JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Study An Enhanced Schmidt Samoa Cryptosystem for Securing information in Big Data

Narayana Galla[1] , Padmavathamma Mokkala[2]

[1]Department of Computer Science, Rayalaseema. University, Kurnool, India

[2]Department of Computer Science, S.V. University, Tirupathi, India

Abstract : Big Data is increasingly being used in many sectors. Research institutions, Industry and Government agencies were active in Big Data technologies and have been working more than ever before on building new data analysis techniques for Big Data. Business players and technology provider's work on creating new products and services and even developing entire new business models that are massively based on aggregation and analysis of extremely large and fast growing volumes of data. It is important to understand that although most of the organizations see the potential of Big Data, they are still in the research phase, and it is very few that are actively exploiting the benefits of the technologies.

IndexTerms **- eywords: Big data analytics, Study of He althcare architecture, ESS concept**

INTRODUCTION:

In the beginnings of Big Data technology many developed difficulty and challenges that are related to huge volumes of data are now with the start of addressed. Many developed organizations are able to consider and process large volumes of data which was once beyond their potential. While many different industrial domains have been benefited through the use of big data technologies where cyber security is one field that is just beginning to explore the compensation of big data analytics to provide the security of susceptible data. The ability to notice or detect and stop cyber-attacks can make or break an endeavor data secure. By means of big data, organizations may be 1able to carefully detect threats, create more defense mechanisms and improve securing the susceptible data.

Big Data Security = Big Challenge

LEATURE SURVEY

Based on the above research paper major aspect is security implementation on whole information in the Big Data. The challenge here is implementing security is not cost effective. To overcome this drawback we are proposing policy wise and sensitive data security. In our research work, we will focus on securing sensitive data in Big data using cryptosystem and classifying the sensitive data applying the standardized policy such as Medical data, Bank data, Education, E-Commerce, Insurance etc., our research work focuses on providing the solutions for securing the sensitive data in Big Data environment for privileged users.

In below table we are enlightening major sectors of Big data operation and their security challenges in real world system like Finance \

Payment, Energy\Power sector, Communication and Health Sector.

tab : Big Data usage in different sector and their security Challenges

Sector	**Finance\Payment Sector**	**Energy Sector\ Power Sector**	**Telecommunications\ Communication**	**Health Sector**
Usage of Big Data	Analytics, data driven decision making, real time services offering, risk quantification and prediction models building, fraud patterns analysis, rogue users identification	Analytics, data driven decision making, risk quantification and prediction models building	Big Data provider: Increase volume for data storage, services optimization, adaptive e-services offering, real time services offering, data analytics, prediction models offering data driven decision making, risk quantification	Analytics, data driven decision making, real time services offering, risk quantification and prediction models offering data driven decision making, risk quantification
Security Challenges	Trustworthiness of devices collecting data · Source validation and filtering of data · Application software security · Access control and authentication · Interoperability of devices · Distributed systems security (DDoS attack)	Source validation and filtering of data · Application software security · Infrastructure Security · Distributed systems security (DDoS attack) · Access control and authentication	Source validation and filtering · Application software security · Access Control and authentication · Supply chain security · Secure data management · Infrastructure security · Secure Cloud use	Source validation and filtering of data · Application software security · Infrastructure Security · Distributed systems security (DDoS attack) · Access control and authentication Supply chain security · Secure data management

PROPOSED SYSTEM

The Scope of the research is developing fast and securing the sensitive data in Big Data. With this new approach, we will apply the standard policy such as PII, PID etc., to classify the sensitive and non-sensitive data, applying the cryptosystem for protecting the sensitive data at application level.

In our approach our secure model will provide organizations which can restrict the sensitive data access and data theft which leads potential threat of the sensitive data. To overcome existing system like Full Disk[2] Encryption, File Level Encryption, sensitive data access issues, we propose the privileged user access control on sensitive data in application level. Sensitive data can be encrypted in application level framework will provide more secure than File level Encryption and Full-Disk encryption.

tab : Demonstration the advantages of different level encryption

RISK	**Full Disk Encryption**	**File Level Encryption**	**Application Encryption-Privileged Users**
Data unrecoverable when drive stolen or lost from data center	Yes	Yes	Yes
Data made inaccessible to root and system administrator	No	Yes	Yes
Data made in accessible to admin	No	Yes	Yes
Create access logs for threat analytic	No	No	Yes
Unstructured data , configure files, logs protected from theft	No	Yes	Yes

