Digital Technologies, 2015, Vol. 1, No. 1, 22-27
Available online at http://pubs.sciepub.com/dt/1/1/5
© Science and Education Publishing
DOI:10.12691/dt-1-1-5

Big Data in Distributed Analytics, Cybersecurity, Cyber Warfare and Digital Forensics

Lidong Wang[1,*], **Cheryl Ann Alexander**[2]

[1]Department of Engineering Technology, Mississippi Valley State University, USA
[2]Technology and Healthcare Solutions, Inc., USA
*Corresponding author: lwang22@students.tntech.edu

Received June 15, 2015; Revised July 03, 2015; Accepted July 07, 2015

Abstract Big Data can reduce the processing time of large volumes of data in the distributed computing environment using Hadoop. It also can predict potential cybersecurity breaches, help stop cyber attacks, and facilitate post-breach digital forensic analysis. This paper introduces Big Data applications in distributed analytics, general cybersecurity (general cyber threats, cyber attacks, and cyber security in cloud computing, etc.), cyber warfare, cyber defense, and digital forensics. Some methods and technology progress in these cyberareas are presented. Some challenges of Big Data applications in the areas and solutions to part of the challenges are also discussed.

Keywords: *Big Data, distributed analytics, cybersecurity, cyber warfare, cyber defense, digital forensics, telecommunication systems, information technology*

Cite This Article: Lidong Wang, and Cheryl Ann Alexander, “Big Data in Distributed Analytics, Cybersecurity, Cyber Warfare and Digital Forensics.” *Digital Technologies*, vol. 1, no. 1 (2015): 22-27. doi: 10.12691/dt-1-1-5.

1. Introduction

Critical infrastructure (CI) is a complex system of components that ensure transport, safety, health, communication, production, and any other activities necessary for a nation’s needs. Its destruction would affect the national economy and security. CI can be found in most of the following areas of activity: (1) government services; (2) transportation; (3) banking and financial services; (4) emergency services and health care; (5) water and food supply; (6) energy, oil, and gas production and storage; and (7) information, communication, and telecommunications [1].

In order to protect critical infrastructures from cyber attacks, system administrators can use a lot of methods such as checking system integrity, securing access control, and securing remote system management [2]. Cybercrime is any kind of crime that can be done in, with, or against networks and computer systems [3]. When data mobility is at a high level, there are highly increased risks, especially when data is transferred to another country with a different regulatory framework. Data relocation with high levels has negative implications for data availability, data protection, and data security [4]. Linguistic deception theory has provided approaches to identifying potentially deceptive texts. The integration of traditional e-discovery methods and linguistic approaches was proposed to discover deceptive text information within a given author’s written work, such as email. Firstly, a set of linguistic characteristics related to deception were identified; then a prototype classifier was constructed to analyze the text information and decide the features’ distributions [5].

Public key infrastructure (PKI) will never be the solution to integrity or usable for large-scale authentication of data at rest. Keyless signature infrastructure (KSI) is a disruptive new technology standard. It can enable mutual auditability of information systems, allow stakeholders to know the cause of a breach incident, and mitigate the risk of breach escalation in real time. KSI also allows companies to manage big data through four dimensions: volume, velocity, variety, and veracity [6]

Big Data will transform security analytics by collecting large data from a lot of sources such as vulnerability databases; performing real-time analysis for streaming data; and offering a consolidated view of security related information [7]. The challenges of Big Data include data inconsistence and incompleteness, data security, scalability, and timeliness. Big data security challenges lie in: (1) Data is extremely large in volume, channeling the protection approaches. (2)Security workload is much heavy. In general, big data is stored in a distributed environment; therefore, there are security threats from networks [8].This paper introduces Big Data applications in distributed analytics, cybersecurity, cyber warfare, cyber defense, digital forensics, and the challenges of Big Data in these cyber areas.

The organization of this paper is as follows: the next section presents distributed analytics; Section 3 introduces general cyber security; Section 4 presents cyber warfare and cyber defense; Section 5 presents digital forensics; and the final section is conclusions.

2. Distributed Analytics

Distributed computing refers to the use of distributed systems to solve computational problems. In distributed computing, a problem is divided into many tasks, each of which is solved by one or more computers [9].

