IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Galois Field and Security for Online Data Storage in Cloud Computing

Rakesh A.Raval[*1], Suhas A. Patel[2], Dhaval B. Patel[3]
[*1,2,3] Assistant Professor, Merchant Engineering College, Basna, Gujarat, India
rakkesh14@gmail.com

Abstract

Cloud computing provides online data storage in which data is travelling over the Internet and is stored in remote locations so cloud computing presents a number of security concerns .We describe in this paper how to use Galois field in key partitioning scheme that uses polynomials of finite field.

Keywords: data storage, finite field, key partitioning, cloud computing.

Introduction

Cloud computing is a general term for anything that involves delivering hosted services over the Internet When you store your photos online instead of on your home computer, or use webmail or a social networking site, you are using a “cloud computing” service. Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications.[1] Securing data stored on distributed servers is of fundamental importance in cloud computing.[2] Data is travelling over the Internet and is stored in remote locations. In addition, cloud providers often serve multiple customers simultaneously. All of this may raise the scale of exposure to possible breaches, both accidental and deliberate. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. Cloud computing security processes should address the security controls the cloud provider will incorporate to maintain the customer's data security, privacy and compliance with necessary regulations.[8] cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance.[7] Security concerns relate to risk areas such as external data storage, dependency on the “public” internet, lack of control, multi-tenancy and integration with internal security.[7]

The approach to securing Data in the cloud which are stored on distributed servers and back it up on a single server and allow access upon the use of passwords that are needed to be frequently changed.[2]

In this paper we discuss the key distribution system for securing data in cloud.

Galois field (Finite Field) $\left(\boldsymbol{Gf}(\mathbf{2}^{\boldsymbol{n}})\right)$

A finite field is also called a Galois Field. It is so named in honor of Évariste Galois, a French mathematician. Galois is the first one who established the following fundamental theorem on the existence of finite fields:

Fundamental theorem of existence of finite field: An order-*n* finite field exists if and only if $n = p^m$ for some prime *p* (*p* is called the characteristic of this finite field) and some positive integer *m*.We usually use$\left(\boldsymbol{Gf}(\boldsymbol{p^n})\right)$ to represent the finite field of order $\boldsymbol{p^n}$.

Galois field is also known as finite field that contains a finite number of elements. Galois fields are important in number theory, cryptography; coding theory etc.It is particularly useful in translating computer data as they are represented in binary forms. [3]

The elements of Galois field is defined as,

$$Gf(p^n) = (0,1,2,\ldots\ldots\ldots\ldots,p-1)$$
$$\cup\ (p,p+1,p+2,\ldots\ldots,p+p-1)$$
$$\cup\ (p^2,p^2+1,p^2+2,\ldots\ldots,p^2+p-1)$$

$$\cup \dots\dots \cup\ (p^{n-1}, p^{n-1}+1, p^{n-1}+ 2, \dots\dots, p^{n-1}+p-1).$$

Where p is any prime number and n is positive integer.

Finite fields of order 2^n are called binary fields or characteristic-two finite fields. They are of special interest because they are particularly efficient for implementation in hardware, or on a binary computer. In binary system we represent each value with 0 and 1.Ultimately, binary system offers an alternative way of representing the elements of Galois field.[3] So a bit is an element of Gf(2),Also byte which is equivalent to 8 bits is an element of $Gf(2^8)$.In our research paper we will discuss about computing so we are focusing on Galois field of order 2 and 2^8.

Arithmetic of Galois field $Gf(2^n)$

Addition and subtraction:

A Galois field $\boldsymbol{Gf(2^n)}$ is consist of polynomials of degree $n-1$ or less, and their coefficients are 1 or 0.Let $\mathcal{F}$ and $\mathcal{g}$ are two polynomials belonging to $(\boldsymbol{2^n})$, with coefficients $a_{n-1}, a_{n-2}, \dots\dots a_1, a_0$ *and* $b_{n-1}, b_{n-2}, \dots\dots b_1,$ b_0 then addition of *f* and *g* is defined as,

$$\mathbb{H} = \mathcal{F} + \mathcal{g}$$

If $c_{n-1}, c_{n-2}, \dots\dots c_1, c_0$ are coefficient of polynomial h then,

$$c_m = a_m + b_m\ (mod\ 2)$$

Where $0 \le m \le n-1$.