In our proposed approach secure model will provide organization which can restrict the sensitive data access and data theft [25] which leads potential threat of the organization. To overcome this issue we are proposing the privilege user access control on sensitive data at application level.

tab. Demonstration the advantages of Time & Security Complexity different

RISK	**Time Complexity**		**Security Level**
	Data Reading	**Data Writing**	
Full Disk	Time	Tim	Semi-
File Disk Encryption	Time Intense	Time Intense	Semi-Moderate
Application level Encryption for Privilege User's	Moderate	Modera te	Moderate

In application level encryption, we are proposing Policy Management [24], Encrypting the Sensitive Data, Decrypting the Sensitive Data for authorized users, privileged user access control management.

METHODOLOGY

In our model these are the necessary standards.

- *Developing the policy of arrangement system which will classify the sensitive and non-sensitive data using standardized policy system*
- *Data is moving\transferring to the Big Data cluster's through App Server, while transferring the data through App Server we need encrypt the sensitive data along with Policy Management using* cryptosystem.

- *Privileged user's Policy classification (PII \ PHI) sensitive data is encrypting and storing in the Big Data clusters*
- *While accessing sensitive data, primarily the system will check users their policy in Policy Management after successful authentication privileged users can decrypt the sensitive data. If non-privileged user's (Admin's, Root user's, Cloud Provider / Outsource Administrators) trying to access the sensitive data they will receive the encrypted data*

In our research work we are developing cryptosystem implementing in application level to achieve following assignment to secure the sensitive data. Using our cryptosystem will provide the different type policy classification system for authorized user's accessing the sensitive data.

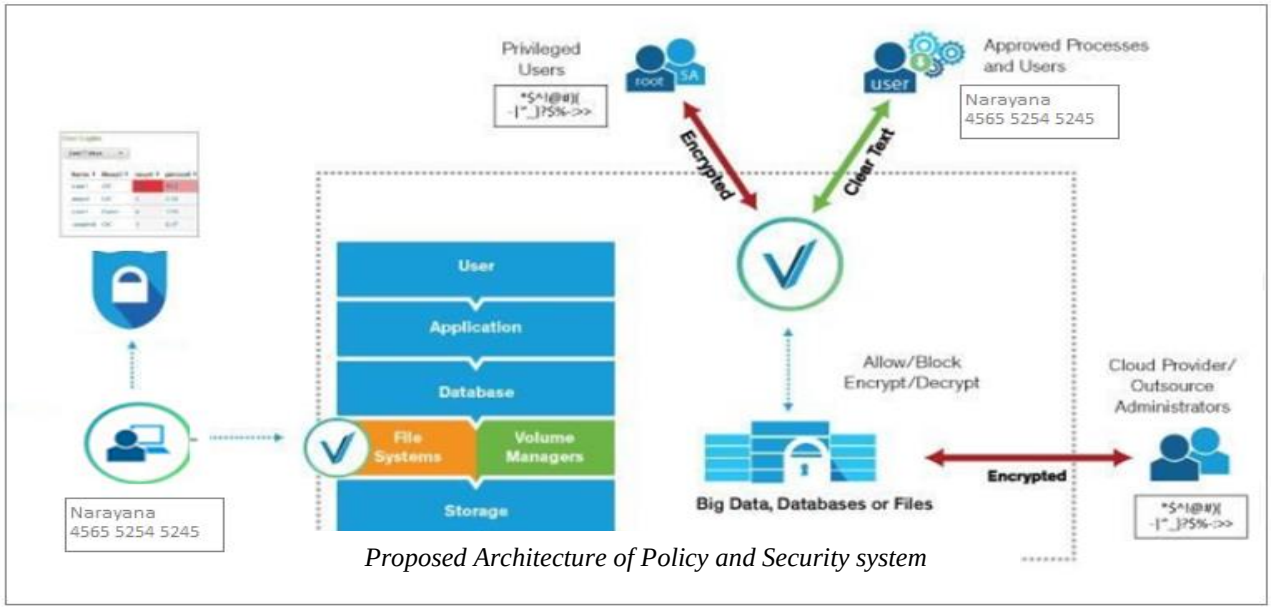
- *Design and Proposing Cryptosystem protocols at application level.*
- *Developing the authorized/ privileged user's access protocol cryptosystem on the sensitive data that they are entitled to access.*
- *Developing the system which will the protect data both at rest and in transit through Cryptosystem on sensitive or vital information.*

Enhanced Schmidt-Samoa keys, parameters

p	The large prime number
q	The large distinct prime number of p
N	The compute of p and q

The more relevant properties of Schmidt-Samoa PKC are the following:

- Two distinct large primes p and q



Proposed Architecture of Policy and Security system

Enhanced Schmidt - Samoa Definitions

Enhanced Schmidt-Samoa public-key algorithm is well described as below

Choose two large distinct primes p and q

Compute$N = p^i * \ q \ \ where \ i > 2$

ENHANCED SCHMIDT-SAMOA KEY GENERATION

The Enhanced Schmidt Samoa key phase consists of public and private key generation.