Big Data technologies include distributed computational systems, distributed file systems, massively parallel-processing (MPP) systems, cloud-based storage and computing, and data mining based on grid computing, etc. Apache Hadoop is a software platform supporting data-intensive distributed applications. NoSQL database is used for large and distributed data management and database design. Clustering big data is also developing to distributed and parallel implementation. The network bandwidth capacity is a bottleneck in cloud and distributed systems, especially for big volume communication [8].

A distributed database (DDB) is interconnected logically and distributed over a computer network. A distributed database management system (DBMS) allows for managing of the distributed database and makes the distribution transparent to the users. A parallel DBMS is implemented on a multiprocessor computer. Parallel database systems help improve data processing performance through parallelizing indexing, loading, and querying data [10].

Hadoop is a framework for distributed processing of large data sets across clusters of computers. The Hadoop distributed file system (HDFS) and MapReduce are two critical components of Hadoop. MapReduce distributes computing jobs to each server in a cluster and collects the results. It is also a parallel data processing model intended for substantial data processing on cluster based computing architectures. The fault-tolerance and scalability of MapReduce is obtained through optimizing the execution engine once. A single-threaded implementation of MapReduce is usually not faster than a traditional (non-MapReduce) implementation, but gains are achieved in multi-threaded implementations. Using MapReduce has benefits only when there are fault-tolerance features and the optimized distributed shuffle operation [11,12].

In a distributed method, the file system is expected to achieve the following goals [10]:

- Reliability: The file systemcan recreate the original data from the distributed nodes in an undistorted and complete manner.
- High performance: It can locate the data of interest in a timely manner on the distributed nodes.
- High availability: It can account for failures and incorporate mechanisms for monitoring, fault tolerance, error detection, and automatic recovery.
- Scalability: The file system should permit additional hardware to be added for more storing capacity and/or better performance.

The extract, transform, and load (ETL) process provides an intermediary transformation layer between the end target database and outside sources. The ETL process is described as follows [10]:

- Extract: Data is read from multiple source systems into a single format; data is extracted from the data source.
- Transform: The source data is transformed into a format related to the solution to makes data consistent.
- Load: The transformed data is written into a warehouse.

In a distributed environment, the distributed execution of ETL is performed and ETL operations can occur on one of many worker servers. Besides HDFS and Map Reduce, there are a lot of other components in Apache Hadoop. Some of the components can help the ETL process. Most important, Big Data technologies make it easier to eliminate sources of latency compared with the traditional ETL approach that is time-consuming [12]. Integration of unstructured and structured data or information from distributed, heterogonous virtual clouds needs further research. Models and methods for continuous analytics as services for streaming data and analytics also need more research [13].

It is often to collect, process, and analyze big data in social network services and media services. Distributed-parallel data processing on cloud platform is becoming a useful approach. Most of distributed parallel application platforms focus on hosting Hadoop on cloud. A new architecture of distributed-parallel virtual environment on cloud (DIVE-C) platform was proposed to offer a transparent virtual computing environment for distributed parallel data processing applications [14]. In a cloud environment, user data is encrypted and stored using a large number of distributed servers [15].

Big Data is by nature a distributed processing and distributed analytics method. It can handle large and diverse structured, semi-structured, and unstructured datasets. It helps reduce the processing time of the growing volumes of data that are common in today’s distributed computing environments.

3. General Cyber Security

3.1. Cyber Security, Cyber Threats and Cyber Intelligence

Cybersecurity covers technologies, processes and practices that are designed to protect computers, networks and programs and data from damage, attack or unauthorized access [16]. A security model is described by three elements (availability, integrity, and confidentiality) and is shown in Table 1 [6]. Privacy infringement and security vulnerability can happen due to internal users or malicious attackers [15].

Table 1. A security model and its elements

Elements	**Description**
Availability	Making sure that the computing systems, the communication channels, and the security controls function correctly.
Integrity	Assuring and maintaining the consistency and accuracy of data and systems.
Confidentiality	Preventing the disclosure of data and information to unauthorized systems and individuals.

Cyber threats include targeted attacks, malware, spam, system privilege abuse, classified information leakage, vulnerabilities exposed by poor maintenance, user indiscretions (unintentional information leaking), and web defacements (misinformation/discredit), etc. [16].

