IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

An Approach towards Data Security in the Cloud Computing Using AES

Santosh Kumar Singh[1], Dr. P.K. Manjhi[2], Dr. R.K.Tiwari[3]

Research Scholar, Department of Computer Applications, Vinoba Bhave University, Hazaribag, India [1]

Assistant Professor, University Department of mathematics, Vinoba Bhave University, Hazaribag, India [2]

Professor, H.O.D CSE, R.V.S College of Engg & Tech., Jamshedpur, India [3]

Abstract: With the rapid development of Internet technology, the data of the user's information have raised up largely, so internet storage became more and more important in today's life. The intelligence and networking development of the electronic products, meeting the needs of the public users or the businesses for portable and high capacity has become the most important in development of the information industry. Cloud storage has become the preferred option to provide portable storage service for ordinary users, solve the requirement of large capacity, the difficulty of management and the requirement of high generic extensions. The security mechanism of cloud storage system is also becoming more and more important. By using AES encryption algorithm the security mechanism of users' files uploading and downloading has been researched. So in this paper a new algorithm is introduced, regarding the extent of Cloud network, the most important feature of the proposed algorithm is its resistivity against the attacks. The algorithm is designed and implemented in java script in CloudSim environment. The objective of this paper is the development and creation of a new algorithm by implication of some changes in the initial key of AES encryption algorithm.

Keywords: Security, Data security, Cloud computing security, Cryptography, AES Encryption Algorithm, CloudSim.

I. INTRODUCTION

There are various types of computing available in current digital world which are effective for various purposes but all they have their different features for different aspects like parallel computing, cluster computing, grid computing, utility computing and cloud computing.
Cloud computing is a recent development in information technology that moves computing and data away from desktop and portable PCs into large data centre. It refers to applications delivered as services over the internet as well as to the actual cloud infrastructure namely, the hardware and systems software in data centers that provide these services. In general, clouds provide services at three different levels namely infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) [1].

• IaaS serves the computational resources that may include high end servers, storage systems, networking technology and staffing expertise. Amazon, Verizon, Rackspace are some of the key players in IaaS.
• PaaS serves availability of application development platform through the cloud infrastructure. By using PaaS, the application developer can develop and deploy new applications without any investment in infrastructure. During the time of development, PaaS manages the software development life cycle like planning, designing, developing, testing and maintenance. Microsoft Azure, Google AppEngine, Force.com, AppJet, Etelos, and Qrimp are the key players in PaaS.
• SaaS serves the application software like customer relationship management, enterprise resource planning, and accounting software. Salesforce.com, Google Apps, Microsoft Business Productivity Online Suit and facebook are the big names in SaaS.
The three major cloud deployment models [2-4] are as follow:

- In the public cloud model, the resources are dynamically provisioned on a fine-grained, self-service basis over the internet, via web services. The customers can quickly access these resources, and only pay for the operating resources. As multiple customers are sharing the resources so major dangers to public cloud are of security, regulatory compliance and quality of service (QoS).
- In the private cloud model, computing resources are used and controlled by a private organization. In private cloud, resource access is limited to the customers that belong to the same organization that owns the cloud.
- A third model can be hybrid cloud that is typical combination of public and private cloud. Through this model an organization can provide and manage different resources in-house and have others provided through external resource.

In cloud environment, a data centre holds information that client or end-users would more traditionally have stored on their own database. This raises concerns regarding user privacy protection because users must outsource their database. Deploying an autonomous system to efficiently provision services in a cloud infrastructure is a challenging problem due to the unpredictability of consumer demand, software and hardware failures, heterogeneity of services,

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

etc. Security requirements in the context of cloud computing are as follow [1]

- Authorization is one of the important security elements in cloud computing to ensure referential integrity. In case of public cloud, multiple customers share the computing resources provided by a single service provider, so proper authorization is required irrelevant of the delivery model used.
- Data collection, internal threats, external threats, privacy and compliance are the major concerns in public and private cloud. So, it is the cloud service provider's ability to have a secure infrastructure to protect customer data and guard against unauthorized access.
- In database as a service (DBaaS), atomicity, consistency, isolation and durability (ACID) properties of the cloud's data should without a doubt be robustly imposed across all cloud computing delivery models.
- In all cloud models, confidentiality plays a major part especially in maintaining control over organizations' data situated across multiple distributed databases. Asserting confidentiality of users' profiles and protecting their data, that is virtually accessed, allows for information security protocols to be enforced at various different layers of cloud applications.

