Cloud Based Security

Nikita M. Ikhar
Dept of CSE, DMIETR,
Sawangi(Meghe),India
nikita123ikhar@gmail.com

Shivani S. Meghal
Dept of CSE, DMIETR,
Sawangi (Meghe), India
shivani3meghal@gmail.com

Prof. Kaustubh Satpute
Dept of CSE, DMIETR,
Sawangi (Meghe), India
kaustubh2008satpute@yahoo.com

Abstract- As we all know that internet is progressing in the terms of social networking website and the site which highly interact with the user also the use spent more time on this kind of website. Also user share their personal information, some important data, photos among various people that may belong their group or community so the security for all this things is mandatory but most of the time the site doesn't give proper attention toward this security requirement by which the user information may leak by unauthorized person.so in this paper we are trying to secure the information of users using different compression and encryption algorithm and the address of information from users. This data is stored at various places on internet which is scattered on worldwide. So when any authorized person is trying to access his data that person only get all the information about his data but still he will never know the location of that data. The system we developed in this paper allows the user to upload all his data in any format including the security feature like compression and encryption. This all uploaded data and information can be access from anywhere in the world. So finally we can say that we developed the very secure system to store the important information on website in a very effective & secured manner.

Keywords-*Cloud, Authentication, Cryptography*

*****

I. INTRODUCTION

In 2007, IBM announced a grand plan for cloud computing. Over the last couple of years, cloud computer has become a hot topic in research and in the field of applications. IBM's White Paper named "Cloud Computing" defined what cloud computing is.

The phrase "Cloud computing" describes it as a system platform or a kind of software application. System platform based on real time, it can dynamically proviso, set, reset. In a cloud computing platform, cloud server is a physical server. High end cloud computing includes other computation resources. Some of these examples are SANs, network, firewall and other security setup. Second, cloud application means its software application utilizes the Internet. Any user can use a standard browser and the Internet to access a cloud software application. Despite there is a lack of clarity in the definition of what cloud storage is, based on the White Paper mentioned above, the authors have deduced two basic characteristics of cloud storage. First, it is about the cloud infrastructure which builds on cheap server clusters. Second, through server clusters, distributed storage and data redundancy can be achieved by making multiple copies of documents which meet these objectives: high usability and high scalability. For high scalability, it means cloud storage can scale to large cluster with hundreds of nodes for processing. For high usability, it means cloud storage can tolerate node failures and do not affect the entire operation.

Cloud Computing is a technology that uses the internet and central remote servers to maintain application & data. Cloud computing allows businesses and consumers to use applications without installation and access their personal files at any computer with by internet. This cloud technology allows for more efficient computing by centralizing memory, processing and bandwidth, storage. Cloud computing is an Internet-based super-computing model, it is a new method of shared infrastructure, it can provide a variety of IT services to large pool of computer resources. In the future, the computing and data resources will gradually migrate to the Web and the computing platform can achieve supercomputing and large-capacity storage in are laxed way, while its computational overhead is much cheaper than the current computing and storage infrastructure.With cloud computing, the users don't need to deploy a strong client computing, they can access to computing power directly from the cloud and pay according to usage.

This paper describes privacy protection and data security issues in cloud. This content of paper is organized as follows: Section II gives a brief description of what are cloud computing security-related issues. Section III discusses data security and privacy protection issues associated with cloud computing across all stages of data life cycle. Section IV shows current solutions for data

security and privacy protection issues in cloud. Section V summarizes the contents of this paper.

II. CHARACTERISTICS OF CLOUD COMPUTING

Ultra large-scale**:** The scale of cloud is very large. The cloud of Google has owned much more than one million servers. Also in Amazon, Yahoo, Microsoft, IBM have more than hundreds of thousands servers. There are thousands of servers in most of the enterprise.

Virtualization**:** Cloud computing makes user to get service from anywhere, through any kind of computer using internet. Anyone can complete all you want through net service using a notebook PC or a by mobile phone. Users can attain it safely through an easy manner. Users can complete a task that can't be completed in a single computer.

High reliability**:** Cloud uses data multi transcript fault tolerant, the computational node isomorphism changeable and so on to ensure the high reliability of the service. Using cloud computing is more reliable and efficient than local computer.

Versatility:Cloud computing produce many types of applications supported by cloud, and one cloud can support different applications running it at the same time.