Companies are increasingly exposed to cyber thieves and are the victims of corporate espionage due to both internal and external security breaches [6].

Cyber intelligence is a cyber-discipline that exploits some information collection and analysis methods to provide decision and direction to cyber commander and cyber operation units. Removing attack trace is necessary to hide the attack source or avoid the hostile cyber force's backtracking. Cyber intelligence helps perform removal methods such as deleting log file, router access records, and backdoor, etc [17].

3.2. Cyber Security in Cloud Computing

Cloud computing inherits a number of security attacks from conventional distributed systems, such as spoofing, password guessing, replay attack, transmission control protocol (TCP) hijacking, and malicious code (viruses, Trojan horses), etc. Cloud computing has its unique security threats including malicious insiders, account and service hijacking, shared technology's vulnerabilities, metadata spoofing attack, unknown risk profile, abuse and nefarious use of cloud computing, cloud malware injection attack, and insecure application programming interface (API) [18].

Security issues in a cloud computing environment include distributed big data processing, serviceability, virtualization, traffic management, access control, cryptography, authentication, and application security. Especially, data access using various resources requires an access control and authentication model for integrated control and management in a cloud computing environment. Ontology-based access control model (Onto-ACM), a semantic analysis model, was proposed to address the difference between users and service providers in the permitted access control. Ontology reasoning and semantic analysis method was used in the proposed model. The model is for intelligent context-aware access and dynamic access control that can address the limitations of cloud computing characteristics [19].

Data security issues in cloud storage include personal privacy protection, data security protection, intellectual property protection, and commercial secrets and financial information protection, etc. [8]. In a Data-as-a-service (DaaS) environment, data unavailability or data loss is a high risk thing. New methods and models should be created to handle the security risk of data that resides in cloud. New encryption approaches should be developed or new processes should be defined to separate core vs. none core data to reduce the security risk of hosting data in cloud [13].

Distributed data should be encrypted using a secret key; but big data is often divided into a large number of segments over a cloud computing environment. This causes difficulty in data management due to the different secret keys used in distributed servers and leads to a substantial overhead because numerous processes require for encryption/decryption and authentication. A weight-applied XOR-based scheme for efficient distribution storage and recovery was proposed to solve this problem. Various security vulnerabilities can happen in the block access token, which is for the permission control of data blocks in Hadoop. A new block access token management scheme was developed through modifying vulnerable parts of user data management over the Hadoop system [15].

3.3. Big Data Applications in Cyber Security

Big data technologies such as the Hadoop ecosystem (e.g. Hive, Pig, Mahout, and RHadoop), NoSQL databases, stream mining, and complex-event processing enable to analyze large-scale, heterogeneous datasets at a high speed. They can transform security analytics by improving the maintenance, storage, and analysis of security information [20].

Big Data analytics helps improve information security. Big Data analytics can be used to analyze network traffic, log files, and financial transactions; correlate multiple information sources into a coherent view; and identify suspicious activities and anomalies [7]. The combination of IBM security intelligence and Big Data analytics helps enhance capabilities for both external cyber security threats and internal risk detection/prevention through analyzing enriched security data (structured and unstructured) and identifying malicious activity hidden in the masses of enterprise data [21].

3.4. Big Data Challenges in Cyber Security

Big Data analytics extracts and correlates data, which makes privacy violation easier. Methods need to be developed to minimize privacy invasions during Big Data analytics. Abuse of big data stores should be prevented. It is necessary to secure big data stores and produce documents on security in cloud computing to secure big data. Big data provenance is another challenge. Because Big Data allows for expanding data sources, data can be from different sources. The integrity, authenticity or trustworthiness of each data source should be verified [7,20].