Similarly subtraction of *f* and *g* is defined as,

$$\mathbb{H} = \mathcal{F} - \mathcal{g}$$

and if $c_{n-1}, c_{n-2}, \dots\dots c_1, c_0$ are coefficient of polynomial h then,

$$c_m = a_m - b_m\ (mod\ 2)$$

Where $0 \le m \le n-1$.

Multiplication and multiplicative inverse

Let $\Theta(2)$ be an irreducible polynomial of degree at least n in $\boldsymbol{Gf(2^n)}$**,** irreducible means it cannot be factored into two or more polynomials in $\boldsymbol{Gf(2^n)}$ and each of the degree less than n.

Then multiplication of *f* and *g* is defined as,

$\mathbb{H} = (\mathcal{F}.\mathcal{g}\ (mod\ \Theta(2)\ )$

The multiplicative inverse of f is given by Ξ (2)such that

$(\mathcal{F}.\Xi\,(2))(mod\ m(2)) = 1.$

Construction of irreducible polynomial:

We now that there is one irreducible polynomial required for multiplication and multiplicative inverse. Thus the problem of how we can generate irreducible polynomials of a given degree.

Theorem 1.1: There exists a probabilistic algorithm which, given as input a finite field $\mathbb{F}_q$ and positive integer n, produces as output an irreducible polynomial p(x) ∈ $\mathbb{F}_q$ [x] of degree n using Order (n^4 log (q)) operations.

The following lemma gives an explicit formula for the exact number of irreducible monic polynomials over $\mathbb{F}_q$ of degree n.

Lemma1.1: The number N_q(n) of monic irreducible polynomials of degree n in $\mathbb{F}_q$ [x] is given by:

$$N_q(n) = \frac{1}{n}\sum_{d/n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n}\sum_{d/n} \mu(d) q^{\frac{n}{d}}$$

Where μ is the Möbius function

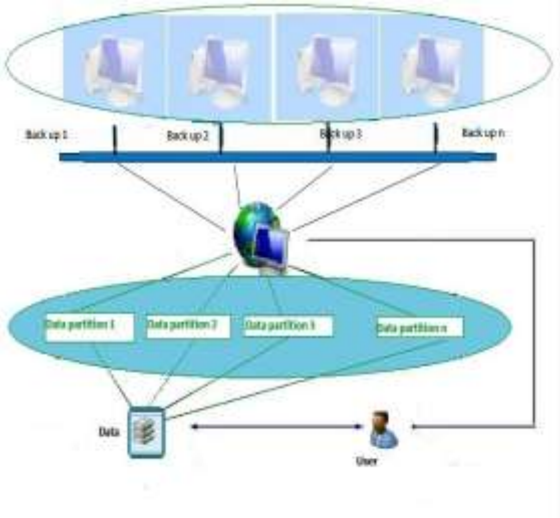
$\mu: N \to \{-1,0,1\}$ defined as,

$$\mu(n) = \begin{cases} 1 & if\ n = 1 \\ (-1)^k\ if\ n\ is\ product\ of\ k\ distinct\ prime \\ 0 \quad ifn\ is\ divisible\ by\ square\ of\ prime \end{cases}$$

Key distribution in cloud computing

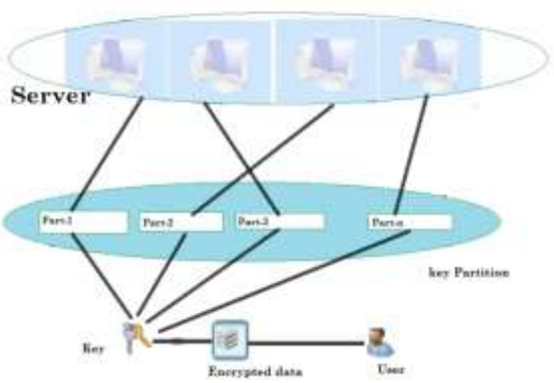
Galois field widely used in cryptography since each data are represented as a vector in finite field encryption and decryption using mathematical arithmetic is very straightforward and easy. [4]In cloud computing mostly used data partitioning scheme in which data are stored in various system on cloud but when size of data are very large then it is inefficient to create data partition and distribute over the network. As shown in figure 1, data are partitioned and stored in different system.