High extendibility:There is no limit for the cloud so the scale of cloud can extend dynamically to meet the increasingly requirement.

On demand service:Cloud is a large data resource pool that you can buy according to your need; cloud is just like running water, electric, and gas that can be charged by the amount that you used.

Extremely inexpensive: The centered management of cloud make the enterprise needn't undertake the management cost of data center. The versatility increase the utilization rate of the available resources compared with conventional system, so users can fully enjoy the low cost service advantage. Below is the list of various application and advantage of cloud computing:

1. Cloud computing do not need high quality & prize equipment for user, and it is easy & efficient to use.
2. Cloud computing provides dependable and secure data storage center. There is no need of worry of problems such as data loss or virus
3. Cloud computing can realize data sharing between different equipment.
4. Cloud provides nearly infinite possibility for users to use internet.

III. CLOUD COMPUTNG SECURITY ISSUES

In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT field. Now, due to recession companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, at negligible cost. But when more and more information on individuals and companies is placed in the cloud, then more concerns are beginning to grow about just how safe an environment it is.

A. Security

Where is your data more secure, on your local hard driver or on high security servers in the cloud? Some told that customer data is more secure when managed internally by company, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security. In the cloud, data of user will be distributed over these individual computers regardless of where your base data is ultimately stored. Industrious hackers or unauthorized can invade any server, and study shows that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent loss is due to hackers.

B. Privacy

Different from the conventional computing model, cloud computing utilizes the logically computing technology, users' personal information may be scattered at various virtual data center rather than stay in the same physical location, even across the any nation borders, at this time, data privacy protection will face the problem of different legal computer systems. On the other hand, customer may leak hidden information when they accessing cloud computing services. Hackers can analyze the critical task depend on the computing task submitted by the users.

C. Reliability

Servers in the cloud have the same problems as your own home servers. The cloud servers may also experience downtimes and slowdowns, what the difference is that users has a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a large difference in the CSP's service model, once you select any specific CSP, you may be locked-in, by which potential business risk minimize.

D. Legal Issues

Regardless of efforts to bring into line the lawful situation, as of 2010, cloud supplier such as Amazon Web Services provide to major markets by developing restricted road & rail network and letting users to select "availability zones". On the other hand, worries stick with security measures and confidentiality from individual all the way through legislative levels.

E. Open Standard

Open standards are critical to the growth of cloud computing environment. Most cloud providers provide APIs which are typically well-documented but also unique to their implementation and thus not interoperable. Some vendors companies have adopted others' APIs and there are a number of open standards under development condition, containing the OGF's Open Cloud Computing Interface. The Open Cloud Consortium is working to develop consensus on early cloud computing standards and practices.

F. Compliance

Numerous regulations pertain to the storage and use of data require audit trails and regular reporting, cloud providers enable their customers to comply appropriately with these regulations. Managing Security and Compliance for Cloud Computing, gives insight on how a top-down view of all IT resources within a cloud-based location can deliver a stronger enforcement of compliance policies and management. In addition to the requirements to which customers are subject to the cloud data centers maintained by cloud providers may also be subject to compliance requirements.

IV. SUGGESTED WORK

Typically, the applications used for file transfers and storage is web based and hence requires web browsers to upload the various files on the servers from node. But the problem arises the time required and also the limits of a browser to run properly till the file is transferred. This cloud application will allow the uploading of files without disturbing other processes and at the same time user may be able to work in web browsers without hanging up the uploads. The file size varies according the premium. The application uses compression as well as encryption algorithms for file security and therefore takes more time to upload a cloud file. The key for encryption can be taken by user or a default key for users can be taken according to the design of application.

An advantage of cloud as solution is that it saves time**.** Businesses that utilize software programs for their management needs are drawback, because of the much time needed to get new programs to operate at functional levels. By turning to cloud computing, we avoid these hassles. we simply need access to a computer with Internet connection to view the information you need.

Another is less glitchas applications serviced through cloud computing require some versions. Up gradation are needed. less frequently and are typically managed by data centers. Sometime businesses experience problems with software because they are not designed to be used with similar applications. Some departments cannot share data because they use different applications.

Security mechanisms

Encryption of data plays a important role in the real time environment to keep the data out of reach of unauthorized people, such that it is not altered and tampered and sending the in splitted format is most secured way to transfer the data through the network.

