UDGAM VIGYATI, Volume 2, 2015, (November)
ISSN 2455-2488
Page No. 188-195

"TWO LEVEL SECURITY ALGORITHM OF DATA IN CLOUD COMPUTING"

Ms. Aarti Shrivastava
Dept .of Computer Science, Govt. Holkar Science College Indore

Mr. Pradeep Sharma
Dept .of Computer Science, Govt. Holkar Science College Indore

Mr. Shivlal Mewada
Dept .of Computer Science, Govt. Holkar Science College Indore

ABSTRACT

Cloud computing is a very popular concept in a computer world now a days. It providing excellent services by flexible infrastructure for development and software for ready to use .Security is the most important facet in cloud computing for ensuring client data is placed on secure mode or not in the cloud environment. Cloud computing is a flexible, cost-effective and proven delivery platform for providing business. Main goal of cloud computing is to provide easily scalable access to computing resources to improve organization performance. In this research paper we have proposed two level of security. To improve the performance of security we combine encryption algorithm namely as AES, RSA to enhance security of data in cloud.

Keyword— *Cloud Computing, Security Algorithm, AES, DES, Blowfish and RSA,MD5.*

INTRODUCTION

Cloud computing means network of computer connected through internet sharing resources given by cloud provider [A] Cloud computing is the concept of using remote service through network using various resources. In cloud computing user can pay on the basis of resources usage as timely basis .In general term we can define it is a technology that provide hosting service over internet it is continuously developed and there are several major cloud providers such as Amazon, Google, Microsoft, Yahoo etc[2].Cloud computing is generally divided in to three segments are: "Application", "Storage" and "connectivity" and each segment is used to service as a different service for a different purpose to use in different business[2][1].The concept of cloud computing is linked closely with those of service model :

- **IaaS (Infrastructure as-a-services):** It basically deals by providers to provide feature on demand utility.
- **PaaS (Platform as-a-services):** It is used by developer for creating new application.
- **SaaS (software as-a service):** It is provide application as a service on internet.

In cloud computing is categorized in four categories

- **Private cloud:** In private cloud data is managed properly within organization only without the limit of network bandwidth .It is some time called internal cloud eg.S3 (simple storage service), EC2 (Elastic Cloud Computing).
- **Public cloud :** This is only one of which cloud service are being available to user via a service provide over the internet it provide service on a pay –per-usage model eg. Google Apps Engine, Blue cloud by IBM.

- **Community cloud:** This type of cloud is basically managed by group of organization that have common objective eg. Security polices etc.
- **Hybrid Cloud:** Hybrid cloud is a combination of private and public cloud means a vendor has a private cloud and forms a partnership with a public cloud provider.

- In this paper we have combine two algorithm for the security purpose .firstly we have done analysis of data security algorithm for cloud computing after that we propose data security model based on studying of cloud computing architecture. Section II literature review. In III section states exiting algorithm. Section IV proposed model. Section V methodology. Section VI conclusion recommendation. Section VII . future work.

LITERATURE REVIEW

The literature review contains the definition of cloud computing by US National Institute of Slandered and Technology (NIST). The NIST definition is one of the clearest and most comprehensive definition of cloud computing and it widely referenced in US government documents and projects [1].

Shivlal mewada et.al [2] mention that securities based model for cloud computing .In this paper we study about security management, awareness, data security etc.

Garima saini,NAvin Sharma et.al [4] triple security of data mention that DSA DES, Stegenography algorithm to provide security of data.

Shivlal mewada ,Aarti shrivastava et.al [5] mention that Analysis of Data Security Algorithm in Cloud Computing in this paper we study performance analysis of encryption algorithm.

Suganya ,N.Boopal,Naveen [6] mention that Implementation Multiprime RSA algorithm to enhance the data security in cloud computing,

A number of researcher have discussed the security challenges that are raised by cloud computing .It is clear that the security issues has played the most important role in hindering the acceptance of cloud computing. For the security purpose of cloud storage various encryption technique are being analyzed by researcher .as discussed in survey there are many security algorithm which are currently used to cloud storage and secure data . Apart from this there are still too many areas which requirement future enhancement like more efficient algorithm can be developed which can increase the security level in the cloud storage[1].