The cloud computing model is not without concerns, as others have noted [4]. The following are the primary concerns,

- Economics of failure: The uptime of cloud computing-based solutions is an advantage, when compared to businesses running their own infrastructure, but often overlooked is the co-occurrence of downtime in vendor-driven monocultures. This was illustrated by the Amazon (S3) cloud outage, which took with it several other dependent businesses.
- Convenience vs. control: The growing popularity of cloud computing comes from its convenience, but also brings vendor control, an issue of ever-increasing concern.
- Environmental impact: The other major concern is the ever-increasing carbon footprint from the exponential growth of the data centers required for cloud computing.

We need to have some identification and authentication process to verifying and validating individual cloud users based upon their credentials before accessing any data over the cloud. That is why identification and authentication is mandatory security requirement in all three cloud models. To enhance the security in cloud network, this paper attempts to present a method for security establishment in cloud environment through proposed algorithm.
The proposed approach is based on development of AES Encryption Algorithm, which is different from conventional security schemes in cloud computing. In continue, the section II expresses the works in relation with security in cloud and development of AES Encryption Algorithm. The proposed approach is presented in section III. In section IV its implementation and compared with previous methods. Finally, the conclusion and future works is presented in section V.

II. AES ENCRYPTION

The Advanced Encryption Standard (AES), also known as Rijndael, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.
AES [5] is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits as shown in Fig. 1.

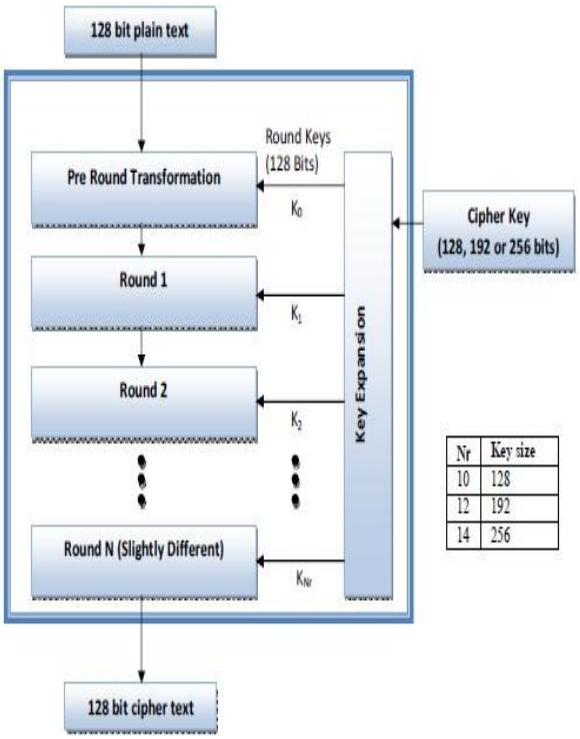

Fig. 1. AES Encryption process

AES operates on a 4 × 4 column-major order matrix of bytes, termed the state For instance, if there are 16 bytes, $b_0, b_1, \ldots, b_{15}$, these bytes are represented as this matrix:

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

DOI 10.17148/IJARCCE.2016.5605

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition is as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key, as shown in Fig. 2.

