**\*\*\*\*\* File Name Mapping \*\*\*\*\***

0: "before\_Big\_Data\_Analytics\_for\_Security\_Intelligence.txt"

1: "before\_Big\_Data\_Taxonomy.txt"

2: "before\_Comment\_on\_Big\_Data\_Future\_of\_Privacy.txt"

3: "before\_CSA13-Top10Crypto\_.txt"

4: "before\_CSCC-Cloud-Customer-Architecture-for-Big-Data-and-Analytics.txt"

5: "iso\_ISO-IECJTC1-WG9\_N0087\_N0087\_WD\_of\_ISOIEC\_20546\_1st\_Edition.txt"

6: "iso\_N0147\_ISO\_IEC\_20546\_2nd\_WorkingDraft\_.txt"

7: "iso\_N0154\_ISO\_IEC\_20547-3\_1st\_Working\_Draft.txt"

8: "iso\_N0200\_ISO-IEC\_20546\_Committee\_Draft.txt"

9: "itu\_ITU-T-A5-TD-new-Y.txt"

10: "itu\_ITUbroshure.txt"

11: "itu\_T-REC-Y.3600-201511-I!!PDF-E.txt"

12: "itu\_T-REC-Y.Sup40-201607-I!!PDF-E.txt"

13: "nist\_NIST.SP.1500-1.txt"

14: "nist\_NIST.SP.1500-2.txt"

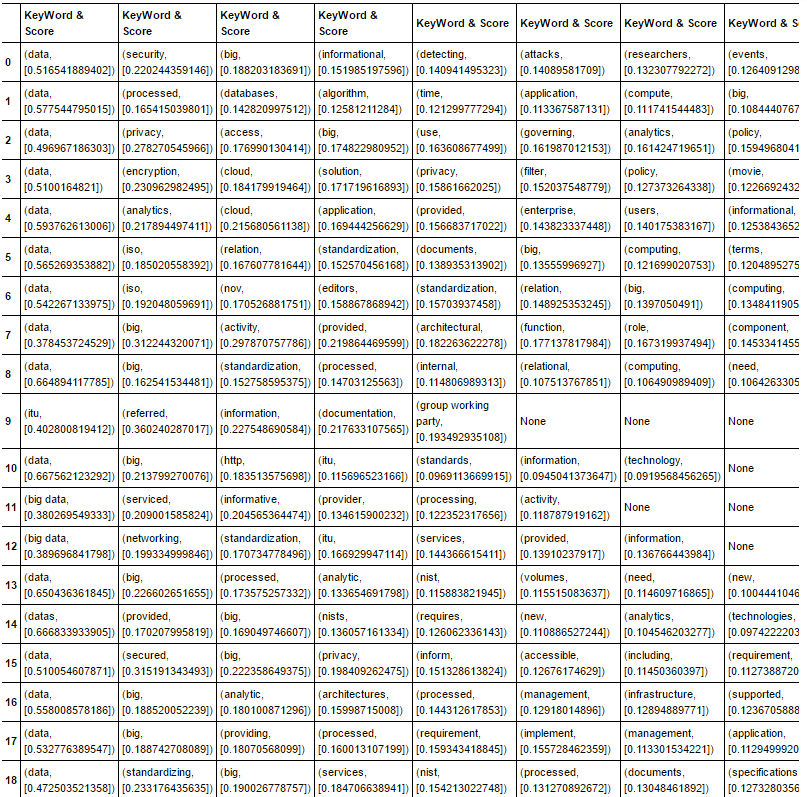
15: "nist\_NIST.SP.1500-4.txt"

16: "nist\_NIST.SP.1500-5.txt"

