ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

Cloud Computing Security Provision Using Twofish Algorithm

[I]R.Mathivanan, [II]A.Christy Jeba Malar
[I]Student IV IT, Sri Krishna College of Technology
[II]Assistant Professor, Dept. of Information Technology, Sri Krishna College of Technology

Abstract
Through out the IT world Cloud Computing Security plays a vital role because of the high available storage and user demands. Data stored in cloud is vulnerable. Users thing about security threads of their data privacy and confidential over the cloud .Data storage is always concerned about security. Twofish algorithm is 128bit block encryption with extensively crypt analyzed. It is one of the efficient algorithm because of the performance on both Hardware and Software platforms with strong keys. Twofish users block ciphering with single key of any length up to 256bits.It allows to implement to trade of encryption and speed key and setup time and code size to balance performance from the key dependent S-boxes it can withstand unknown attacks come next and resist known attacks. The performance of the encryption algorithm is also balanced.

Keywords
Twofish, Confidentiality, Cloud Computing, Security, Performance

I. Introduction

The cloud computing becomes the host issue in industry and academic with the huge development of computer hardware and software. The result of many factor like Business mode and communication mode. It provides high reliability & scalability.

The Cloud provide many services like
* Storage as a Service (StaaS)
*Software as a Service (SaaS)
*Platform as a Service (PaaS)
*Container as a Service (CaaS)
*Infrastructure as a Service (IaaS)
*Network as a Service (NaaS)

Now a days clouds are "Pay as a Service"
The resource of the cloud system provide transparent for the application and the user don't know where the resource come from. The user can access the data from anywhere through the application.

(i) Storage as a Service

This module of cloud computing deals with the storage of enormous amount of data that is being generated every day. Each day, a huge pile of data is being uploaded to the servers. SAAS incorporates with the technologies of how the data is efficiently stored in those servers, ensuring stability, reliability, robustness, backup and security. The data is also geographically replicated from servers from one geographical location to a different geographical location for Disaster Management Practice.

(ii) Platform as a service

This module of cloud computing incorporates with the idea which allows the developers to only focus on development of their projects and apps, rather than focusing on how to setup the coding and working environment about the language they are willing to work upon. Most of the programmers find it tedious to create and maintaining their own cloud environment as from being a developer mindset, it is a waste of time for them. They rather want to invest their time in coding and development, which is more productive for them and the organizations.

(iii) Infrastructure as a service

This service is the mother of all services in cloud computing. This service allows institutions or individuals to create their own virtual environment with no maintenance cost[1]. This service incorporates with virtual servers, which can be up, and running in no time by anyone willing to.
This service provides storage resources like hard disks or ephemeral disks, computing resources like RAM, CPU processing power in a place, which may or may not be physically accessible by the user but is accessible for working through various protocols for working. This service ensures the portability of our computer, as it is not running at our local area. It is running in cloud and every instance in cloud has a public IP address and hence it can be accessed from any corner of the world. Virtual servers come with a lot of variety based on the ram size and data transfer rate. Some of the providers are Amazon Web Services, Rackspace, IBM Soft watch, Google Compute Engine, Microsoft Azure, Openstack etc. n easy way to comply with the Recent Science journal paper formatting requirements is to use this document as a template and simply type your text into it.

II. Challenges

The following are some of the notable challenges associated with cloud computing, and although some of these may cause a slowdown when delivering more services in the cloud, most also can provide opportunities, if resolved with due care and attention in the planning stages.[3]

(i) Security and Privacy

Perhaps two of the more "hot button" issues surrounding cloud computing relate to storing and securing data, and monitoring the use of the cloud by the service providers. These issues are generally attributed to slowing the deployment of cloud services. These challenges can be addressed, for example, by storing the information internal to the organization, but allowing it to be used in the cloud. For this to occur, though, the security mechanisms between organization and the cloud need to be robust and a Hybrid cloud could support such a deployment.

(ii) Lack of Standards

Clouds have documented interfaces; however, no standards are associated with these, and thus it is unlikely that most clouds will be interoperable. The Open Grid Forum is developing an Open Cloud Computing Interface to resolve this issue and the Open Cloud Consortium is working on cloud computing standards and

practices.
The findings of these groups will need to mature, but it is not known whether they will address the needs of the people deploying the services and the specific interfaces these services need. However, keeping up to date on the latest standards as they evolve will allow them to be leveraged, if applicable.

(iii) Continuously Evolving

User requirements are continuously evolving, as are the requirements for interfaces, networking, and storage. This means that a "cloud," especially a public one, does not remain static and is also continuously evolving.