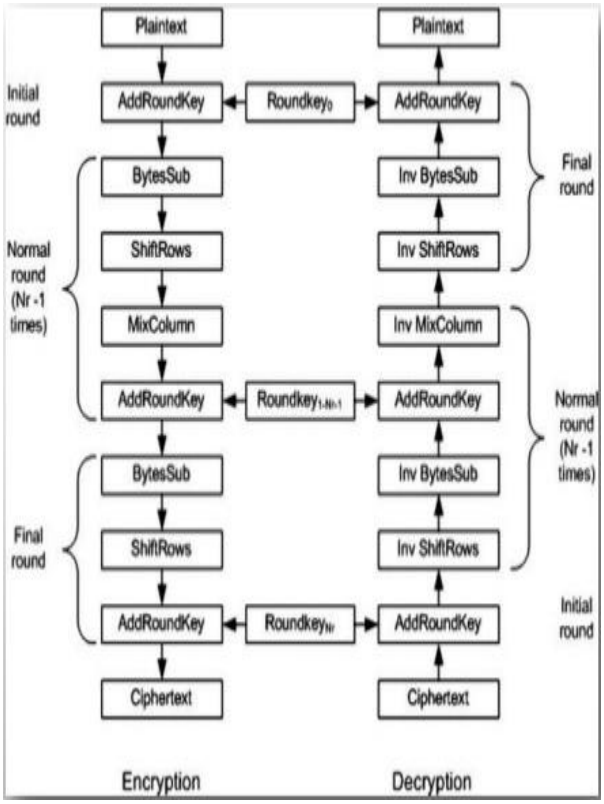

Fig. 2. AES Encryption and Decryption

Description of the algorithm and how it works shown in Flow chart Fig. 3.

1. Key Expansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial Round
1. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds
1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. AddRoundKey
4. Final Round (no MixColumns)
1. SubBytes
2. ShiftRows
3. AddRoundKey.
4.

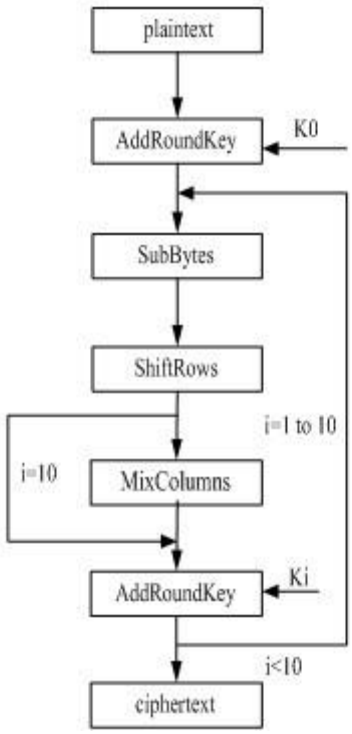

Fig. 3. Flow chart of AES Encryption Algorithm

AES has the optimized efficiency, speed and security. The below Fig. 4, illustrate the superiority of AES over other methods.

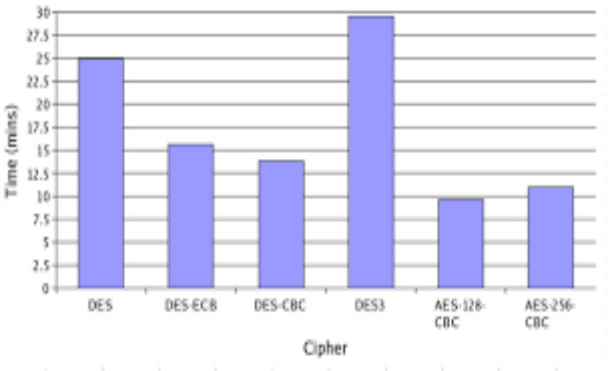

Fig. 4. Encryption Performance

When file size increases like 1kb, 5kb, 500kb, 1000kb respectively the performance of algorithms decreases as shown in Fig. 5 but among all, AES encryption performing better than other [6].

DOI 10.17148/IJARCCE.2016.5605

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

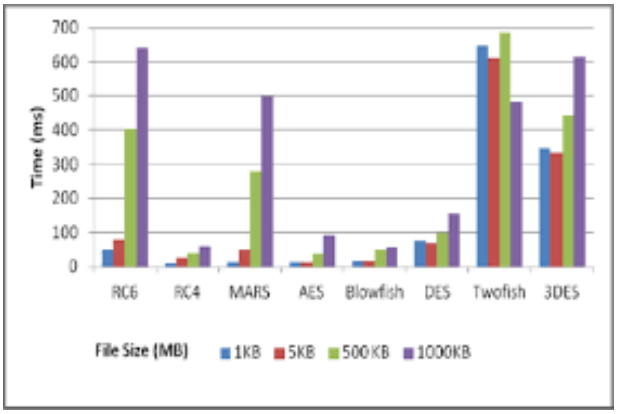

Fig. 5 comparison of the speed of encryption algorithms

AES algorithm is very fast, and as it applies the iterative operations, parallelization is possible. Also, since the environment is inherently a distributed environment with high volume of data, AES algorithm is suitable for cloud data; however, attacks such as side channel have been reported [7, 8].