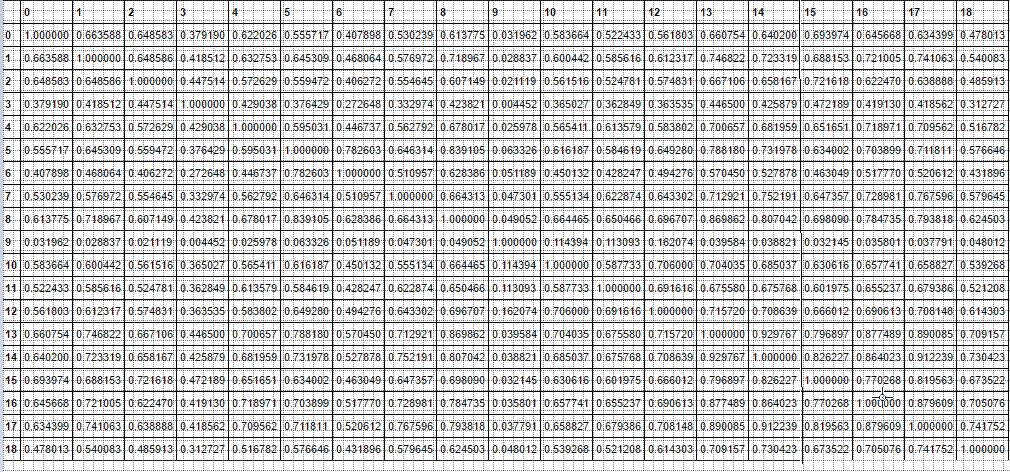
17: "nist\_NIST.SP.1500-6.txt"

18: "nist\_NIST.SP.1500-7.txt"

#### KeyWords extraction.



**TF – IDF matrices and Search cosine similarity between documents.**



#### Examples of Summaries by improved "TextRank" algorithm.

**The length is 120 words.**

|  |  |
| --- | --- |
| **Document ID** | **Summary** |
| **0** | The technological advances in storage, processing, and analysis of Big Data include (a) the rapidly decreasing cost of storage and CPU power in recent years; (b) the flexibility and cost-effectiveness of datacenters and cloud computing for elastic computation and storage; and (c) the development of new frameworks such as Hadoop, which allow users to take advantage of these distributed computing systems storing large quantities of data through flexible parallel processing.  Big Data Analytics for Security Intelligence Analyzing logs, network packets, and system events for forensics and intrusion detection has traditionally been a significant problem; however, traditional technologies fail to provide the tools to support long-term, large-scale analytics for several reasons. |
| **4** | Provider cloud elements include: Data Integration Streaming Computing Data Repositories Actionable Insight Transformation and Connectivity. A cloud computing environment often allows provisioning decisions to be delayed until data volume, velocity and related processing requirements are better understood.  Types of data repositories include: Copyright 2015 Cloud Standards Customer Council Catalog Data Virtualization Landing, Exploration & Archive Deep Analytics & Modeling Interactive Analysis & Reporting Results from discovery and IT data curation create a consolidated view of information that is reflected in a catalog.  Key capabilities include: Copyright 2015 Cloud Standards Customer Council Page 10 Enterprise Security Connectivity Transformations Enterprise Data Connectivity API Management Monitors usage and secures results as information is transferred to and from the cloud provider services domain into the enterprise network to enterprise applications and enterprise data. |
| **9** | A.5 justification information for draft new Y.3600 (ex Y.BigData-reqts).  Introduction According to ITU procedures, as described in ITU-T Recommendation A.5, any normative reference to documentation produced outside the ITU (other than ISO and IEC texts) needs to be evaluated by the study group or working party before a decision is made to incorporate the reference in an ITU-T Recommendation.  This TD contains the A.5 justification information for new Y.3600 (ex Y.BigData-reqts). |
| **13** | Christine Hawkinson U.S. Bureau of Land Management Thomas Huang NASA Philippe Journeau ResearXis Pavithra Kenjige PK Technologies Orit Levin Microsoft Eugene Luster U.S. Executive Summary The NIST Big Data Public Working Group (NBD-PWG). Definitions and Taxonomy Subgroup prepared this NIST Big Data Interoperability Framework: Volume 1. Definitions to address fundamental concepts needed to understand the new paradigm for data applications, collectively known as Big Data, and the analytic processes collectively known as data science.  To ensure that the concepts are accurate, future NBD-PWG tasks will consist of the following: Defining the different patterns of communications between Big Data resources to better clarify the different approaches being taken; taking into account the efforts of other working groups such as International Organization for Standardization (ISO) Joint Technical Committee 1 (JTC 1) and the Transaction Processing Performance Council; Improving the discussions of governance and data ownership; Developing the Management section; Developing the Security and Privacy section; and Adding a discussion of the value of data. |
| **15** | PII disclosure issues abound Various issues; for example, playing terrorist podcast and illegal playback Unknown Privacy-preserving data analytics Aggregate reporting to content owners Compliance with regulations Government access to data and freedom of expression concerns Data-centric security such as identity/policy-based encryption Policy management for access control Computing on the encrypted data: searching/ filtering/ deduplicate/ fully homomorphic encryption Audits Securing data storage and transaction logs Key management Security best practices for non- relational data stores Security against DoS attacks Data provenance User, playback administrator, library maintenance, and auditor Unknown Audit DRM usage for royalties Unknown N/A Traceability to data owners, producers, consumers is preserved Analytics for security intelligence Machine intelligence for unsanctioned Unknown Unknown use/access 37 NIST BIG DATA INTEROPERABILITY FRAMEWORK: VOLUME 4, SECURITY AND PRIVACY NBDRA Component and Interfaces Security and Privacy Topic Use Case Mapping Event detection Forensics Playback granularity defined Subpoena of playback records in legal disputes 6.2 NIELSEN HOMESCAN: PROJECT APOLLO Nielsen Homescan involves family-level retail transactions and associated media exposure using a statistically valid national sample. |

