomes as compared to other calculations. Using CBC mode added some processing time, but it was mostly insignificant in most cases, especially for applications that require secure encryption of fairly large data blocks.

REFERENCES

[1] Kumar, A.Y. (2013) Comparative Study of Different Symmetric Key. International Journal of Application or Innovation in Engineering & Management, 2, 204-206.

[2] Microsoft - White paper, "Forecast: Improved economy in the cloud,", ww.microsoft.com/government, March 2010.

[3] Rajkumar Buyya, James Broberg and Abdrzej Goscinski, "Cloud Computing Principles and Paradigm,", John Wiley and Sons, Inc publication, 2011.

[4] Amazon, "Amazon Web Services," http://aws.amazon.com/,

[5] Brian Hay, Kara Nance and Matt Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing,", In., Proc, of Hawaii International Conference, IEEE – 2011

[6] Subashini S, Kavitha V. "A survey on security issues in service delivery models of cloud computing.," Network Compute App. (2010), doi: 10.1016/j.jnca.2010.07.006, Elsevier.

[7] R. Sravan Kumar and A. Saxena, "Data integrity proofs in cloud storage," in 2011 Third International Conference on Communication Systems and Networks (COMSNETS), 2011, pp. 1-4.

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Service Computing (TSC), 2012

[9] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multi-cloud storage," IEEE Transactions on Parallel and Distributed Systems, no. 99, 2012.

[10] J. Feng, Y. Chen, W.-S. Ku and P. Liu, "Analysis of Integrity Vulnerabilities and a Non-repudiation Protocol for Cloud Data Storage Platforms," 2nd International Workshop on Security in Cloud Computing (SCC 2010), San Diego, California, USA, Sep. 14, 2010.

[11] Un Feng, Yu Chen, Douglas H. Summerville, and Kai Hwang "Fair Non-repudiation Framework for Cloud Storage: Part II," in Cloud Computing for Enterprise Architectures, Springer - 2011, pp. 283-300.

[12] Feng, Y. Chen, D. Summerville, W.S. Ku, and Z. Su. "Enhancing Cloud Storage Security against Roll-back Attacks with A New Fair Multi-Party Non-Repudiation Protocol,", in The 8th IEEE Consumer Communications & Networking Conference, 2010.

[13] A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584-59

[14] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598-609.

[15] Abdel-Karim Al Tamimi Performance Analysis of Data Encryption Algorithms https://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/#Dhawan2002

[16] Yogesh Kumar, Rajiv Munjal, and Harsh Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures ,(IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 - 4853

[17] AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram Comparative analysis of performance efficiency and security measures of some encryption ISSN: 2248-9622

[18] Hamdan.O.Alanazi, B.B.Zaidan, . A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani New Comparative Study Between DES, 3DES and AES within Nine Factors JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617

[19] Ritu Tripathi, Sanjay Agrawal Comparative Study of Symmetric and Asymmetric Cryptography Techniques . IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011 ISSN (Online): 2231-5268

[20] Manisha Mahindrakar Evaluation of Blowfish Algorithm based on Avalanche Effect International Journal of Innovations in Engineering and Technology (IJIET) 2014

[21] RituPahal, Vikaskumar, Efficient Implementation of AES, Volume 3, Issue 7, July 2013 ISSN: 2277 128X, © 2013, IJARCSSE

[22] Pratap Chandra Mandal Superiority of blowfish Algorithm , , Volume 2, Issue 9, September 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[23] A study and performance of RSA algorithm, IJCSMC, Vol. 2, Issue. 6, June 2013, pg.126 – 139, ISSN 2320– 088X

[24] Karthik .S ,Muruganandam Data encryption and decryption by using triple DES and performance analysis of crypto system.A, ISSN (Online): 2347-3878 Volume 2 Issue 11, November 2014