AES encryption

AES is based on a design principle known as a Substitution permutation network. It is fast in both hardware and software. Unlike its predecessor, AES, DES does not use a Feistel network. AES has a constant block size of 128 bits and a key size of 128, 192, or 256 bits, while Rijndael can be specified with block size and key sizes in any multiple of 32 bits, with a minimum number like 128 bits.

The block size has a maximum of 256 bits, but the key size in bits has no theoretical limit. AES operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are performed in a special finite field. After the implementation of the application, it needs to be hosted so that it is available to the customer. So various hosting services including cloud are available.

The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into cipher text. Each round consists of various processing steps, including which depends on the encryption key. A set of reverse rounds are applied to change cipher text back into the original plaintext using the same encryption key.

AES decrypto

This fancily-named block performs the most importantoperation in the whole project; it accepts 128-bit datafrom Nios, decrypts it and then sends it back to Nios. 128-bit decryption needs a 128-bit key and 128-bit cipher textto decrypt, and results in 128 bits of decrypted data.It must be noted here that the source data is encryptedbeforehand (even before it is placed on the SD card)through a custom-coded C program that can encrypt anddecrypt arbitrary size files. This program's code is listed inAppendix A.

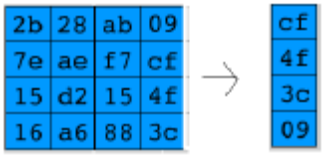
Algorithm

The AES decryption [1] basically traverses the encryptionalgorithm in the opposite direction. The basic modulesconstituting AES Decryption are explained in excruciating
detail below:

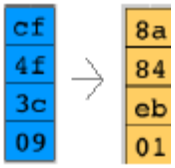
From the block level diagram, it can be seen that AESdecrypto initially performs key-expansion on the 128-bitkey block that creates all intermediate keys (which aregenerated from the original key during encryption forevery round).

The RTL for key expansion module is below. The generateroundkey module performs the algorithm that generates asingle round key. Its input is multiplexed between the userinputted key and the last round's key. The output is storedin a register to be used as input during the next iterationof the algorithm. The expansion keys module is a RAMwhich stores the original key and the 10 rounds ofgenerated keys for use during the decryption algorithm.

a) Key Expansion - The algorithm for generating the 10rounds of the round key is as follows: The 4th columnof the i-1 key is rotated such that each element ismoved up one row.



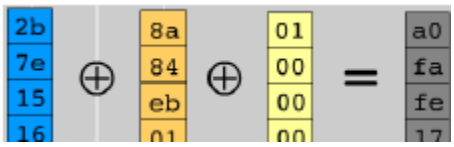
It then puts this result through a forwards Sub Boxalgorithm which replaces each 8 bits of the matrixwith a corresponding 8-bit value from S-Box. (Seefigure for Inverse Sub Byte below)



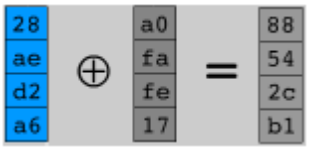
To generate the first column of the ithkey, this resultis XOR-ed with the first column of the i-1th key as wellas a constant (Row constant or Rcon) which isdependent on i.

Rcon=

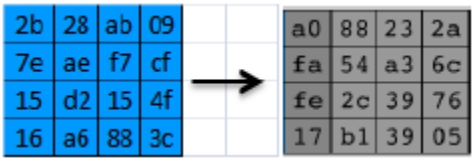
01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00



The second column is generated by XOR-ing the 1stcolumn of the ithkey with the second column of the i-1th key.

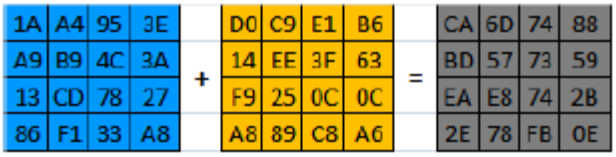


This continues iteratively for the other two columnsin order to generate the entire ithkey.



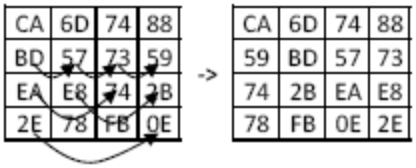
Additionally this entire process continues iterativelyfor generating all 10 keys. As a final note, all of thesekeys are stored statically once they have beencomputed initially as the ithkey generated is requiredfor the (10-i)thround of decryption.

b) Inverse Add Round Key – Performs XOR operationbetween the cipher text and intermediate expandedkey corresponding to that particular iteration. E.g., ifthe diagrams on the left represent the cipher and thekey values, the final value after it has generated bythis step is shown on the right.

