World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(6): 108-110
www.wwjmrd.com
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Deep kumar
Software Engineer, Igniva Solutions Private Limited, Mohali, Punjab, India

Various Approaches of Cryptography for Big Data Security: A Review

Deep kumar

Abstract
Big data is the emerging fields that linked to management of the huge records of data. That is the evolutionary concept of data warehousing that has been used for data mining and data processing. Big data provide better management under knowledge discovery process. Various operations have been implemented on the dataset instance to remove abnormal and un-useful information from the raw data so that a valuable dataset can be easily initialized. In this paper big data theory has been discussed that has been used for data management and security approaches that provide big data security. In this paper various approaches have been discussed that are based on group sharing of secret keys, ID based authentication and mobile based authentication and cryptography. On the basis of these approaches an optimum approach has to be discussed for safety of the information so that data can be stored under encrypted manner.

Keywords: Cryptography, Encryption, Big Data, KDD and Private Key Sharing

Introduction

Big Data

Big data and its analysis are at the center of modern science and business. These data are generated from online transactions, emails, videos, audios, images, click streams, logs, posts, search queries, health records, social networking interactions, science data, sensors and mobile phones and their applications. They are stored in databases grow massively and become difficult to capture, form, store, manage, share, analyze and visualize via typical database software tools. Big data is changing the land scape of security technologies for network monitoring, SIEM, and forensics. However, in the eternal arms race of attack and defense, big data is not a panacea, and security researchers must keep exploring novel ways to contain sophisticated attackers. Big data can also create a world where maintaining control over the revelation of our personal information is constantly challenged. In today's ambitious world, people desire everything to take place at their door steps. The knowledge or material which is saved in the system can be perceived over the mobile by the person anywhere in the world. This encourages more to move towards wireless technology as the peoples are able to obtain information anytime anywhere. Now a day there is an increase in users every day due to the fast growth in Wi-Fi telecommunication and cyberspace [4]. Since mobile devices are becoming smaller, economical, better and more linked, they are modifying the way people using and work with data. The ease and dynamic functionality provided by mobile devices, has lead to the inspiration for many industries to interrogate the benefits of using them.

Knowledge Discovery from Big Data

Knowledge Discovery from Data (KDD) entitle as some operations designed to get information from complicated data sets [6]. Reference [18] outlines the KDD at nine steps:

1. Application domain prior to information and defining purpose of process from customer's perspective.
2. Generate subset data point for knowledge discovery.
3. Removing noise, handling missing data fields, collecting required information to model and calculating time information and known changes.
4. Finding useful properties to present data depending on purpose of job.
5. Mapping purposes to a particular data mining methods.

Correspondence:
Deep kumar
Software Engineer, Igniva Solutions Private Limited, Mohali, Punjab, India

6. Choose data mining algorithm and method for searching data patterns.
7. Researching patterns in expressional form.
8. Returning any steps 1 through 7 for iterations also this step can include visualization of patterns.
9. Using information directly, combining information into another system or simply enlisting and reporting.

Cloud Computing in Big Data

If we talk about cloud computing it is a kind of technology that depends on the sharing of computer resources. It basically delivers the services through INTERNET. Primary goal of cloud computing is to reduce the investment cost for hardware and software, to increase the scalability as it provides everything on demand and the resources on cloud are always available and reliable. Cloud computing consist of computers connected to network that handles the load. The main benefit of cloud computing is to eliminate the cost at users end. User only required having a computer and simple software to access the cloud services rest is handled by the cloud. The user can put any king of data in the cloud and data in the cloud is safe from any damage and the user can access that data any time any place he or she just needs an INTERNET connection.

Benefits of Big data

- Easy analysis of information from multiple sources that otherwise have no meaning.
- Big data is timely that means that workers are working hard to manage the data and make decisions.
- Big data is trust worthy. Data accumulated from multiple sources help in identification of exact patters. This data is more reliable than the one performed manually by workers.
- Big Data is Secure
- Big Data is Relevant -most of the companies are not happy with the way their filtering applications work. Thus they turn to big data.
- Big Data is Actionable
- Big data provides ample of opportunities for scratch companies to enter into the market.