Figure1: Data partition method



For this type of problem user may wish to encrypt the data and store on the trusted single server and keep encryption key secret. The encryption key is almost very large and can not easy to remember it, therefore user may create partition of key and distribute them over the different system on the network. The key distribution of public keys is done through public key servers as shown in figure 2. When a person creates a key-pair, he keeps one key private and the other, public-key, is uploaded to a server where it can be accessed by anyone to send the user a private, encrypted, message.

Figure 2: Key Partition Method



Key partitioning using Galois field $Gf(2^n)$

We use polynomials in Galois field $\boldsymbol{Gf(2^n)}$**,** for key partitioning which is better than polynomial generalization of power encryption transformation. A Galois field $Gf(2^n)$ consist of polynomials of degree n-1 or less, such that their coefficients lie in $Gf(2\,)$.

Let $a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0$ $,where\ a_j = 1\ or\ 0.$ be a polynomial in $Gf(2^n)$.It may written in binary representation as$(a_{n-1}a_{n-2} \ldots .. a_1a_0)$.Now we generate p number of random polynomials of any random degree in $(\boldsymbol{2^n})$, say $k_1(x), k_2(x), \ldots ., k_p(x)$.

Let $\Theta(x) = x^n + d_{n-1}x^{n-1} + \cdots + d_1x + d_0$ $,where\ d_j \in Gf(2^n\,)$ be any irreducible polynomial.

Now we perform multiplication of product of p –polynomials modulo $\Theta(x)$ as defined earlier.

$$k_1(x)k_2(x) \ldots . k_p(x) \equiv \chi(x)\ mod\ \Theta(x)$$

Where $\chi(x)$ is the key polynomial.

$$\chi(x) \equiv k_1(x)k_2(x) \ldots . k_p(x)\ \ mod\ \Theta(x)$$

The random key generate is binary representation of $\chi(x)$ say, and the key partitions are binary representation of polynomials $k_1(x)k_2(x) \ldots . k_p(x)$ say $k_1, k_2, \ldots . k_p$.

Conclusion

We know that there are large numbers of problems of data security in cloud data storage. In this paper we have describe key encryption method, which include the encryption keys rather than the data. When sizes of data are very large then it is inefficient to create data partition and distribute over the network. This approach of data security is very secure and efficient when sizes of data are very large. Also the keys are distributed to authenticate person on the network so the data stolen or any other data security issues become very less.

References

[1] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing , Data Security Model for Cloud Computing, Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009) ,Qingdao, China, November 21-22, 2009, ISBN 978-952-5726-06-0.

[2] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, Ensuring Data Storage Security in Cloud Computing.

[3] Galois Field in Cryptography by Christoforus Juan Benvenuto May 31, 2012.

[4] S.Hemalatha1, Dr.R.Manicka Chezian2, Implicit Security Architecture Framework in Cloud Computing Based on Data Partitioning and Security Key Distribution, International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), 3(1), Dec.12-Feb.13, pp. 76-81, ISSN (Print): 2279-0047.

[5] Amit Sangroya, Saurabh Kumar, Jaideep Dhok, and Vasudeva Varma, Towards Analyzing Data Security Risks in Cloud Computing Environments.

[6] Vic (J.R.) Winkler, Data security in cloud computing.

[7] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, Homomorphic Encryption Applied to the Cloud Computing Security, Proceedings of the World Congress on Engineering 2012 Vol- I WCE 2012, July 4 - 6, 2012, London, U.

[8] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, An analysis of security issues for cloud computing, computing-security Journal of Internet Services and Applications 2013, ***4****:5 doi: 10.1186/1869-0238-4-5*

[9] www. en.wikipedia.org.

[10] http://searchcompliance.techtarget.com .
[11] http://www.jisajournal.com