#### Summaries by algorithms: LSA, Kullback–Leibler, LexRank.

|  |  |
| --- | --- |
| Document ID | Summary |
| 0 | LSA algorithm: For example, Big Data analytics can be employed to analyze financial transactions, log files, and network traffic to identify anomalies and suspicious activities, and to correlate multiple sources of information into a coherent view.  The human analyst is given the flexibility of combining multiple sensors according to known attack patterns (e.g., command-and-control communications followed by lateral movement) to look for abnormal events that may warrant investigation or to generate behavioral reports of a given users activities across time.  By using a MapReduce implementation, an APT detection system has the possibility to more efficiently handle highly unstructured data with arbitrary formats that are captured by many types of sensors (e.g., Syslog, IDS, Firewall, NetFlow, and DNS) over long periods of time.  **Kullback–Leibler algorithm:**  Big Data Working Group Big Data Analytics for Security Intelligence September 2013 CLOUD SECURITY ALLIANCE Big Data Analytics for Security Intelligence v 2013 Cloud Security Alliance All Rights Reserved All rights reserved.  Big Data differentiators The term Big Data refers to large-scale information management and analysis technologies that exceed the capability of traditional data processing technologies.1 Big Data is differentiated from traditional technologies in three ways: the amount of data (volume), the rate of data generation and transmission (velocity), and the types of structured and unstructured data (variety) (Laney, 2001) (Figure 1).  Experiments on a 2 billion HTTP request data set collected at a large enterprise, a 1 billion DNS request data set collected at an ISP, and a 35 billion network intrusion detection system alert data set collected from over 900 enterprises worldwide showed that high true positive rates and low false positive rates can be achieved with minimal ground truth information (that is, having limited data labeled as normal events or attack events used to train anomaly detectors).  **LexRank algorithm:**  Big Data Analytics for Security Intelligence Analyzing logs, network packets, and system events for forensics and intrusion detection has traditionally been a significant problem; however, traditional technologies fail to provide the tools to support long-term, large-scale analytics for several reasons: Big Data Analytics for Security Intelligence. The security data warehouse driving this implementation not only enables users to mine meaningful security information from sources such as firewalls and security devices, but also from website traffic, business processes and other day-to-day transactions. This incorporation of unstructured data and multiple disparate data sets into a single analytical framework is one of the main promises of Big Data. Big Data Analytics for Security Intelligence. The WINE Platform for Experimenting with Big Data Analytics in Security The Worldwide Intelligence Network Environment (WINE) provides a platform for conducting data analysis at scale, using field data collected at Symantec (e.g., anti-virus telemetry and file downloads), and promotes rigorous experimental methods (Dumitras & Shoue, 2011). |
| 4 | LSA algorithm: Another benefit is the ability to develop applications on dedicated resource pools in a hybrid cloud deployment that eliminates the need to compromise on configuration details like processors, GPUs, memory, networking and even software licensing constraints. Finally, because data is generally held in its original form for longer periods of time, it is possible to create multiple correlation and prediction algorithms to drive organizations towards better analytics and, ultimately, the best supported version of the truth. They promote better understanding of results by showing important areas of interest, highlighting outliers, offering innovative ways to refine and filter complex data, and by encouraging deeper exploration and discovery.  **Kullback–Leibler algorithm:**  Cloud Customer Architecture for Big Data and Analytics illustrates a simplified enterprise cloud architecture for big data and analytics.  