Review of literature

SagirogluandDuyguSinanc et al [1] Big data is a term for massive data sets having large, more varied and complex structure with the difficulties of storing, analysing and visualizing for further processes or results. The process of research into massive amounts of data to reveal hidden patterns and secret correlations named as big data analytics. These useful information's for companies or organizations with the help of gaining richer and deeper insights and getting an advantage over the competition for this reason, big data implementations need to be analyzed and executed as accurately as possible. This paper presents an overview of big data's content, scope, samples, methods, advantages and challenges and discusses privacy concern on it.

Alvaro A. Cárdenaset al [2] Enterprises routinely collect terabytes of security-relevant data (for instance, network events, software application events, and people's action events) for regulatory compliance and post hoc forensic analysis. Large enterprises generate an estimated 10 to 100 billion events per day, depending nsize. These numbers will only grow as enterprises enable event logging in more sources, hire more employees, deploy more devices, and run more software. Unfortunately, this volume and variety of data quickly become overwhelming. Existing analytical techniques don't work well at large scales and typically produce so many false positives that their efficacy is undermined. The problem becomes worse as enterprises move to cloud architectures and collect much more data.

Ahmed DheyaaBashaet.al. [3] "Mobile Applications as Cloud Computing: Implementation and Challenge" As of now, mobile application and computing is picking up a high momentum and assuming an important part in upgrading the web figuring foundation. What's more, the cell phones and their applications have high procedure in the service ever had, and grew quickly. Mobile cloud computing is required to produce altogether more inventive with multi applications.

Alabbadi, M.et.al. [4] "Cloud computing for education and learning: Education and learning as a service (ELaaS)" This paper present Cloud figuring, regardless of its buildup, is as a rule broadly sent, with its dynamic versatility and use of virtualized assets, in numerous associations for a few applications. The Jericho Forum proposes a distributed computing arrangement model, called the Cloud Cube Model (CCM), which is in view of 4 criteria. To save the symmetry of the block, another distributed computing development model, called the Complete Cloud Computing Formations (C3F), is proposed. The IT exercises in the instructive and learning associations are then grouped as for the two criteria: mission criticality and affectability. Every class is then mapped into the proper position in the C3F, making ELaaS Quadrant. This basically creates a general theoretical system for ELaaS.

Cong Wanget.al. [5]Concentrated on cloud information storage security, which has dependably been a vital part of nature of administration. To guarantee the rightness of clients' information in the cloud, they propose a powerful and adaptable conveyed plan with two striking highlights, contradicting to its ancestors. Far reaching security and execution examination demonstrates that the proposed plan is profoundly productive and versatile against Byzantine failure, malevolent information change assault, and considerably server conspiring assaults.

FarzadSabahi. et.al. [6] Cloud registering worries about basic issues (for example, security) that exist with the across the board execution of distributed computing These sorts of concerns start from the way that information is put away remotely from the client's area; truth be told, it can be put away at any area. Security, specifically, is a standout amongst the most contended about issues in the distributed computing field; a few endeavours take a gander at distributed computing carefully because of anticipated security dangers. Subsequently, a few issues emerge that customers need to consider as they think about moving to distributed computing for their organizations. In this paper the creator compress unwavering quality, accessibility, and security issues for distributed computing issues, and propose doable and accessible answers for some of them.

Approaches used

Quantum cryptography and privacy with authentication for mobile data center: Quantum cryptography was proposed with Grovera AZ s algorithm (GA), and Pair Hand authentication protocol, to asset secure communications between the mobile users and authentication servers. Proposed model includes several

layers, and supports secure big data sending by mobile user to the nearest mobile data center. Data center front end Layer: verifications and identifications of the mobile user and big data using Quantum cryptography and authentication protocols Data reading interface Layer: during each operation of the interface, provides the best performance to minimize the complexity Quantum key processing Layer: quantum key distribution (QKD) based on QC is taken into considerations, and the size of the big data and level of the security key management Layer: the size of the big data and traffic load, the security key generations is performed, protocols based on QC are applied.