III. Twofish

Twofish is a block cipher by Counterpane Labs, published in 1998. It was one of the five Advanced Encryption Standard (AES) finalists, and was not selected as AES. Twofish has a 128-bit block size, a key size ranging from 128 to 256 bits, and is optimized for 32-bit CPUs. Currently there is no successful cryptanalysis of Twofish.
S-boxes: An S-box is a table-driven non-linear substitution operation used in most block ciphers.it can be created randomly or algorithmly because of the various input and output size this algorithm uses four different 8 by 8 bit key dependant s-boxes
Large s-boxes: large s-boxes are generally assumed to be secured than the small s-boxes it is vary as GOST 4 by 4 bit s-boxes and TIGER 8 by 8 s-boxes

Twofish builds four bijective key-dependent 8x8-bit S-boxes using a key/permutation "sandwich" (shown for a 128-bit key):
s0(x) = q1[q0[q0[x] ^ k0] ^ k1]
s1(x) = q0[q0[q1[x] ^ k2] ^ k3]
s2(x) = q1[q1[q0[x] ^ k4] ^ k5]
s3(x) = q0[q1[q1[x] ^ k6] ^ k7]
where q0,q1 are two fixed 8-bit permutations.
Key schedule: design the key schedule for the ciphers reuse the all same primitives and making it hard to attack both s-boxes and sub key generation process. Two fish is fast and can perform 17.8 clock cycles per byte. It has minimal table requirements and make it efficient on 8 bit CPU's suitable for hardware tradeoffs and smartcards

TWO FISH: was developed and designed to meet NIST's design criteria for Advance Encryption Standard (AES) which includes key lengths of 128 bits, 192 bits, and 256 bits. It is a 128-bit symmetric block cipher. It is Efficient on both Intel Pentium Pro and other software and hardware platforms. There are no weak keys and it has Flexible design.

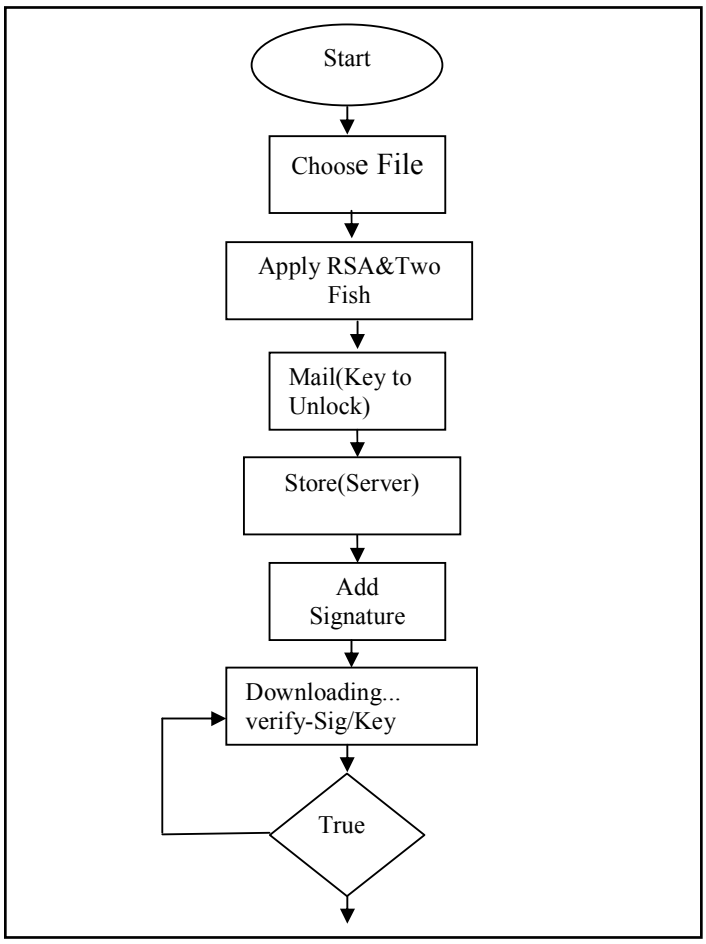

Fig. 1: Propsed algorithm

Blowfish is symmetric key block cipher. Blowfish has 64-bit block size and variable key length from 32bits to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. Blowfish is known to be susceptible to attacks on reflectively weak keys. Blowfish is in public domain that is it is license free and opens for everyone. Blowfish splits 64 bit input into two halves each of 32 bit and then according to Feistel structure cipher text will get produced from plain text.
Modified version of Blowfish2. block size of 128 bits 3. 128,192,256 bit keys 4. No weak Keys 5.Extensively Cryptanalyed 6.Safety Facto 2.67r.
For experiment purpose, we have used one pc with IntelI CoreI i3-4005U CPU@ 1.70 GHZ CPU with 4GB RAM. We implemented the algorithms according to their standard specifications in Java Runtime environment using Java, on Windows 7 Operating System. In the experiment we encrypt the pdf, text, Doc files of different size ranges between 15KB to 400KB and calculate their mean encryption time. Table.2 Time Comparison between Twofish & Blowfish According to the results found, as the data size increases the time to encrypt the data also increases. If the time to encrypt the data by Twofish and Blowfish get compared then we can find that Twofish encrypts data in lesser time. Based on these results we can say that the most efficient attack against Twofish is the brute force attack as for 128-bit key it needs 2^{128} complexity, for 192-bit key it requires 2^{192} complexity and for 256-bit key the complexity is 2^{256}