The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use [9].

III.PROPOSED APPROACH

The proposed approach is addressed here. The objective is the development and creation of a new algorithm by implication of some changes in the initial key of AES encryption algorithm. As it was mentioned before, due to parallelization technique and use of piece encryption, AES algorithm is so fast. This means that each piece could be assigned to one processor and the calculation could be done in parallel. In the proposed method, 128-bit AES is used which divides the data into 4 equal pieces and 4 processor perform the calculation in parallel. As the environment is inherently distributed with high data volume, AES is an appropriate algorithm for cloud data.

However, attacks such as side channels were reported. As it can be seen, AES algorithm is faster and more efficient than the other algorithms, so it is an appropriate choice. Now this proposed model attempts to optimize the security and create a complicated initial key. Stronger the key of the algorithm, more effort is needed to hack. The proposed model also shows that by the changes in AES algorithm and application of parallelization techniques, the speed would remain constant. One of the major concerns of symmetrical algorithms such as AES is sharing of the key. The solution of this paper for key transfer is as follows: they must be transferred physically or the key is divided into several parts and sent by different communicational channels to protect the security of the key. For construction of the initial key of AES algorithm, two methods from cellular automata along with phase operators were used. The reason for application of phase operators is solving the problem arisen from algebraic and mathematical definitions and production of more precise key [10]. By application of binary cellular automata, several keys will be created and one will be selected randomly. This can be used as the key in AES encryption algorithm. Due to application of phase operators, a more precise and non-repetitive key would be created. In the proposed method, by application of cellular automata 90 law and substitution of Boolean operators with phase operators, the phase 90 law is created.

The cellular automata 90 law could be considered as: a'b'c+a'bc+ab'c'+abc' Reports and experiments show that by application of the phase laws, the uniform random numbers with desirable quality are obtainable [10]. The possibility of implication of this method in parallel and its high speed along with its desirable quality are among the distinctive features of this method.

In the proposed model, the initial key of AES encryption algorithm must be developed by use of cellular automata and phase operator. The reason of application of cellular automata is its high speed and possibility of parallelization and the reason behind the use of phase operators is its accuracy and uniformly distributed random numbers. The mechanism of proposed algorithm is as follows: by application of cellular automata and phase operator several keys are created. In the next step, one key is randomly selected and the rest of steps are like AES algorithm. The decoding operations are not changed and use the same AES algorithm. Regarding these added properties, proposed algorithm resolves the problems and bugs of AES algorithm which makes it an appropriate algorithm in distributed environment of cloud.

In fact, proposed algorithm is the same as AES algorithm with this difference that it produces more complicated keys to be more resistant against attacks. As we know, one of the main parts of all algorithms is encryption of their keys. In the proposed model, the key of AES is constructed more resistant and reliable. One of the advantages of proposed encryption algorithm is its speed and efficiency which is inherited from AES algorithm.

IV. IMPLEMENTATION AND COMPARED WITH PREVIOUS ALGORITHM

Proposed algorithm can be used in parallel in cloud environment with huge amount of data. The implementation steps of proposed algorithm are as follows: first, by application of cellular automata and phase operation FAC (Fuzzy Cellular Automata), several words will be produced.

In the next step, one key is randomly selected as the initial key of proposed algorithm, and then encryption stages will be started, as shown below in Fig. 6.

