Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

A comparative study on shells in Linux: A review

Abdullah Kidwai[a], Chandrakala Arya[b,*], Prabhishek Singh[a], Manoj Diwakar[c], Shilpi Singh[d], Kanika Sharma[e], Neeraj Kumar[f]

[a] Department of CSE, Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida, India
[b] Department of School of Computing, Graphic Era Hill University, Dehradun, Uttarakhand, India
[c] Department of CSE, Graphic Era (Deemed to be University) Dehradun, Uttarakhand, India
[d] Department of CSE, Amity School of Engineering and Technology, Amity University Patna, India
[e] Department of IT, IMS Noida, India
[f] Department of IT, BBAU Lucknow, India

ARTICLE INFO

ABSTRACT

TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 8595 - 8602

Efficient Wavelet related Transforms in Image Denoising

Prabhishek Singh[1], Chandrakala Arya[2], Kanika Sharma[3], Manoj Diwakar[4]*, Shilpi Singh[5]

[1]Department of CSE, Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida, India Email: prabhisheksingh88@gmail.com

[2]Department of School of Computing, Graphic Era Hill University, Dehradun, Uttarakhand, India, Email:

arya.chandrakala@gmail.com

[3]Department of IT, IMS Noida, India, Email: sharma.kanika247@gmail.com

[4]Department of CSE, Graphic Era (Deemed to be University) Dehradun, Uttarakhand, India, Email:

manoj.diwakar@gmail.com

[5] Department of CSE, Amity School of Engineering and Technology, Amity University Patna, India, Email: shilpi.singh.it@gmail.com

Asian Journal of Computer Science and Technology
ISSN: 2249-0701 Vol.7 No.1, 2018, pp. 33-39

An Improved Security Threat Model for Big Data Life Cycle

Kanika[1], Alka[2] and R.A. Khan[3]
[1]Research Scholar, [2]Assistant Professor, [3]Professor,
[1,2&3]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Uttar Pradesh, India
E-Mail: Sharma.kanika247@gmail.com, alka_csjmu@yahoo.co.in, khanraees@yahoo.com

Abstract **- Big data is a huge amount of data created by individuals related to their medical, internet activity, social networking sites, energy usage communication patterns etc. From these sources, data is being collected and processed by various survey organizations, national statistical agencies, medical centres, and other companies etc. There are many security challenges which occur during data transactions, such as un-authentication, phishing, Vishing, data mining based attacks, etc. From a security point of view the biggest challenge for big data is the protection of user's privacy. Yazan et.al, have presented big data lifecycle threat model. This paper does a critical review of the work. An Improved Security Threat Model for Big Data Life Cycle has been proposed as a main contribution of the paper. A new phase i.e. data creation phase has been added to the life cycle and it is claimed that the phase is very important one with respect to security and privacy. To justify the claim theoretical and statistical evidences have been provided.**

behalf of this information, two reporters from New York Times were able to find the identity of user No. 4417749 based on just search history [17]. CISCO has estimated that at the end of 2016 the annual global data traffic will reach 6.6 zettabytes. So there is a need to develop such approaches that not only support the collection of a large amount of data but also effectively handle or operate vast data requests with minimum time and maximum privacy [3, 4]. While protecting the big data is a big question which needs to be answered whether a particular data is in the category of `public and private. [4].

For providing privacy and security, big data should be examined from diverse angles. A careful thinking should be there for the protection of data itself. To maintain the security of big data Yazan et.al proposed a Big Data Lifecycle threat model. This threat model is based on the

Journal of Advanced Research in Dynamical and Control Systems
ISSN 1943-023X

Privacy Policy: A Novel Approach to Preserve Confidentiality in Big Data

Kanika, Alka Agrawal, R.A.Khan

Abstract:

Information security is the essential part of any individual's life. Users data is fragmented everywhere in the cyber space, so it has increased the risk of privacy violation on user's information. This big data scattered environment multiple parties are involved and provided a rich ground for unauthorized parties to misuse the data including information theft, unauthorized access, privacy attacks etc. Preserving privacy is a way to share anonymous information to make sure security against identity disclosure of a user. There is need to impose big data privacy policies to avoid misuse of individuals information. In this paper authors proposed privacy preserving policies to address privacy and security of user's data with architecture to minimize security risks and privacy. The proposed privacy policy framework consists of the reutilization of an open-source and opens specifications rights management system, and adapting the required components to address the specific privacy and security requirements that must be faced when managing user's data.

Issue: 04-Special Issue

Year: 2018

Pages: 50-56

Purchase this Article

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

RSA based encryption approach for preserving confidentiality of big data

Kanika Sharma [a], Alka Agrawal [a], Dhirendra Pandey [a], R.A. Khan [a], Shail Kumar Dinkar [b]

[a] Department of IT, Babasaheb Bhimrao Ambedkar University, Lucknow, India
[b] G.B. Pant Institute of Engineering and Technology, Pauri Garhwal, Uttarakhand, India

ARTICLE INFO

Article history:
Received 30 April 2019
Revised 17 October 2019
Accepted 18 October 2019
Available online xxxx

Keywords:
Big data
Sensitive health information
Security
Key generation
RSA encryption

ABSTRACT

Sensitive Health Information (SHI) is a developing patient-centric model of medical data exchange, which is frequently outsourced to be stored at third party servers. Though, there have been various privacy issues as SHI could be disclosed to the unauthorised and third parties. This is a promising method to encrypt the SHI before outsourcing to assure the patients' control over access to their own SHI. However, challenges like scalability in key management and flexible access have remained the most significant issues toward achieving fine-grained, cryptographically data access control. In this paper, the authors proposed a novel patient-centric system model for access control to SHIs stored in semi-honest servers. For fine-grained and scalable access control for SHIs, authors have proposed an encryption technique which is an improvement over RSA techniques to encrypt every patient's SHI file. To different from previous works in secure data transmission, the authors focus on the data owner and divide users into several domains in SHI, which greatly decrease the key management complexity for data owners and users. Comprehensive analytical and experimental results are presented which reflect the efficiency of the proposed approach.