Vulnerabilities of datasets to cyber intrusion and design of biological weapons derived from the integration and analysis of Big Data in the life sciences are also possible risks related to Big Data. Table 2 lists current approaches to some challenges. These challenges affect the complete use of Big Data analytics to address health care, agricultural, environmental, and national and transnational security issues, etc. [22]

Table 2. Current solutions to some technical challenges of Big Data

Technical challenges	Current solutions
Lack of standard language and terminology	• Specific data collection techniques • Natural language processing technologies
Lack of access to need technical infrastructure	• Data storage, analysis, and sharing based on cloud • Open-source analytic techniques
Security of the cyber infrastructure and data repositories	• Cyber and data security law • Different approaches, including digital certificates, data encryption, access control technologies, and segregation of the networks
Data confidentiality and privacy	• Privacy protection laws • Corporate responsibility and/or norms • Different approaches, including data encryption, access control technologies, and segregation of the networks
Over fitting the analytic model	• Testing the model using different data sources

4. Cyber Warfare and Cyber Defense

Cyber war is a kind of war that occurs on the Internet and on computers through electronic means. It is the use of computers to disrupt the activities of an enemy country, especially the deliberate attack of communication systems. A successful cyber war can inflict big damage on both a country's utility grids and its information infrastructure [23,24].

Cyber warfare is a kind of latent aggression committed by a state or organized crime groups to weaken the military and economic resources of an attack target state or target groups [3]. Cyber warfare includes deterrence, offense, and defense. The most possible targets of cyber warfare are critical networks [23,25]. At present, cyber warfare is limited to networks of computers and network-attached systems. However, it will expand and encompass all electronic information processing systems across land, sea, air, space, and cyberspace [26].

Cyber space is called the 5th space of warfare (after land, sea, air, and space). It is a network of interdependent information technologies including computer systems, the Internet, telecommunications networks, and embedded processors [16,26]. It is a virtual unowned computer creation. It requires a good information infrastructure as well as technical equipment with a high level [3]. Cyber space is a very dynamic domain that crosses national boundaries and always produces uncertainty with new dimensions. The total cyber domain will also include non-Internet-connected networks such as satellite control networks, tactical data links, launch-control networks, and other non-traditional networks [16,26].

Cyber warfare consists of a lot of different threats. These threats can be divided into cyber espionage and cyberattacks [27,28]. Cyber espionage or cyber spying is a network penetration to learn how to steal information, prepare the network for theft, or commit theft [24]. Cyber attacks are any actions that are taken to destroy the function of a computer network for a political or national security purpose [24]. Cyber attacks take place in a near-instantaneous manner and on a frequent basis. Attackers use malicious worms as a main approach to targeting software vulnerabilities. Antivirus programs can prevent, detect, and remove malware. An e-epidemic SEIR (susceptible-exposed-infectious-recovered) model for the transmission of worms in a computer network was proposed. Efficiency of antivirus software and crashing of the nodes because of worms attack was analyzed [23].

Cyber terrorism is unlawful attacks and threats of attack against computers, networks and the information stored therein to intimidate or coerce a government or people in furtherance of social or political purposes [25]. In the era of information technology, cyber defense is emerging as a high priority. Ideal cyber defense is possibly achieved through the cooperation and partnership among countries, international organizations, and big information technology companies such as Microsoft and IBM [16]. Cyber defense methods can be divided into passive cyber defense and active cyber defense.

Passive cyber defense methods include firewalls, virus detection, threat detection, or patches. They mainly use a four-step model: (1) locate invading code; (2) unplug affected systems; (3) thwart particular attacks using security patches and solutions; and (4) use the patches and solutions system-wide. Cyber space security has been achieved much through passive cyber defense strategies. However, the increasing ineffectiveness to prevent threats and attacks using passive cyber defense has led to the emergence of active cyber defense [29].

Active cyber defense has three methods: detection and forensics, deception, and attack termination. Detection and forensics uses honeypots to attract potential adversaries (detection) and then look for behavior patterns (forensics). Allowing for a cyber-adversary to steal misleading or false information involves deception. Attack termination can be actions such as launching Denial of Service (DoS) attacks against attackers. Active cyber defense has challenges because it is defensive in name, but offensive in nature [29].