DOI 10.17148/IJARCCE.2016.5605

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

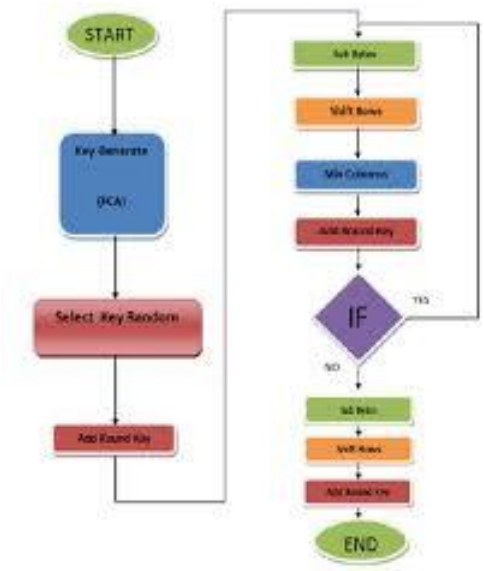

Fig. 6. Proposed algorithm

As it was mentioned before, one of the advantages of the proposed algorithm is its high speed due to use of parallelization technique. Fig. 7 shows the number of processors in each step. Due to large numbers of communications between the processors, shift rows stage is implemented in series.

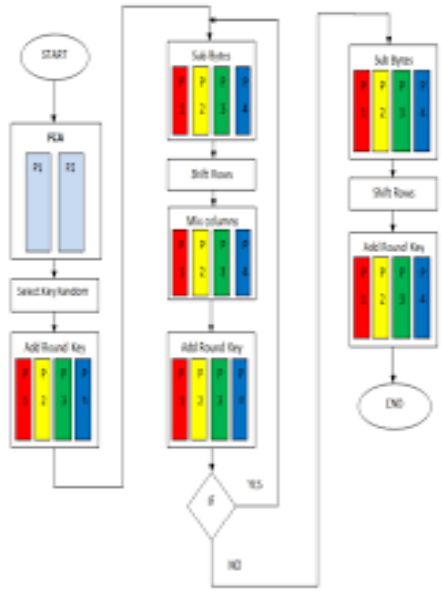

Fig. 7. Proposed algorithm implemented in parallel

The experiments showed that by addition of phase operators, the efficiency and speed of the algorithm remained unchanged. Because cellular automata random producer and phase logic have the capability to be performed in parallel, therefore, in addition to retaining the algorithm efficiency, its strength against the attacks is improved. By employment of cloudsim simulator, proposed algorithm was tested on several virtual servers and it was proved that the efficiency and speed of the proposed algorithm remained unchanged. Below Fig. 8, indicates that.

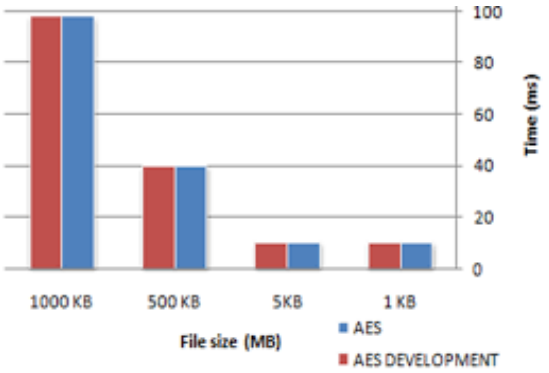

Fig. 8. Keeping the speed constant in proposed algorithm

CloudSim provides a generalised and extensible simulation framework that enables seamless modelling and simulation of app performance. By using CloudSim, developers can focus on specific systems design issues that they want to investigate, without getting concerned about details related to cloud-based infrastructures and services.

Simulation is important for the cloud environment [11] because Cloud service providers offer elastic, on-demand, and measured infrastructure, platforms and software services. In the public cloud, tenants have control over the OS, storage and deployed applications. Resources are provisioned in different geographic regions. In the public cloud deployment model, the performance of an application deployed in multiple regions is a matter of concern for organisations. Proof of concepts in the public cloud environment give a better understanding, but cost a lot in terms of capacity building and resource usage even in the pay-per-use model.