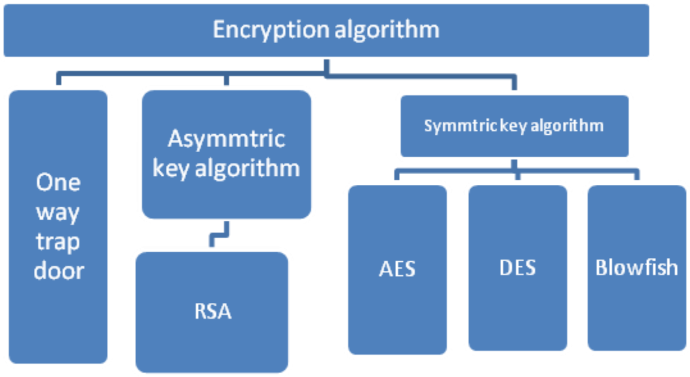
EXISTING ALGORITHM FOR CLOUD SECURITY

In cloud computing there are various encryption algorithm are used .Encryption algorithm convert the data in to scrambled form by using “the key” and only used have the key to decrypt data .Encryption algorithm is divided in three types :

One way trap door: It is one way to encrypt that is not intended to be decrypt.

Symmetric key algorithm :
In symmetric key algorithm only one key is used to encrypt and decrypt the message.

Asymmetric key algorithm: In asymmetric key algorithm two keys are used one key(public key)for encryption and other one key (private key) for decryption .



A. Symmetric key algorithm :

DES(data encryption standard): The common UNIX utility ,DES was released to the public in 1970.It is a strong symmetric key encryption algorithm developed by IBM. In 1998 it is replaced by AES.

AES (Advanced encryption standard): It is a strong symmetric key encryption algorithm developed by NIST .it uses 10,12,or 14 rounds each of ciphers has a 128-bit block size with the key size of 128,192 and 256 bits respectively[3,7].It ensure that the hash code is encrypted in highly secure manner its algorithm step are follows:

1. Expansion of key
2. Start your preliminary round (initial round)
3. Addition of round key (add round key)
4. Rounds
5. Sub bytes
6. Shift row
7. Mix column
8. Add round key
9. Final round
10. Sub bytes
11. Shift row
12. Add round key[3].

Blowfish : It is a strong symmetric key encryption algorithm developed by Bruce Schneider in 1993 . the key size of algorithm is different like Blowfish algorithm is 128-448 bits the key size of Blowfish is greater than AES[2].

B. Asymmetric key algorithm:

RSA (RonRivest,Adi Shamir and Lenard Adleman)

It is a strong asymmetric key encryption algorithm created by RonRivest,Adi Shamir and Lenard Adleman in 1978.It is used for public key cryptography. In this, two public/private keys are used for encryption/decryption [2].RSA is not normally a standalone encryption method .It is commonly used conjunction with DES or some other secret key.

Key generation :keyGen(p,q)

Input: two large prim no like .p,q.

Compute n=p.q

Φ(n) =(p-1)(q-1)

Choose e such that gcd(e, Φ(n))=1

Determine d such that e.d _=1 mod Φ(n)

Key

Public key =(e,n)

Secret key =(d,n)

Encryption :

$C= m^e$ mod n

Where c is the cipher text and m is the plain text

COMPARISON OF EXITING ALGORITHM

Characteristics	DES	Belowfish	RSA	AES
developed	1977	1993	1977	2000
Block size	64	64	64	256
Speed	slow	slow	slow	fast
developed	1977 by NIST	1977 by Ron rivest	1998	2000
Block size	64	64	64	256
Speed	slow	Slow	slow	Fast

The data will be encrypted using the algorithm such as AES, DES , BELOWFISH ,RSA and MD5 in cloud computing analysis perform of these algorithm in erm of Speed-Up ratio and Mean Processing Time for the different input are calculated.

- Speed-Up ratio is defined as the difference between mean processing time of a single system and cloud network .It provide information us how fast the data have been encrypted. IT will give us the idea about speed of encryption.

- Mean processing time is the difference between the starting time taken to encrypt the data and ending time. when size of input is increase the time taken to encrypt the data will increase and with the increase in time speedup ratio decreases.
  From the above result, if your requirements in performance algorithm now prefer MD5 Blowfish, AES and then DES.