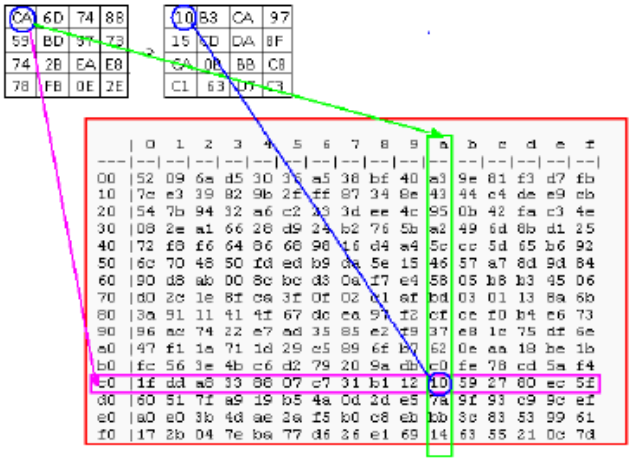


c) Inverse Shift Row – This step rotates each ithrow by I elements right wise, as shown in the figure.

ISSN: 2321-8169
513 – 518



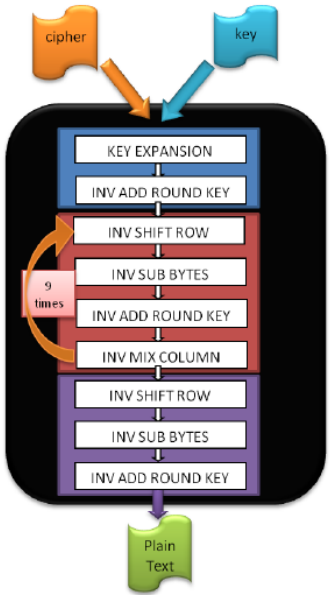
d) Inverse Sub Bytes – This step replaces each entry inthe matrix from the corresponding entry in theinverse S-Box[2] as shown in figure.



e) Inverse Mix Column - The Inverse MixColumns[3]operation performed by the Rijndael cipher, alongwith the shift-rows step, is the primary source of allthe 10 rounds of diffusion in Rijndael. Each column istreated as a polynomial over Galois Field (2^8) and isthen multiplied modulo $x^4 + 1$ with a fixed inversepolynomial is $c^{-1}(x) = 11x^3 + 13x^2 + 9x + 14$. TheMultiplication is done as shown below.

$$\begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{bmatrix} = \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

As shown in the block level diagram below, the AESdecrypto initially performs key-expansion on the 128-bit key block. Then the round key signals the start ofthe actual decryption process once the data processis ready. It starts by executing an inverse add roundkey between cipher text with the modified key(generated in the last iteration of the encryptionprocess) from key expansion. After this step, the AESdecrypto repeats the inverse shift row, inverse sub,inverse add round key, and inverse mix column steps nine times. At the last iteration, it does an inverseshift row, inverse sub bytes and inverse add roundkey to generate the original data.



AES 128-bit Decryption Algorithm
Optimized Hardware Design

Considering that the SD-card is the main source of latencyin reading the block, the design was optimized at fourlevels.

a) Elimination of inverse shift row by swapping therespective lines before sending it to inverse sub bytes.

b) Optimization of inverse mix columns to removemultiplication operations by turning them into shiftoperation / comparison operations

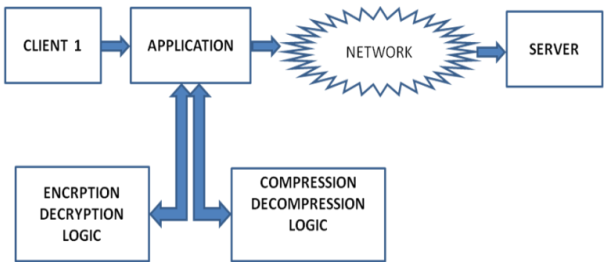
c) Elimination of duplicate modules to save FPGAresources.