CloudSim, which is a toolkit for the modelling and simulation of Cloud computing environments, comes to the rescue. It provides system and behavioural modelling of the Cloud computing components. Simulation of cloud environments and applications to evaluate performance can provide useful insights to explore such dynamic, massively distributed, and scalable environments.

The principal advantages of simulation are:

- Flexibility of defining configurations
- Ease of use and customisation
- Cost benefits: First designing, developing, testing, and then redesigning, rebuilding, and retesting any application on the cloud can be expensive. Simulations take the building and rebuilding phase out of the loop by using the model already created in the design phase.
- CloudSim is a toolkit for modelling and simulating cloud environments and to assess resource provisioning algorithms.

CloudSim is a simulation tool that allows cloud developers to test the performance of their provisioning policies in a repeatable and controllable environment, free of cost. It helps tune the bottlenecks before real-world deployment.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

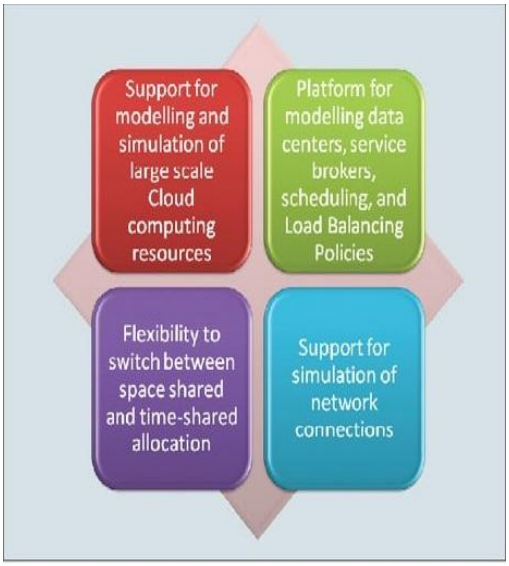

Fig. 9. Features of CloudSim

It is a simulator; hence, it doesn't run any actual software. It can be defined as 'running a model of an environment in a model of hardware', where technology specific details are abstracted.

CloudSim is a library for the simulation of cloud cenarios. It provides essential classes for describing data centers, computational resources, virtual machines, applications, users, and policies for the management of various parts of the system such as scheduling and provisioning. Using these components, it is easy to evaluate new strategies governing the use of clouds, while considering policies, scheduling algorithms, load balancing policies, etc. It can also be used to assess the competence of strategies from various perspectives such as cost, application execution time, etc. It also supports the evaluation of Green IT policies. It can be used as a building block for a simulated cloud environment and can add new policies for scheduling, load balancing and new scenarios. It is flexible enough to be used as a library that allows you to add a desired scenario by writing a Java program. By using CloudSim, organisations, R&D centers and industry-based developers can test the performance of a newly developed application in a controlled and easy to set-up environment. The prominent features offered by CloudSim are given in Fig. 9.

Architecture of CloudSim: The CloudSim layer provides support for modelling and simulation of cloud environments including dedicated management interfaces for memory, storage, bandwidth and VMs. It also provisions hosts to VMs, application execution management and dynamic system state monitoring. A cloud service provider can implement customised strategies at this layer to study the efficiency of different policies in VM provisioning.

The user code layer exposes basic entities such as the number of machines, their specifications, etc, as well as applications, VMs, number of users, application types and scheduling policies. The main components of the CloudSim framework are, Regions: It models geographical regions in which cloud service providers allocate resources to their customers. In cloud analysis, there are six regions that correspond to six continents in the world. Data centers: It models the infrastructure services provided by various cloud service providers. It encapsulates a set of computing hosts or servers that are either heterogeneous or homogeneous in nature, based on their hardware configurations. Data centre characteristics: It models information regarding data centre resource configurations. Hosts: It models physical resources (compute or storage). The user base: It models a group of users considered as a single unit in the simulation, and its main responsibility is to generate traffic for the simulation. Cloudlet: It specifies the set of user requests. It contains the application ID, name of the user base that is the originator to which the responses have to be routed back, as well as the size of the request execution commands, and input and output files. It models the cloud-based application services. CloudSim categorises the complexity of an application in terms of its computational requirements. Each application service has a pre-assigned instruction length and data transfer overhead that it needs to carry out during its life cycle. Service broker: The service broker decides which data centre should be selected to provide the services to the requests from the user base. VMM allocation policy: It models provisioning policies on how to allocate VMs to hosts.