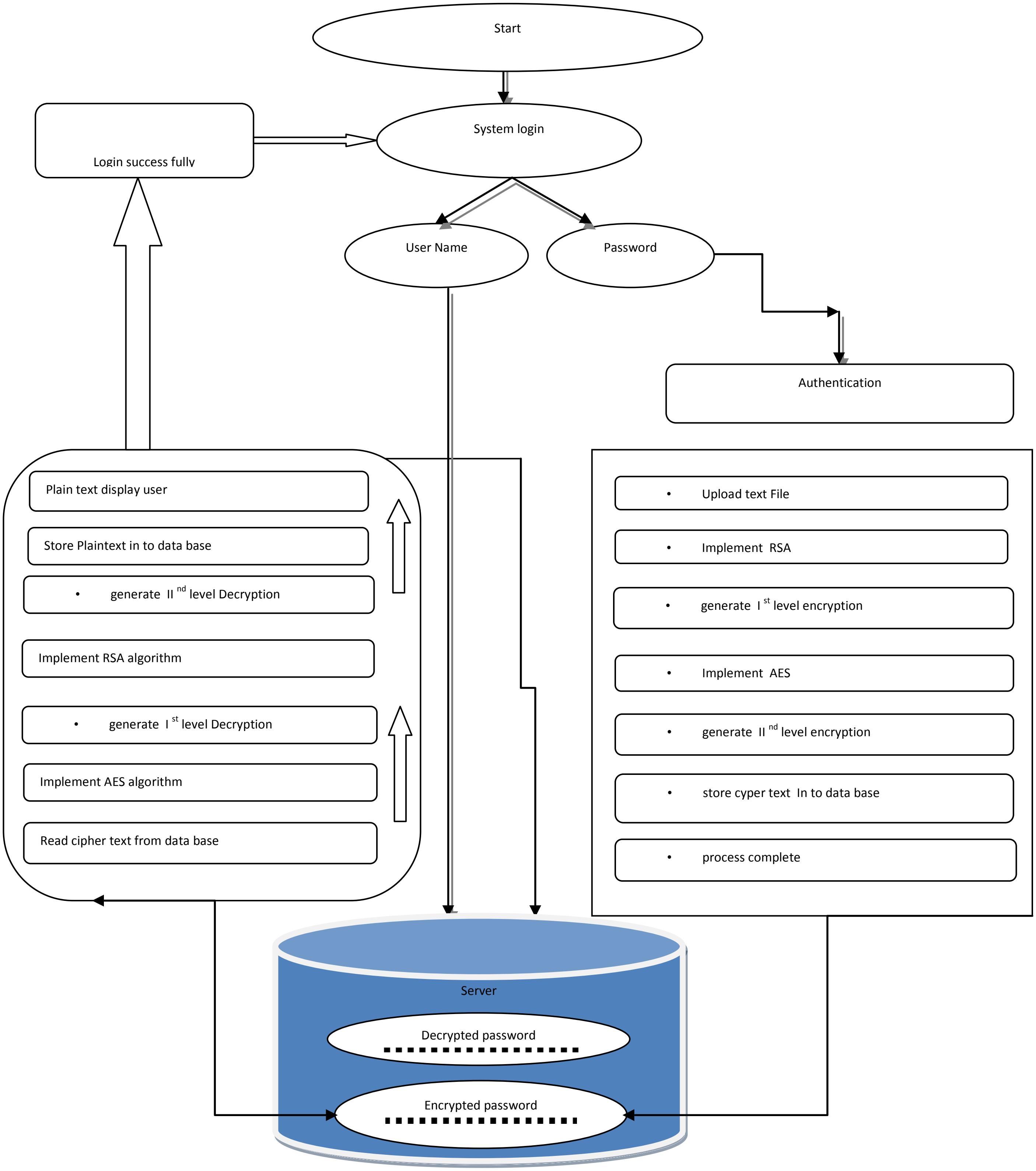
If you think the security purpose of data now prefer the MD5,AES.

PROPOSED MODEL

Now a day's cyber crime is viral. That means cyber criminals can easily access data storage. In Personal Cloud important data, files and records and entrusted to third party, which enables data security to become the main security issues in cloud computing .

In cloud storage any organization or individual's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud .To provide secure communication over distributed and connected resources authentication of stored data becomes a compulsory task. To maintain security of text file only .this proposed two level security model used RSA and AES algorithm to generate encryption when user upload the text file in cloud storage for increasing security .

It is called two level security model because it encrypt data two times first used RSA algorithm and second it used AES algorithm similarly it decryption in two level first used AES algorithm and second level used RSA algorithm


Start
System login
Login success fully
User Name
Password
Authentication
Plain text display user
Store Plaintext in to data base
• generate II nd level Decryption
Implement RSA algorithm
• generate I st level Decryption
Implement AES algorithm
Read cipher text from data base
• Upload text File
• Implement RSA
• generate I st level encryption
• Implement AES
• generate II nd level encryption
• store cyper text In to data base
• process complete
Server
Decrypted password
Encrypted password

METHODOLOGY

In complete purpose, our work will provide the following contribution

In client Phase: the client sends the query to the server. depend on query the server respond to the client with the corresponding file .before this process, the client authorization step in involved. In server side [6][10],it checks client name and its password for security process .If it is satisfied, the queries are received from the client and the corresponding files are searched in the data base. Finally, the corresponding file is retrieved which will be send to the client [6][3].