Cyber attacks infiltrate networks and systems. They include advanced malware, advanced persistent threats, and zero day attacks. A survey was completed among 706 IT security practitioners in government, financial services, and manufacturing in USA in December 2012. All respondents have an average of 10 years of experience and are responsible for managing cyber security. Table 3 shows that malware, malicious insiders, and server side injections (SSI) have most risk mitigation priority [30]. Table 3 only reflects general situations. Actually, DDoS has a higher mitigation priority compared with DoS in some situations. Viruses, worms and Trojans have worse impacts in a lot of business activity compared with Malicious insiders, SSI, DoS, and DDoS. Different perceptions and practices of Big Data analytics in cyber defense among government, financial services, and manufacturing are shown in Table 4 [30].

Table 3. Cyber attacks and their risk mitigation priority (Highest: 10; lowest: 1)

Cyber attacks	Risk mitigation priority
Malware	9.16
Malicious insiders	8.88
Server side injection (SSI)	8.81
Denial of service (DoS)	8.40
Distributed denial of service (DDoS)	8.04
Botnets	7.61
Viruses, worms and Trojans	7.35
Phishing and social engineering	5.66
Cross-site scripting	3.11
Web scrapping	1.41

Table 4. Importance, implementation, and awareness of the availability of Big Data analytics in cyber defense

Items	Government (%)	Financial Services(%)	Manufacturing (%)
Considering the great importance of Big Data analytics in cyber defense	41	53	48
Being aware of the availability of big data analytics for cyber defense	57	64	49
Have started implementing big data analytics in cyber defense	20	31	20

5. Digital Forensics

Cybercrime is the behavior of using computers in violation of laws for criminal purposes. Main cybercrimes include misuse of devices, access offenses, interception of data offenses, and the impairment of data [25].

Digital forensics (DF) refers to the set of techniques and method for collecting, analyzing, and preserving digital data collected from digital media, involved in an incident to extract useful evidence for the court. The key sources of digital forensic data on the Internet and network are shown in Table 5 [31].

Table 5. Key digital forensic data sources on the Internet and network

Digital forensics (DF) evidence source	**Type of evidence source**
Firewalls	Log files
Internetservice provider(ISP)	Client's traffic logged data that ismandatory preserved (1 year)
Network device	Log files, memories, buffers
Corrupted computer	Log files, working files, ambient data
Attacker's computer	Log files, working files, ambient data(slack and non-allocated space of HD)
Victim's computer	Log files, working files, ambient datachange of configuration, storestolen files, hash value changed files, web traces of the attack, and remained malicious files (Trojans, viruses, rootkit),etc.

Digital forensics uses scientific methods to analyze and interpret electronically stored information (ESI) to reconstruct events. Traditional forensics analyzes entire hard drives though the forensic examiner could be asked to analyze single e-mail messages or documents. The criminal targeting and criminal use of cloud computing has been increased; the need for civil forensic analysis of cloud computing has become more important. Cloud forensics has challenges in remotely located data, layers of complexity, authenticity, and lack of control [32].

Digital forensics software enables to analyze any information that is on a computer or over a network. The information can be office documents, disk images, program executables, memory dumps, network packet captures, and web pages and container files, etc. Digital forensics (DF) software development is different from that in other areas. The difference lies in data scale, data diversity, human capital, temporal diversity, and the crime scene investigation effect (called CSI effect). Data diversity is a challenge. Another problem in DF tool development is the amount of data that should be processed and the never-ending battle with storage and performance bottlenecks [33].

Douglas Schweitzer (2003) dealt with the principles of computer forensics [34]. With incident response and computer forensics, the safeguarding and protection of evidence is vital. A well-informed computer forensics professional should ensure that a subject computer system is carefully handled: (1) No potential evidence is damaged, destroyed, or compromised in any way by the procedures used to investigate the computer. (2) Extracted and possibly relevant evidence is properly handled and protected from later physical or magnetic damage. (3) A continuing chain-of-custody is established and maintained. (4) Business operations are affected for a limited amount of time, if at all. (5) Any client-attorney information that is inadvertently acquired during a forensic exploration is ethically and legally respected and not divulged. An organization should implement and maintain an effective records security program that incorporates the following: (1) Ensure that only authorized personnel have access to electronic records. (2) Minimize the risk of unauthorized modification or erasure of electronic records by storing sensitive data on removable media. (3) Ensure that appropriate personnel are trained to protect sensitive or classified electronic records. (4) Provide for backup and recovery of records to protect against information loss. (5) Ensure that electronic records security is included in the organization's overall information security plans [34].