Table 1 : Size after Encryption

Algorithm	Plaintext	After Encryption	After Decryption
DES	240KB	328KB	240KB
TDES	240KB	614KB	240KB
AES	240KB	847KB	240KB
Blowfish	240KB	955KB	240KB
Twofish	240KB	955KB	240KB

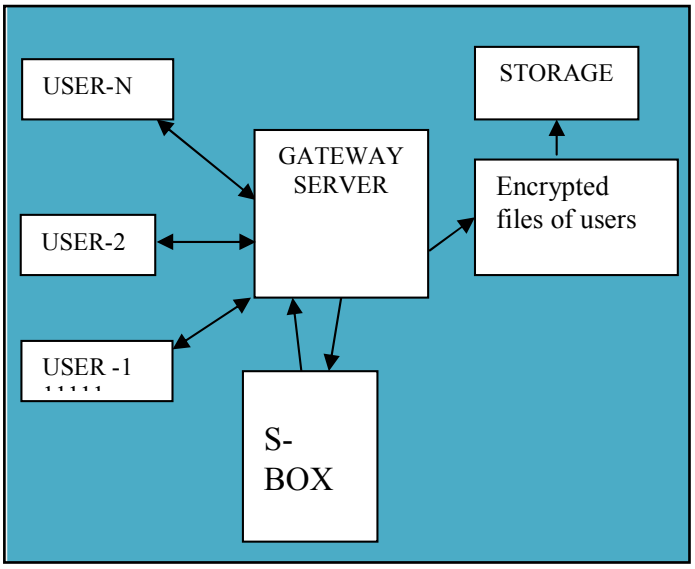

Fig. 2: System Architecture

User: A user can upload/ download file. When uploading file RSA & Twofish Encoding schemes are used to encrypt data and generate key & signature is included to lock that data and when downloading file inverse RSA & Twofish are used to decrypt data & signature is used to unlock the file.
Mail Server: When user upload data, then RSA generate a public key & a private key. This private key automatically picked by session but public key again encrypted by using Twofish algorithm and is sending to user by mail service. This key is used when user download their content or data.

IV. Conclusions

Cloud computing is changing the way IT departments buy IT. Businesses have a range of paths to the cloud, including infrastructure, platforms and applications that are available from cloud providers as online services. Many people may be confused by the range of offerings and the terminology used to describe them and will be unsure of the risk and benefits. Security is a major requirement in cloud computing while we talk about data storage. There are number of existing techniques used to implement security in cloud. It is expected that the data loss will be reduced and increased security using RSA & Twofish algorithm's private key along with signature.

References

[1]. *RuWei Huang, Si Yu, Wei Zhuang and XiaoLin Gui, "Design of Privacy-Preserving Cloud Storage Framework" 2010 Ninth International Conference on Grid and Cloud Computing.*
[2]. *Dr. Chander Kant and Yogesh Sharma, "Enhanced Security Architecture for Cloud Data Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, pp.571-575.*
[3]. *Cong Wang, Qian Wang, KuiRen and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", In Quality of Service, 2009. 17th International Workshop on, page 19, 2009.*
[4]. *Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing." IEEE 2009.*
[5]. *Kowsigan M, Balasubramanie P. "An Improved Job Scheduling in Cloud Environment using Auto-Associative-Memory Network", Asian Journal of Research in Social Sciences and Humanities Vol. 6, No. 12, December 2016, pp. 390-410. ISSN 2249-7315*
[6]. *Kowsigan M, Balasubramanie P. "Scheduling Of Jobs In Cloud Environment Using Soft Computing Techniques", International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.38 (2015)*
[7]. *Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, "Cloud security issues" In Services Computing, 2009. IEEE International Conference on, page 517520, 2009.*
[8]. *Kashish Goyal, Supriya Kinger" Modified Caesar Cipher for Better Security Enhancement" International Journal of Computer Applications (0975 – 8887) Volume 73– No.3, July 2013.*
[9]. *Yogesh Kumar, Rajiv Munjal and Harsh Sharma, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.*
[10]. *Mr. Gurjeevan Singh, , Mr. Ashwani Singla and Mr. K S Sandha " Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.*
[11]. *D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.*
[12]. *Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.*
[13]. *Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).*
[14]. *Z. Hu, C. Peter, S. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02, 1986.*
[15]. *R. Sonzgiri, M. Dehill, V. P. Levine, C. Shields, E. M. Belding-Royer," A Secure Routing Protocol for Ad-Hoc Networks, in Proceedings of ICNP'02, 1978.*
[16]. *Y. Hu, A. Perrig, D. Johnson,"Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad-Hoc Networks", in Proceedings of IEEE INFOCOM'03, 1965.*

Author's Profile

R.Mathivanan studying IV IT in Sri Krishna College of Technology, got placed in Accenture Technologies. His research interest is in cloud computing.

A.Christy Jeba Malar currently working as assistant professor in the Department of Information Technology at Sri Krishna College of Technology.She is currently working toward the Ph.D. degree on Pervasive Computing. Her research interests mainly focused on wireless indoor localization systems, virtualization ,security in cloud computing.