In second phase, virtual setup is configured. Since virtual machine is dynamic, they can rapidly be reverted to previous instance, paused and restarted, relatively without difficulty. Virtualization technology allows the user to run multiple operating systems simultaneously on a single physical machine sharing the underlying resources. The user's subscribed application is stored in the data center which is a collection of servers.

In third phase, encryption policy will be implemented .Encryption is done on the end point before being sent across the network or is already stored in the suitable encrypted format .Stored object is used as the back end for the application data gets encrypted by using an encryption engine, which is embedded in the application or client. In our method we used two algorithm one is symmetric and other is asymmetric algorithm.

It is an efficient and independent examination of data, record of an enterprise for state purpose .IT maintained and reviewed properly to overcome security issues. Whenever the client login and updates or request for the any activity it is recorded and reviewed properly

CONCLUSION

In this research paper we have analyzed encryption algorithm and after that I decided that we combine both algorithm. To enhance the security algorithm the algorithm are applied both cloud network and single system.

.

FUTURE WORK

In future we will extend our research by providing algorithm implementation and during implementation we also give an option to user to select encryption algorithm according his/her requirement either encrypt or decrypt data on cloud and provide new concept to enhance security in cloud computing.

.

REFERENCES

1. Pradeep Sharma, Aarti Shrivastava and *Shivlal Mewada*, "Analysis of Data Security Algorithm in Cloud Computing (CC)", National Conference on Emerging Trends in m Technologies (NCETCT-2014)", School of Engineering and Technology, Vikram University, Ujjain, Page no (36-41), August 26-27th 2014.(full length paper)
2. Shivlal Mewada and Umeshkumar Singh and Pradeep Sharma, "Security Based for Cloud Computing","International Journal of Computer Network and Wireless Communication" ,Volume -1,Issue -1,Page No (13-17),1december 2011.

3. BhushanLalsahu and RajeshTiwari ,"A Comprehensive study on cloud computing" , International Journal of Advanced Research in Computer Science and Software Engineering ",Vol ume-2,Issue -9, Page No.(33-36),September 2012,ISSN 2277.
4. Garimashaini ,Navinsharma,"Triple security of data in cloud computing ",International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5825-5827
5. *Shivlal Mewada*, AartiShrivastava, Pradeep Sharma, N Purohit and S.S. Gautam" Performance Analysis of Encryption Algorithm in Cloud Computing", International Journal of Computer Sciences and Engineering, Volume-03, Issue-03, Page No (83-89), Jun -2014, E-ISSN: 2347-269.
6. *Suganya.N,N.Boopal,Naveen.M," "implementation Multiprime RSA algorithm to enhance the data security in cloud computing",International journal of innovative Research in Science Engineering and technology,vol 4,Issue 1,Page no 18953-18957,January 2015.*
7. *Randeepkaur,surpriyakinger," analysis in security algorithm in cloud computing", International journal of application or innovation in engineering and management ,vol3,issue 3,march 2014.*
8. Er. RimmyChuchra ,"data security in cloud computing ",International Journal of Societal Application of computer science, Volume -01, Issue -1,Page N0 (1-5),1 Nov 2012.
9. Farzadsabhi,"Cloud Computing Threat and Responses" ,IEEE, Page No(245-249) ,27-29 may-2011.
10. MandieepKaur and Manish Mahajan ," International Journal of Communication and Computer Technologies ", Volume -1,Issue-3, Page No.(56-59), January 2013.
11. GurpreetKaur and Manish Mahajan, "Evolution and Comparison of Symmetric Key algorithms", International Journal of Science ,Engineering and Technology Research, Volume-2,Issue -10, Page No(1960-1962),October 2013,ISSN 2278-7798.
12. Vijeyta Devi and VadlamaniNagalakshmi, "A Prospective Approach on Security with RSA algorithm and cloud sql in cloud computing", International Journal of Computer Science and Engineering ,Volume n-2,Issue -2 ,Page No(35-44),May 2013.
13. Ms. Disha H. Parekh and Dr. R. Sridaran," An Analysis of Security Challenges in Cloud Computing", Volume – 4,Issue-1, page No.(30-44),2013.
14. Navneet Sharma and Vijay Singh Rathore, " Different Data Encryption Methods Used in Secure Auto Teller Machine Transactions",Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-4, Page No.(176-177) April 2012.