An integrated proactive digital forensic (IPDF) model was proposed for internal and external attacks and overall network security in context of high-volume network traffic, big data and virtualized cloud environment. **The model is a** three layered **intrusion detection system (IDS)** architecture for external and internal threats. The first layer registers malicious attacks from black-listed web sites and unauthorized internal user processes. The second layer uses a role based access control (RBAC) rule to capture the internal unauthorized processes associated with particular user role. The third layer performs statistical analysis over the remaining users' processes for any "low-and-slow" deviations from the referenced process patterns associated with user and group of users' roles [31]. Big Data analytics can provide help for fraud detection. Big Data can provide security intelligence by shortening the time of correlating long-term historical data for forensic purposes [7].

6. Conclusions

Big Data can shorten the processing time of the growing volumes of data with diversity in the distributed analytics environments. Big data technologies help enhance cyber security by improving the maintenance, storage, and analysis of security information; identifying suspicious activities and malicious activities in general computer systems, distributed systems, and cloud computing environments.

Cyber warfare occurs in the cyber space. Cyber space is a global domain in the information environment. Cyber warfare includes a lot of actions and activities such as deterring information attacks and defending computer/ information networks. Cyber warfare can be engaged by states, agents of states, and non-state groups. Big Data will play an important role in cyber warfare and facilitate cyber defense.

Big Data analytics can help detect fraud and identify theft (such as credit card theft and identity theft). Big Data can facilitate digital forensic analysis.

Big Data analytics has some challenges such as data provenance, privacy invasions, and privacy violation, etc.

Solutions to part of challenges have been achieved; further research is need for the other challenges.

Big Data in terrorism informatics and computational criminology, Big Data visualization and human-computer interaction, integration of structured and unstructured data from distributed and heterogonous virtual clouds, and Big Data in cybersecurity and cyber warfare domains with non-Internet-connected networks, etc. can be further research topics.

Acknowledgment

This research was supported in part by Technology and Healthcare Solutions, Inc. in Mississippi, USA.

References

[1] F. Kadri, B. Birregah and E. Châtelet, The Impact of Natural Disasters on Critical Infrastructures: A Domino Effect-based Study, *Homeland Security & Emergency Management,* 11(2), 2014, pp. 217-241.

[2] A. Pătrascu, E. Simion, Critical infrastructures cyber protection using kernel based supervised learning techniques, *MTA Review,* Military Technical Academy Publishing House, Vol. XXIV, No. 2, 2014, pp. 59-66.

[3] Ž. Spalević, Cyber security as a global challenge today, *Singidunum Journal of Applied Sciences*, 2014, pp. 687-692.

[4] Z. Mahmood, Data Location and Security Issues in Cloud Computing, 2011 International Conference on Emerging Intelligent Data and Web Technologies, 7-9 Sept., 2011, Tirana, Albania, pp. 49-54.

[5] E. S. Crabb, Time for some traffic problems: enhancing e-discovery and big data processing tools with linguistic methods for deception detection, *Journal of Digital Forensics, Security & Law*, 9(2), 2014, pp. 167-179.

[6] S. Crawford, D. Piesse, Cyber insurance, security and data integrity, Part 1: Insights into cyber security and risk-2014, Technical Report, Ernst & Young LLP, 2014, pp. 1-17.

[7] A. A. Cárdenas, P. K. Manadhata, S. Rajan, Big Data Analytics for Security Intelligence, Technical Report, Cloud Security Alliance, September 2013, pp. 1-22.

[8] C.L. P. Chen, C.-Y. Zhang, Data-intensive applications, challenges, techniques and technologies: A survey on Big Data, *Information Sciences*, Vol. 275, 2014, pp. 314-347.

[9] P. Saxena, K. Govil, An Effective Reliability Efficient Algorithm for Enhancing the Overall Performance of Distributed Computing System, *International Journal of Computer Applications*, 82(5), 2013, pp. 30-34.

[10] B.A. Catalin, A. POCOVNICU, L. BĂTĂGAN, Distributed Parallel Architecture for "Big Data", *Informática Económica,* 16 (2), 2012, pp. 116-127.

