International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 07, Issue: 03 (May- June, 2021)

RESULT AND ANALYSIS OF A NOVEL DATA SECURITY METHOD OVER CLOUD COMPUTING USING HYBRID TECHNIQUES

Raval Dharabahen Bhupendrabhai, Pankaj Richhariya

Abstract— Nowadays, Computers networks are significantly used for the transmission of data. Information security has become the main problem while using an anxious network like the internet to allocate confidential data such as credit tag information and electronic forms. The information cannot be transmitted in unencrypted form as an attacker may intercept it. So, to secure sensitive data, a cryptographic algorithm is required. Recently, various researches are being done to germinate a strong encoding algorithmic program to improve the security of the data than traditional existing algorithms. A symmetric key encryption scheme is obtained by vigorously creating the matrix depending on the data size. The key is obtained in the array of the formed matrix. The logical action and encrypted matrix increase the intensity of safety.

Keywords:- Cryptography, Chunk Speed, Hybrid Cloud, Encryption, Decryption.

1. INTRODUCTION

In today's Information Technology epoch, processor networks are usually used to share information and communicate with others. The chances of compromising the information being transferred over the networks are ever-increasing. Susceptible data must be protected from unauthorised admittance from transmitting over insecure and timid networks, for instance, the Internet. Safety measures during transmission of data have become one of the difficult challenges over the networks. To deal with data safety issues, Cryptography is one of the techniques. It is based on encryption and decryption algorithms for the secure transmission of data over the network. It is a technique used for thousands of years to keep the data secure from others. Modern cryptography techniques are used to provide safety measures that use arithmetic techniques based on two essential components: An algorithm and a key used to establish the algorithm operation. This modern cryptographic method aims to attain the security goals such as data secrecy, data reliability, non-repudiation and verification. They use computer networks to transfer credit card information, electronic transfer credentials, and online shopping. Every single transmission requires a well-organised security system. There is a possibility of interpreting the information by an unauthenticated third party. Cryptography is a proficient method that uses encryption and decryption to secure the data from illegal access to conserve reliability and isolation of data. Encryption and decryption methods are used.

The plaintext is the original form of data, and the ciphertext is the encrypted form of data. Encryption techniques obtain pure content (the original form of data) as an input and translate it into ciphertext (an encrypted form of data) based on an input algorithm using a secret key. An input is a component-based on which information is encoded. The decryption technique obtains the encoded text (an encrypted form of data) and converts it into plain text (the original form of data) based on an algorithm using a key input. Cryptography algorithms are classified into two categories based on the keys used: Bilaterally symmetric Key Coding algorithms and Unsymmetric Key Coding algorithms. In the Symmetrical coding method, solitary key input is required for encoding and decoding the data.

A key input is a transfer to both sender and recipient proceeding to connection. It is also best-known as a surreptitious key cryptography algorithm. On the further side, the Asymmetrical key Coding method put a key input in a couple well-known as the private key and public key. The public key is utilised for encoding the content, but the private key is utilised to decipher the content. They are also called public-key cryptography techniques. Symmetric key encryption is faster than asymmetric key encryption.

2. LITERATURE SURVEY

In this part, the literature survey is done to understand the cryptography field in detail, and the problems associated with it is described. The gaps in the existing work are identified to develop the proposed methodology and presented in the following sections.

IMPORTANCE OF CRYPTOGRAPHY:

Nowadays, computer networks are significantly used by billions of people for banking, shopping [1]. Security has become a challenging issue for communicating the data over the networks. Every time there may be a threat to the security of the data. Attackers try to intercept the message being transmitted over the networks.

CRYPTOGRAPHY:
Cryptography is a technique that secures information from unauthorised access. Encryption algorithms and key are the basic components of cryptography. The simple text is transformed into encoded text (encrypted form) using an encoding algorithm known as the encryption method. The coded text is transformed into original text using a decoding algorithm known as the decryption method.

3. PROBLEM STATEMENT
Nowadays, there are several cryptography algorithms available that ensure the security or certification of the content. The necessity to assist the data has magnified with the section of information processing system networks. In the same way, the attacks on the data are also increasing to break the security. The traditional cryptography methods cannot be useful in today's computing world. Thus, the use of modern cryptography approaches is significantly increasing for protecting the data in comparison to the issues related with the traditional approaches such as:

- Generation of the large ciphertext consumes a huge amount of gap.
- Enhance the encryption and decryption time through the rise in the quantity of data.

4. PROPOSED ALGORITHM
Different cloud computing data storage techniques allow users to perform their applicability over the data centre, server, and access. Multiple file upload and its usage make to access it from the cloud data storage and its server.

As the study is in use and performed with unusual technology and unusual consequence from the algorithms such as RSA, AES, Hash-Based and other additional technique for information processing, safety approach over information accumulate. Furthermore, dissimilar services' methodology for safety over the cloud statistics is performed to formulate it more protected and reachable.