Provider cloud elements include: Data Integration Streaming Computing Data Repositories Actionable Insight Transformation and Connectivity A cloud computing environment often allows provisioning decisions to be delayed until data volume, velocity and related processing requirements are better understood.  Copyright 2015 Cloud Standards Customer Council Data to be integrated can come from public network data sources, enterprise data sources, or streaming computing results.  **LexRank algorithm:**  These insights are used by users and enterprise applications as well as stored in data storage systems. Provider cloud elements include: Data Integration Streaming Computing Data Repositories Actionable Insight Transformation and Connectivity A cloud computing environment often allows provisioning decisions to be delayed until data volume, velocity and related processing requirements are better understood. Key capabilities include: Copyright 2015 Cloud Standards Customer Council Page 10 Enterprise Security Connectivity Transformations Enterprise Data Connectivity API Management Monitors usage and secures results as information is transferred to and from the cloud provider services domain into the enterprise network to enterprise applications and enterprise data. |
| 9 | LSA algorithm: A.5 justification information for draft new Y.3600 (ex Y.BigData-reqts).  Introduction According to ITU procedures, as described in ITU-T Recommendation A.5, any normative reference to documentation produced outside the ITU (other than ISO and IEC texts) needs to be evaluated by the study group or working party before a decision is made to incorporate the reference in an ITU-T Recommendation.  This TD contains the A.5 justification information for new Y.3600 (ex Y.BigData-reqts).  **Kullback–Leibler algorithm:**  A.5 justification information for draft new Y.3600 (ex Y.BigData-reqts).  Introduction According to ITU procedures, as described in ITU-T Recommendation A.5, any normative reference to documentation produced outside the ITU (other than ISO and IEC texts) needs to be evaluated by the study group or working party before a decision is made to incorporate the reference in an ITU-T Recommendation.  This TD contains the A.5 justification information for new Y.3600 (ex Y.BigData-reqts).  **LexRank algorithm:**  A.5 justification information for draft new Y.3600 (ex Y.BigData-reqts).  Introduction According to ITU procedures, as described in ITU-T Recommendation A.5, any normative reference to documentation produced outside the ITU (other than ISO and IEC texts) needs to be evaluated by the study group or working party before a decision is made to incorporate the reference in an ITU-T Recommendation. This TD contains the A.5 justification information for new Y.3600 (ex Y.BigData-reqts). |
| 13 | LSA algorithm: Six federal departments and their agencies announced more than $200 million in commitments spread across more than 80 projects, which aim to significantly improve the tools and techniques needed to access, organize, and draw conclusions from huge volumes of digital data. Motivated by the White House initiative and public suggestions, the National Institute of Standards and Technology (NIST) has accepted the challenge to stimulate collaboration among industry professionals to further the secure and effective adoption of Big Data.  While bounded in comparison to Big Data, past solutions considered legal, social, and technical requirements for privacy in distributed systems, very large databases, and in High Speed Computing and Communications (HPCC).  **Kullback–Leibler algorithm:**  **LexRank algorithm:** |