Group key transfer based on secret sharing over big data: A key transfer protocol for secure group communications over big data was proposed and is designed particularly for group-oriented applications over big data. Linear secret sharing schemes are used. A secret is divided into shares and is shared among a set of shareholders by a trusted dealer in such a way that authorized subsets of shareholders can reconstruct the secret but unauthorized subsets of cannot. The Vander monde Matrix is used as the share generation algorithm, [36]. Key transfer protocol consists of two phases: the secret establishment phase and the session key transfer phase.

ID-based generalized sign crypt ion method to obtain confidentiality or/and authenticity: Generalized sign crypt ion (GSC) methods ware used to provide multi-receiver identity-based generalized sign crypt ion (MID-GSC) method. Bilinear Diffie-Hellman (BDH) assumption and Computational Diffie-Hellman (CDH) assumption was used to ensure safety of the system. Either a single message or multiple messages can be sign crypted for one or multiple receivers and by one or multiple senders.

Conclusion

Big data has been widely used for storage of data at a large scope. Millions of GB data has been stored on the big data storage. In this paper various approaches that has been used for security of the information that has been uploaded on the big data server has been discussed. Encryption and cryptography are the best approaches that can be used for data preservation. On the basis of review of the study encryption approaches provide better data management for the entire network so that data can be stored in safe manner. In big data various servers are interconnected so that information can be easily transmitted through transmission channel.

References

1. Sagiroglu and DuyguSinanc“Big Data: A Review”, International Conf. on Big Data, 2013, pp. 42-47.
2. Alvaro A. Cárdenas, Pratyusa K. Manadhata, Sreeranga P. Rajan, “Big Data Analytics for Security”, 2016, pp. 112-119.
3. Ahmed Dheyaa Basha, IrfanNaufal Umar, and Merza Abbas, Member, IACSIT “Mobile Applications as Cloud Computing: Implementation and Challenge”, 2011 IEEE International Conference on Cloud Computing and Intelligence Systems, pp.467 – 471, 2013.
4. Alabbadi, M.M “Cloud computing for education and learning: Education and learning as a service (ELaaS)”, IEEE Conf. on Interactive Collaborative Learning (ICL), vol.134, PP 589 – 594, 2011.
5. Cong Wang, Qian Wang, KuiRen and Wenjing Lou “Ensuring Data Storage Security in Cloud Computing”, IEEE conf. on Parallel Distributed and Grid Computing (PDGC), pp.1-9, 2009.
6. FarzadSabahi, “Cloud Computing Security Threats and Responses”, IEEE Trans. on Cloud Computing., vol. 11, no. 6, pp. 670 - 684, 2002.
7. Gaurav Raj, Dheerendra Singh, AbhayBansal, “Load balancing for resource provisioning using Batch Mode Heuristic Priority in Round Robin (PBRR) Scheduling”, Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), pp.308 – 314, 2012.
8. Jianfeng Yang, Zhibin Chen “Cloud Computing Research and Security Issues” Computational Intelligence and Software Engineering (CiSE), Vol. 978-1-4244-5392, pp.1 – 3, 2010.
9. Jaber, A.N. “Use of cryptography in cloud computing”, IEEEControl System, Computing and Engineering (ICCSCE), PP 179 – 184, 2013.
10. Kalagiakos, P. Karampelas, P “Cloud computing learning” IEEEApplication of Information and Communication Technologies (AICT), pp. 1 – 4, 2011.
11. Mehmet Yildiz, JemalAbawajy, TuncayErcan and Andrew Bernoth “A Layered Security Approach for Cloud Computing Infrastructure” 2009 10th International Symposium on Pervasive Systems, pp 763 – 767, 2009.
12. Md. ImrulKayeset al. “Test Case Prioritization for Regression Testing Based on Fault Dependency” 2009 10th International Symposium on Pervasive Systems,pp.3-11, 2013