VM scheduler: It models the time or space shared, scheduling a policy to allocate processor cores to VMs.

We can use CloudSim with Ubuntu,Windows, NetBeans IDE and Eclipse is an integrated development environment (IDE) for Java and other programming languages like C, C++, PHP, and Ruby etc, steps for installing CloudSim in Windows easily and efficiently.Step1. First of all we need to download the CloudSim and latest version of the Java Development Toolkit (JDK). Step2. CloudSim requires a working JRE, so install the JDK.Step3. Now install the CloudSim Unpack the downloaded 'CloudSim-3.0.3.tar.gz' or 'CloudSim-3.0.3.zip' (let the name of the unpacked folder be 'cloudsim-3.0.3'). In our implementation four processors of the same specification is defined in CloudSim, each processor has 2X2 matrix of AES algorithm relationship and parallel processors to perform the steps of the algorithm, the result is high processing speed that is suitable for big data cloud.

Table 1.comparison of the speed of proposed algorithm with other algorithms in cloudsim

Algorithm	Speed (ms)	Resistivity against Attacks
AES DEVELOPMENT	98	YES
AES	98	NO
DES	150	NO
RSA	370	NO

Some attacks were imposed on proposed algorithm by use of picklock software. The results showed that proposed algorithm is resistant against attacks. Following Fig. 10 indicates this issue.

DOI 10.17148/IJARCCE.2016.5605

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

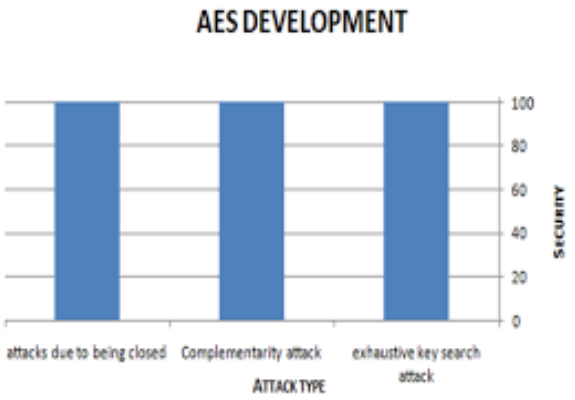

Fig. 10. Testing proposed algorithm against attacks

As it is clear in figure, proposed algorithm is resistant against attacks and it can be used for protecting the data in cloud.

Comparing proposed algorithm with previous algorithms: we compare the proposed algorithm with previous encryption algorithm in terms of efficiency, speed and different types of attacks. The results are presented in following table.

Table 2. comparing the efficiency of proposed algorithm with other algorithms

Algorithm	Efficiency	Speed	Attacks
AES Development	High	High	Resistant
AES	High	High	No Resistivity
DES	High	Low	No Resistivity
RSA	Average	Low	No Resistivity

It is observed that the proposed algorithm has very good results in all tested criteria. Proposed algorithm was individually compared with previous algorithms in terms of attacks the obtained results are shown in figure 11.

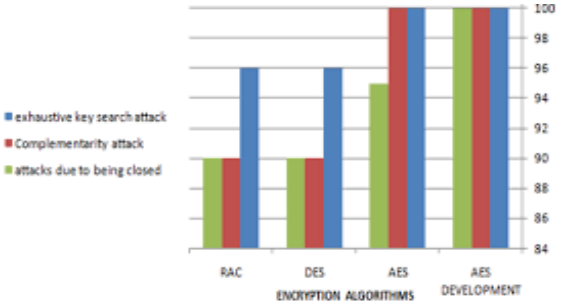

Fig. 11. Comparing proposed algorithm with the other algorithms

The obtained results proved that the proposed algorithm can be a good method for protecting the data.