Choose random distinct two large prime number p and q.

$$N = p^i * \ q \ \ where \ i > 2$$

Where N is the public key of enhanced Schmidt Samoa

Compute the Private Key

$$d = N^{-1} \ mod \ lcm \ (p-1, q-1)$$

The public key is N and the private key is the set (d, pq)

The following is a numerical example for key generation operation of Enhanced Schmidt Samoa.

Domain parameters are as follows:

$$p = 11 \quad p = 13$$

We choose two distinct prime numbers p and q

Public key generation is below

$$N = p^i * q \quad where\ i > 2$$

Let's calculate N where N is public key

$$p = 11 \quad p = 13$$

Where $i = 3$

$$N = p^3 * q \quad where\ i = 3$$

$$N = 11^3 * 13$$

$$N = 11 * 11 * 11 * 13$$

$$N = 1331 * 13$$

$$N = 17303$$

N = 17303 is the Public Key

Private Key generation phase

First we need to calculate

$$lcm\ (p-1, q-1)$$

$$lcm\ (p-1, q-1) = lcm\ (11-1, 13-1)$$

$$= lcm\ (11-1, 13-1)$$

$$= lcm\ (10, 12)$$

$$= 60$$

$$d = N^{-1}\ mod\ lcm(p-1, q-1)$$

$$d = 17303^{-1}\ mod\ lcm(11-1, 13-1)$$

$$d = 17303^{-1}\ mod\ lcm(10, 12)$$

$$d = 17303^{-1}\ mod\ 60$$

$$d = 47$$

In Enhanced Schmidt-Samoa Cryptosystem public key N = 17303 and Private key $(d, pq) = (47, 60)$

Encryption: Suppose plaintext m to convert cipher text using public key

Plain text m = 7

$$cipher\ (c) = m^N\ mod\ N$$

$$cipher\ (c) = 7^{17303}\ mod\ 17303$$

$$cipher\ (c) = 8582$$

Decryption: The decryption returns the message m from the encrypted message c using the private key $(d, pq) = (47, 60)$

Compute

$$de - cipher = c^d\ mod\ pq$$

$$de - cipher = 8582^{47}\ mod\ (11 * 13)$$

$$de - cipher = 8582^{47}\ mod\ (143)$$

$$de - cipher = 8582^{47}\ mod\ (11 * 13)$$

$$de - cipher = 7 = message$$

$$de - cipher = message$$

Therefore de-cipher is equal to the plaintext m.

CONCLUSIONS:

The focus of this thesis is on security solutions for accessing the sensitive data for authorized user in Big-Data. The need for such services is based on a simple fact that for past couple of years Big-Data is creating a huge impact on the information technology and services. To protect the data secures and security we need a secure cryptosystem which we have presented in the chapter 3 i.e.,w3w threshold ENHANCED SCHMIDT SAMOA cryptosystem.

REFERENCES:

[1]. http://www.sas.com/en_us/insights/big-data/what-is-bigdata.html
[2]. https://globalecco.org/big-data-insider-threats-and-internationalintelligence-sharing
[3]. "Sensitive Information" (definition) Aug. 23, 1996. Retrieved Feb. 9 2013.
[4]. "Department Of Industry: Personal Information Protection And Electronic Documents Act" Canada Gazette, Apr. 03 2002. Retrieved Feb. 9 2013.
[5]. http://motherboard.vice.com/read/even-tor-cant-save-small-timehackers
[6]. https://www.qubole.com/blog/big-data/hadoop-security-issues/
[7]. https://securosis.com/assets/library/reports /Securing_Hadoop_Fi nal_V2.pdf
[8]. https://securosis.com/blog/securing-hadoop-architecturalsecurity-issues
[9]. http://www.bmc.com/blogs/big-data-security-issues-challengesfor-2016/