| 15 | LSA algorithm: Six federal departments and their agencies announced more than $200 million in commitments spread across more than 80 projects, which aim to significantly improve the tools and techniques needed to access, organize, and draw conclusions from huge volumes of digital data. Motivated by the White House initiative and public suggestions, the National Institute of Standards and Technology (NIST) has accepted the challenge to stimulate collaboration among industry professionals to further the secure and effective adoption of Big Data.  Improved security software will include physical data correlates (e.g., access card usage for devices as well as building entrance/exit) and likely be more tightly integrated with applications, which will generate logs and audit records of previously undetermined types or sizes.  **Kullback–Leibler algorithm:**  Mapping Web Traffic Analytics to the Reference Architecture Security and Privacy Topic Use Case Mapping NBDRA Component and Interfaces Data Provider Application Provider Application Provider Data Consumer Data Provider Framework Provider Framework Provider Fabric End-point input validation Real-time security monitoring Data discovery and classification Secure data aggregation Privacy-preserving data analytics Compliance with regulations Government access to data and freedom of expression concerns Data-centric security such as identity/policy-based encryption Policy management for access control Computing on the encrypted data: searching/filtering/deduplicate/ful ly homomorphic encryption Audits Securing data storage and transaction logs Key management Security best practices for non- relational data stores Security against DoS attacks Data provenance Device-dependent.  Table 6: Mapping Pharmaceutical Clinical Trial Data Sharing to the Reference Architecture Security & Privacy Topic Use Case Mapping End-point input validation Real-time security monitoring Data discovery and classification Opaquecompany-specific Secure data aggregation Privacy-preserving data analytics Data to be reported in aggregate but preserving Opaquecompany-specific None Third-party aggregator NBDRA Component and Interfaces Data Provider Application Provider Application Provider Data Consumer Compliance with regulations Government access to data and freedom of expression concerns Data Provider Framework Provider Data-centric security such as identity/policy-based encryption Policy management for access control Framework Provider Computing on the encrypted data: searching/filtering/deduplicate/ful ly homomorphic encryption Audits Securing data storage and transaction logs Key management Security best practices for non- relational data stores Security against DoS attacks Data provenance 42 potentially small-cell demographics Responsible developer and third-party custodian Limited use in research community, but there are possible future public health data concerns.  **LexRank algorithm:**  The scope of the Subgroups work includes the following topics, some of which will be addressed in future versions of this Volume: Provide a context from which to begin Big Data-specific security and privacy discussions; Gather input from all stakeholders regarding security and privacy concerns in Big Data processing, storage, and services; Analyze/prioritize a list of challenging security and privacy requirements that may delay or prevent adoption of Big Data deployment; 2 NIST BIG DATA INTEROPERABILITY FRAMEWORK: VOLUME 4, SECURITY AND PRIVACY Develop a Security and Privacy Reference Architecture that supplements the NBDRA; Produce a working draft of this Big Data Security and Privacy document; Develop Big Data security and privacy taxonomies; Explore mapping between the Big Data security and privacy taxonomies and the NBDRA; and Explore mapping between the use cases and the NBDRA. Support both internal and third-party audits by unions, state agencies, responses to subpoenas Large enterprise security, transaction-level controlsclassroom to the federal government CSOs from the classroom level to the national level --- Standard NBDRA Component and Interfaces Data Provider Application Provider Application Provider Data Consumer Compliance with regulations Government access to data and freedom of expression concerns Data Provider Framework Provider Data-centric security such as identity/policy-based encryption Policy management for access control Computing on the encrypted data: searching/filtering/deduplicate/ful ly homomorphic encryption Audits Framework Provider Securing data storage and transaction logs Key management Security best practices for non- relational data stores Security against DDoS attacks. |