V. CONCLUSION AND FUTURE WORK

Today, one of the important recommended methods for storing the data is application of cloud computing. But many people still have problem with that and prefer to store their data hard disks, rather than saving them in virtual environments. The main reason is their security concerns. In this regard, cloud computing has not yet convince the users completely. If they succeed in enforcement of their security condition, this method would be the best method for storing the data. One the advantages of cloud computing is the feasibility of access to IT resources. Due to high flexibility and versatile application of this capability, this field has been introduced as a platform for new generation of communication. But due to the security concerns, its application is with errors. Therefore, maybe security issue is the reason for its limited spread. Although data storing in virtual level has provided good capabilities and provided the space costs for users for data storing, but it has not yet succeeded in completely satisfying the users. Many companies and organizations either don't know this technology or even if they relatively know it, the first thing hits there is the vulnerability of the information against attacks. In this paper, cloud environment, the works done in relation with security condition in cloud, encryption algorithm types and different types of attacks are investigated. After investigation of these methods, a new approach was presented vi development of standard AES encryption algorithm and application of cellular automata along with phase operator, which is entitled as proposed algorithm. This algorithm, which is different from previously presented algorithm, could strengthen the key of AES algorithm by help of phase operators and cellular automata. The results show that proposed algorithm is resistant against different types of attacks. In addition, its speed remains that same. The proposed method reveals that it has optimized speed and resistivity, when compared with other algorithms. In future as cloud network is an extensive network of resources and security is also an important challenge, it is proposed to add a layer, called security, to cloud layers to protect the security of cloud services.

REFERENCES

[1] A.Salim, S.Tripathi, R.K.Tiwari " A Secure and Timestamp-based Communication Scheme for Cloud Environment" Int.J.Electronic Security and Digital Forensics, Vol 6, No. 4, pp. 319-332, 2014.

[2] I.Chana, and T.Kaur 'Delivering IT as a utility – a systematic review', International Journal in Foundations of Computer Science & Technology (IJFCST), May, Vol. 3, No. 3, IBM Research Lab, 2013.

[3] I.Foster, Z.Yong, I.Raicu, and S.Y.Lu 'Cloud computing and grid computing 360-degree compared', Grid Computing Environments Workshop, 12–16 November 2008, pp.1–10, 2008.

[4] M.K.Khan, S.K.Kim, and K.Alghathbar 'Cryptanalysis and security enhancement of a more efficient & secure dynamic ID-based remote user authentication scheme', Computer Communications, IJCSE, Vol. 34, No. 21, pp.305–309, 2010.

[5] William Stallings, Cryptography and Network Security principles and practice sixth edition, Pearson, ISBN 10: 0-13-335469-5.

[6] M.Eman, S.Abdelkader, E.Sherif, Data Security Model for Cloud Computing, The Twelfth International Conference on Networks, DOI: 10.13140/2.1.1540.1600, 2013.

[7] S.Narjeet, R. Gaurav, "Security on BCCP through AES Encryption Technique". International Journal of Engineering Science & Advanced Technology, 2012.

[8] S.A.Manavski , CUDA Compatible GPU As an Efficient Hardware Accelerator for AES ryptography, In Proceedings of IEEE

International Conference on Signal Processing and Communication (ICSPC), Dubai, United Arab Emirates, pp.65–68, 2007.

[9] Lynn Hathaway, "National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information", June 2003.

[10] R.Ayanzadeh, A.S.Z.Mousavi, E.Azamshahamatnia. "Fuzzy cellular Automata Based Random Numbers Generation", Academic Journals Inc, ISSN 1819-3579, DOI: 10.3923/tasr.2012.96.102, Year 2012.

[11] opensourceforu.com/.../cloudsim-framework-modelling-simulating.

BIOGRAPHY

Santosh Kumar Singh is a Research Scholar in the Department of Computer Applications, Vinoba Bhave University, Hazaribag, Jharkhand, India. He received M. Phil (Computer Science) degree in 2011 and Master of Philosophy Dissertation entitled "study on the network security & network topology". He Qualified Doctoral (Ph.D) Eligibility Test 2014 of Vinoba Bhave University, Hazaribag. His research interests are Cloud Computing, Parallel and Distributed Computing etc.