In the lead verifying different state and the access method, different tiny comes with the Existing algorithm AES-SHA2 with organiser based re-duplication, which is in use as a foundation for our investigation work.

The subsequent are the maintained points recognised as trouble, and supplementary analysed and performed further with enhancements.

1. A prior method such as file-based scheduling doesn't overcount all its data parts or internal division, duplicating over a large amount of data. Thus, efficient monitoring is required, which can further be monitor file duplicacy with data division.

2. AES algorithm takes advantage of the asymmetric encryption technique used by base paper, but still when we talk about the multiple tenants, multiple ownership, and multiple users over the data. Thus, the security of key sharing is still a challenging issue which authors face.

3. The Key length taken for security purpose in previous research is not considered today. Today's scenario required an efficient and long length key for security purpose.

4. The existing approach for security uses MD5 for the hashing for content matching, but the MD5 algorithm faces collision issue with value generation. The hashing algorithm is the best practice to have a long hash value.

5. RESULT & ANALYSIS
5.1 PLATFORMS AVAILABLE

The description of some platforms is presented, which can be used to implement the proposed method.

Eclipse :
It is an integrated development environment. It is mainly written for Java but has features that use plug-ins and provide development environments for other programming languages like C/C++, FORTRAN, COBOL, PERL, PHP. It is an open-source software development environment; the Eclipse Software development kit is easily available to develop their programs.

Dotnet :
It is a software development framework developed by Microsoft mainly run on the Microsoft Windows platform. It uses a large class library called Framework class library (FCL) and provides language interoperability for many

programming languages. It uses common language runtime (CLR), a development environment, to run the program. FCL and CLR jointly constitute a .NET Framework.

Java with NetBeans Ide :
Java is a high-level programming language. With a compiler, a Java program is translated into an intermediate language called Java byte codes--the platform-independent codes interpreted by the Java interpreter. With an interpreter, each Java byte code instruction is parsed and run on the computer. Compilation happens just once; interpretation occurs each time the program is executed.

Every Java interpreter, whether a Java development tool or a Web browser that can run Java applets, implements the Java VM. Java byte codes help make "write once, run anywhere" possible. The Java program can be compiled into byte codes on any platform that has a Java compiler. The byte codes can then be run on any implementation of the Java VM.

NetBeans IDE is a software development environment written in Java. It was developed in 1996 as Xelfi by a java student under the guidance of the faculty of mathematics and physics in Charles laboratory Prague in 1997. Roman Stanek introduced the commercial version of NETBEANS IDE; further, it was bought by Sun Microsystem in 1999.

It mainly written for JAVA but also provide an environment to develop programs in other languages like C/C++, PHP. It is an open-source framework that uses JVM to provide a development environment that makes it platform-independent.

NetBeans Ide is multi-platform and runs on MS WINDOWS, MAC OS, LINUX, SOLARIS and other platforms which support compatible JVM.

We are building an application which is provided two feature authentications. For developing this relevance, we are using JDK 1.8 that is JAVA developing kit.

Java is a computer language. It helps developer to write computer instruction using English based commands. This type of language is known as "high-level language" because it is stable and easily written by human.JAVA has a set of rules that determine how the instruction is written. These rules are known as their "syntax". Once a program has been written, the high-level instruction is translated into numeric codes that computers can understand and execute. Web-based content and enterprise software. JAVA development kit a software development kit (SDK) for producing JAVA programs. The JDK is a development by Oracle INC java soft division.

How to use CloudSim with NetBeans
Step1 Setting up Development Environments: CloudSim is a simulator that does not have a GUI application for user interaction, so we can run this simulator using command prompt or use GUI developed for java programming languages. Now we can use either Eclipse or NetBeans as an interface for interacting with the source code of CloudSim. We also required JDK for java programming and some libraries which are used in the CloudSim. Download CloudSim zip file, extract and open it in the NetBeans. We use the CloudSim 3.0.3 version of the CloudSim.

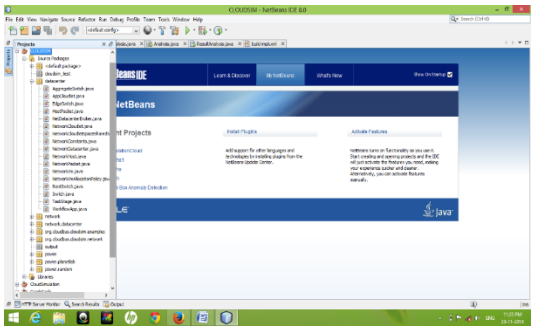
Fig 1: Deploying CloudSim into NetBeans

Step2 UseCloudSim with NetBeans: In the CloudSim, source codes are given for the cloud computing functionality. Since cloud computing is a technique that provides computing as a source rather than an invention, so CloudSim provides us with the resource codes for these concepts. In cloud computing, the implicit machine is used for computation purpose, so source code for creating a virtual machine, broker, cloud servers given in the CloudSim.