[11] U. Kumar and J. Kumar, A Comprehensive Review of Straggler Handling Algorithms for MapReduce Framework, *International Journal of Grid Distribution Computing*,7 (4), 2014, pp. 139-148.

[12] T. Davenport, Big data at work: dispelling the myths, uncovering the opportunities, Harvard Business Review Press, Boston, Massachusetts, USA, 2014.

[13] H. Demirkan, D. Delen, Leveraging the capabilities of service-oriented decision support systems: Putting analytics and big data in cloud, *Decision Support Systems,* 55, 2013, pp. 412-421.

[14] I.-Y. Jung, B.-J. Han, H. Lee and C.-S. Jeong, DIVE-C: Distributed-parallel Virtual Environment on Cloud Computing Platform, *International Journal of Multimedia and Ubiquitous Engineering*, 8 (5), 2013, pp.19-30.

[15] S.-H. Kim and I.-Y. Lee, Block Access Token Renewal Scheme Based on Secret Sharing in Apache Hadoop, *Entropy*, 16, 2014, pp. 4185-4198.

[16] T. Naumovski, V. Kenkov, Concept and priorities of cyber defence, *Contemporary Macedonian Defense*, 14 (27), 2014, pp. 77-85.

[17] J. H. Eom, Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace, *International Journal of Software Engineering and Its Applications*, 8 (9), 2014, pp. 137-146.

[18] Y. A.Younis, M. Merabti, K. Kifayat, Secure Cloud Computing for Critical Infrastructure: A Survey, The 14th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting (PGNet 2013), Liverpool, UK, July 24-25, 2013, pp. 1-6.

[19] C. Choi, J. Choi, P. Kim, Ontology-based access control model for security policy reasoning in cloud computing, *Journal of Supercomputing*, 67, 2014, pp.711-722.

[20] A. A. Cárdenas, P. K. Manadhata, S. P. Rajan, Big Data Analytics for Security, *IEEE Security & Privacy*, 11 (6), 2013, pp. 74-76.

[21] R. Coulombe, Analyzing Big Data, *Security Technology Executive*, April 2013, pp.10-57.

[22] AAAS-FBI-UNICRI, National and Transnational Security Implications of Big Data in the Life Sciences, Prepared by the American Association for the Advancement of Science in conjunction with the Federal Bureau of Investigation and the United Nations Interregional Crime and Justice Research Institute, 2014, pp. 1-91.

[23] B. K. Mishra, A. Prajapati, Cyber Warfare: Worms' Transmission Model, *International Journal of Advanced Science and Technology*, 63, 2014, pp.83-94.

[24] D. Ritchey, Cyber Risk and Special Security Report, *SECURITY*, February 2014, pp. 40-46.

[25] G. D. Solis, Cyber warfare, *Military Law Review*, 219, spring 2014, pp. 1-52.

[26] C. W. J. Poirier, M. J. Lotspeich, Air Force Cyber Warfare, *Air & Space Power Journal*, September–October, 2013, pp. 73-97.

[27] K. Geers, Cyberspace and the changing nature of warfare. *SC Magazine*, 27 August, 2008.

[28] T. Gjelten, Cyberattacks, Terrorism Top U.S. Security Threat Report. *NPR.org*. 12 March 2013.

[29] A. Flowers and S. Zeadally, US Policy on Active Cyber Defense, *Homeland Security & Emergency Management*, 11(2), 2014, pp. 289-308.

[30] Ponemon Institute, Big data analytics in cyber defense, Research Report, EB-7499 02.13, February 2013, pp. 1-31.

[31] G. Grubor, I. Barać, Integrated proactive forensics model in network information security, *Singidunum Journal of Applied Sciences*, 2014, pp. 693-699.

[32] J. Dykstra, D. Riehl, Forensic collection of electronic evidence from infrastructure-as-a-service cloud computing, *Richmond Journal of Law & Technology*, Vol. XIX, No. 1, 2012, pp.1-47.

[33] S. Garfinkel, Lessons learned writing digital forensics tools and managing a 30TB digital evidence corpus, *Digital Investigation*, 9, 2012, S80–S89.

[34] D. Schweitzer, Incident Response: Computer Forensics Toolkit, Willey Publishing, Inc., 2003.