d) Sharing of 32-bit input line both for accepting key andcipher text.Since Nios has a 32-bit MM Master Port (and therefore cantransmit up to 32 bits of data at a time), we buffered the32-bit data into the 128-bit bus one by one, before weactually proceed with decryption. The 32-bit data line isused as a common bus to accept both the key and thecipher text. Initially, the key used for encryption is beingsent to the key expansion module to generate and store allintermediate key-values required for correspondingiteration into the key-table. Then, the same 32-bit bus asused to send the input cipher text, and uses the at 88.31 MHz.intermediate keys stored in key table to perform itsdecryption. The eoc (end of computation) signal both fromkey expansion and AES Decrypto is multiplexed into thefinal eoc indicating which corresponding unit (keyexpansion or AES Decrypto) is done with its computation. [16]

Design

In this diagram we can see that there is a one client and one server and between this application is present. By using this application we are able to send the data on the server. When we want to send the data, at that time firstly data is reach to the application and this data is encrypted and compress. After compress and encryption, data are send to the server through the network at the time of uploading. By using this two techniques that is encryption and compression, data is secure by unauthorized users. Same technique is use for

decryption and decompression at the time of downloading.



System Architecture

Functionality

The application must be able to upload and download file from server without the client knowing the location of files. The application must provide the options to upload multiple files one at a time. The application must provide data after checking proper authentication of the user. The application must also ask for key while encrypting the file of the user and the same while downloading it from the server.

V. CONCLUSION

In this paper we have proposed a new security approach of file uploading mechanism which is easy & very effective for every user in a secured manner by which no one get the information about location of file. Also it increases the speed so this will work better in low network area where internet band width is low as compare to other techniques.

VI. REFERENCES

[1] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, On Technical Security Issues in Cloud Computing. IEEE, 2009.

[2] Greg Boss, Padma Malladi, Denis Quan, Linda Legregni, Harold Hall, "Cloud Computing", October 2007, pp. 4-4

[3] PankajArora, RubalChaudhryWadhawan, Er. Satinder Pal Ahuja, Cloud Computing Security Issues in Infrastructure as a Service.Research paper volume 2,2012.

[4] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall, Four Edition, 2005, pp 189-193

[5] S. Halevi and H. Krawczyk, Public-key cryptography and password protocols Proceedings of the Fifth ACM Conference on Computer and Communications Security, pp. 122-131, 1998, ACM

[6] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. AtanuRakshit, "Cloud Security Issues", IEEE International Conference on Services Computing,2009.

[7] Meiko Jensen, J¨orgSchwenk, Nils Gruschka, Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing" .

[8] Samir El Adib and NaoufalRaissouni, "AES Encryption Algorithm Hardware Implementation:Throughput and Area Comparison of 128, 192 and 256-bits Key", International Journal of Reconfigurable and Embedded Systems (IJRES)Vol. 1, No. 2, July 2012, pp. 67~74ISSN: 2089-4864

[9] D. S. Kundi, S. Zaka, Q. Ain and A. Aziz, "A compact AES encryption core on Xilinx FPGA", in Proc. of 2nd International Conference on Computer, Control and Communication, pp.1-4, 2009.

[10] F. R-. Henriquez, N. A. Saqib and A. D-. Perez, "4.2 Gbits/s single chip FPGA implementation of AES algorithm",Electronics Letters, Vol. 39, No. 15, pp. 1115-1116, 2003.

[11] A.Aziz and N. Ikram, "Memory efficient implementation of AES S-boxes on FPGA", Journal of Circuits, Systems,and Computers, Vol. 16, No. 4, pp. 603-611, 2007.

[12] Joan Daemen and Vincent Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard."Springer, 2002. ISBN 3-540-42580-2

[13] J. Nechvatal, et. al., Report on the Developmentof the Advanced Encryption Standard (AES), National Institute of Standards and Technology, October 2, 2000, available at

[14] DES Encryption. Tropical Software. 2010. http://www.tropsoft.com/strongenc/des.htm (accessed March, 15,2010)

[15] Mohammad Musa, Edward Schaefer, and Stephen Wedig, A simplified AES algorithm and its linear and differentialcryptanalyses, Cryptologia27(April 2003), no. 2, 148–177.

[16] ShrivathsaBhargav, Larry Chen, AbhinandanMajumdar, Shiva Ramudit"128 bit AES Decryption" CSEE 4840 Project Report – May 2008, Spring 2008, Columbia University