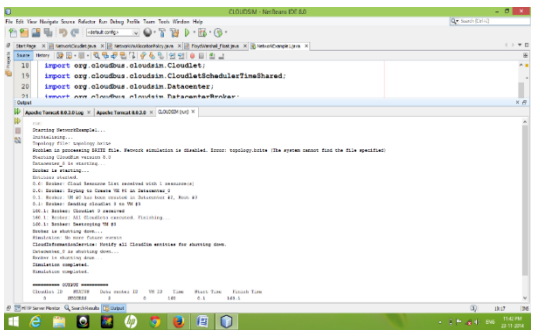
Fig.2: Execution of CloudSim example in NetBeans

Step3 Run Source code using CloudSim: To run our source code using CloudSim, we have to link our source code with CloudSim. So, we have to

write code for cloud concepts and then link our source code with CloudSim to enjoy the functionality of the CloudSim.

SYSTEM DESCRIPTION

Here in our investigation, we are experimentally available to offer a recreation of a Peer communication scheme where uncertainty work with unusual circumstances interrelated to precedent performance of query and data processing method and help give the exact result. Here are the described outcome screen and specific discussion on the subject of the result. Different operations we can provide and can be valid once we execute the verification process on the proposed technique. Here we have established our work in different respects and practical the result and evaluate the results based on the research performance we have observed and notified that the proposed algorithm can be more superior when we are using the Blowfish expansion technique before applying the purpose data process method while dealing with the protected system before the client can describe the things.

5.2 PERFORMANCE MEASURES

5.2.1 Computation Time :

An instruction time of a dataset in Java is computed with the help of initial and final time class variables distinct in the device, and here as we load the dataset and verifies the eligibility and taking their features for consideration or not is the time taking process to recognise and to load the images and selection of password comes under training time of a dataset, extracting the properties and making them in process configure is training time.

Ct = final time completion – initial time;

5.2.2 Bandwidth :

A Bandwidth in the cloud and network server is the total consumption of data amount in its process. All the data consumption, including the coding part, client end graphics and many other related components. They are finding the usage. All the combination data usage by all resources get to the bandwidth computation.

Bw = summation of (all data usage by resources);

5.2.3 Traffic Volume :

Traffic volume is also one of the important parameters of monitoring the parameter for comparison. It can be computed as total work performed by the available resources. It is the product multiplication of traffic intensity with time.

Tv = traffic intensity * time;

5.2.4 Traffic Cost

A specific amount of financial unit measures the volume and convert it into the traffic cost.

Tc = Tv* basic unit cost value;

5.2.5 Chunk Speed

A chunk speed can be defined in MBPS or KBPS, and it is specifically the speed at which chunking is performed either at the sender side or either receiver side. Observation: In result analysis, the coordination acceptance specifies that I have applied various accidental click and practically most admirable analysis results.

CONCLUSION

Cloud computing is an emerging area of research, where most of the IT infrastructure is moving to make their service and delivery more efficient. Cloud computing makes it more scalable, more reliable, secure and accessible, with plenty of option to perform its best. Our work approach leads behind the multiple copies and duplicate data uploading over the cloud and its different data centre in this Dissertation due to different possession. The idea following the study is to take a secure and consistent algorithm approach that can get the result for safety measures and re-duplication redundancy optimisation over the data store.

The presented paper discussed the file point allocation and redundancy recognition through file-level chunking, wherever as to broadcast and stock up the information AES (Asymmetric encryption system) algorithm to give data safety. They have also used MD5 for hashing calculation. The safety measures and hashing algorithm evaluate a long intermission to calculate and in the region where huge data files are obtainable. The presented de-duplication algorithm also a great deal efficient with the large data file.

Thus, to defeat these issues related to the established paper approach. Our optimisation algorithm PROPOSED algorithm with extra secure algorithm blowfish is performed along with SHA-2 as a more constant hashing approach. Our algorithm, in addition, checks for appropriate redundancy using more secure and consistent parameters.

Our proposed algorithm uses comparison parameter as computation time and computation

cost to compute the comparison analysis. The algorithm is a developer in Java language with Java net-beans tool setup using intel i3 processor, 750 GB RAM. The comparison analysis and execution result shows that our proposed approach outperforms best while comparing with the existing algorithm.

REFERENCES

[1]. Jianghong Wei, Wenfen Liu, Xuexian Hu "Secure Data Sharing In Cloud Computing Using Revocable-Storage Identity Based Encryption"-PKC 2015.
[2]. Seo and Emura," Towards black-box accountable authority IBE with short ciphertext and private keys, in Public Key Cryptography"–PKC 2009. Springer, 2009, pp. 235–255.
[3]. J. H. Seo and K. Emura, "Revocable identity-based encryption revisited: Security model and construction, in Public-Key Cryptography"–PKC 2013. Springer, 2013, pp. 216–234.
[4]. K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Computer Security-ESORICS 2014.Springer, 2014, pp. 257–272.
[5]. S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralised access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.
[6]. K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.