MEMORIAS

VIII CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA

III Taller Iberoamericano de enseñanza e innovación educativa en seguridad de la información

CIBSI ECUADOR 2015

10-12 NOV 2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS DEL ECUADOR - ESPE

Sangolquí, ECUADOR

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Con la Organización de

ESPE-Innovativa EMPRESA PÚBLICA

CRIPTORED

fundación IN-NOVA Centro de Innovación

Memorias del VIII Congreso Iberoamericano de Seguridad Informática

CIBSI 2015

Sangolqui (Quito), Ecuador, 10 al 12 de Noviembre del 2015

Compiladores

Luis Enrique Sánchez Crespo

Walter Marcelo Fuertes Díaz

Jorge Ramió Aguirre

ISBN: 978-9978-301-61-6

Universidad De Las Fuerzas Armadas Del Ecuador -ESPE

Quito, Ecuador

COMITÉ DEL PROGRAMA

Acurio, Santiago.	Pontificia Universidad Católica del Ecuador, ECUADOR
Antezana, Nicolás.	Sociedad Peruana de Computación, PERÚ
Areitio, Javier.	Universidad de Deusto, ESPAÑA
Baluja, Walter.	Ciudad Universitaria Juan Antonio Echeverría, CUBA
Betarte, Gustavo.	Universidad de la República, URUGUAY
Blanco, Carlos.	Universidad de Cantabria, ESPAÑA
Blasco, Jorge.	City University London, ESPAÑA
Borrell, Joan.	Universidad Autónoma de Barcelona, ESPAÑA
Caballero, Ismael.	Universidad de Castilla-la Mancha, ESPAÑA
Caballero, Pino.	Universidad de La Laguna, ESPAÑA
Cano, Jeimy José.	Universidad de Los Andes, COLOMBIA
Cansian, Adriano Mauro.	Universida de Estadual Paulista, BRASIL
Carozo, Eduardo.	Universidad de Montevideo, URUGUAY
Climent Coloma, Joan Josep.	Universitat d'Alacant, Espanya
Clotet, Roger.	Universidad Simón Bolívar, Venezuela
Daltabuit, Enrique.	Universidad Nacional Autónoma de México, MÉXICO
De Fuentes, José María.	Universidad Carlos III de Madrid, ESPAÑA
Del Rey, Ángel Martín.	Universidad de Salamanca, ESPAÑA
Ferrer, Josep Domingo.	Universidad Rovira i Virgili, ESPAÑA
Ferrer, Josep Lluis.	Universidad de Las Islas Baleares, ESPAÑA
Flórez, Angélica.	Universidad Pontificia Bolivariana, COLOMBIA
Fuertes Díaz, Walter Marcelo.	Universidad de las Fuerzas Armadas ESPE, ECUADOR
Fúster, Amparo.	Consejo Superior de Investigaciones Científicas, ESPAÑA
García, David.	Universidad de Castilla – La Mancha, ESPAÑA
García, Luis Javier.	Universidad Complutense de Madrid, ESPAÑA
Garrido, Giovana.	Universidad Tecnológica de Panamá, PANAMÁ
González Manzano, Lorena.	University Carlos III of Madrid
Hecht, Pedro.	Universidad de Buenos Aires, ARGENTINA
Henriques, Marco Aurelio.	Universidade de Campinas, BRASIL
Hernández, Emilio.	Universidad Simón Bolívar, VENEZUELA
Hernández, Leobardo.	Universidad Nacional Autónoma de México, MÉXICO
Hernández, Luis.	Consejo Superior de Investigaciones Científicas, ESPAÑA
Herrera Joancomartí, Jordi.	Universitat Autònoma de Barcelona
Karel Huerta, Monica.	Universidad Politécnica Salesiana, Ecuador

López, Javier.	Universidad de Málaga, ESPAÑA
López, Julio César.	Universidade de Campinas, BRASIL
Martínez Gasca, Rafael.	Universidad de Sevilla, ESPAÑA
Mendillo, Vincenzo.	Universidad Central de Venezuela, VENEZUELA
Merino Garcia, Jorge.	Universidad de Castilla-la Mancha, España
Miret, Josep María.	Universidad de Lleida, ESPAÑA
Modelo Howard, Gaspar,	Universidad Tecnológica de Panamá, Panamá
Monge, Raúl.	Universidad Técnica Federico Santa María, CHILE
Monteiro, Edmundo.	Universidade de Coimbra, PORTUGAL
Morales, Guillermo.	CINVESTVA Instituto Politécnico Nacional, MÉXICO
Muñoz Muñoz, Alfonso,	Criptored, ESPAÑA
Peinado, Alberto.	Universidad de Málaga, ESPAÑA
Pirrone, José.	Universidad Católica Andrés Bello (UCAB), Venezuela
Ramió, Jorge.	Universidad Politécnica de Madrid, ESPAÑA
Ramos, Benjamín.	Universidad Carlos III de Madrid, ESPAÑA
Rezk, Tamara.	INRIA, FRANCIA
Sánchez, Luis Enrique.	Universidad de Castilla-la Mancha, ESPAÑA
	Universidad de las Fuerzas Armadas ESPE, ECUADOR
Santos-Olmo Parra, Antonio.	Sicaman Nuevas Tecnologías, ESPAÑA
	Universidad de Castilla-la Mancha, ESPAÑA
Satizabal, Isabel Cristina.	Universidad Politécnica de Cataluña, España
Simoes, Paulo.	Universidade de Coimbra, PORTUGAL
Soriano, Miquel.	Universidad Politécnica de Cataluña, ESPAÑA
Tapia Recillas, Horacio.	Universidad Autónoma Metropolitana, MÉXICO
Torres Olmedo, Jenny Gabriela.	Escuela Politécnica Nacional, ECUADOR
Zurutuza, Urko.	Mondragon Unibertsitatea, ESPAÑA

ORGANIZACIÓN

PhD. Walter Marcelo Fuertes Díaz	Universidad de las Fuerzas Armadas ESPE. ECUADOR
PhD. Luis Enrique Sánchez Crespo,	Universidad de Castilla-la Mancha. ESPAÑA
	Universidad de las Fuerzas Armadas ESPE. ECUADOR
PhD. Jorge Ramió Aguirre,	Universidad Politécnica de Madrid. ESPAÑA

COMITÉ ORGANIZADOR LOGÍSTICO

MsC. Luis Recalde,	Universidad de las Fuerzas Armadas ESPE. ECUADOR
MsC. Fernando Delgado,	Fundación In-Nova. ESPAÑA
MsC Laura Gómez	Fundación In-Nova ESPAÑA
MsC. Esther Álvarez,	Fundación In-Nova. ESPAÑA
MsC Nolivos, Jaime	ESPE-Innovativa E.P,ECUADOR
MsC Quishpe, María Dolores	ESPE-Innovativa E.P,ECUADOR

COMITÉ DIFUSIÓN

PhD. David Garcia Rosado,	Universidad de Castilla-la Mancha. ESPAÑA
MsC. Antonio Santos-Olmo,	Universidad de Castilla-la Mancha. ESPAÑA

COMITÉ TÉCNICO

PhD. Walter Marcelo Fuertes Díaz	Universidad de las Fuerzas Armadas ESPE. ECUADOR
PhD. Luis Enrique Sánchez Crespo,	Universidad de las Fuerzas Armadas ESPE. ECUADOR

EDITORES

PhD. Luis Enrique Sánchez Crespo,	Universidad de Castilla La-Mancha. ESPAÑA
	Universidad de las Fuerzas Armadas ESPE. ECUADOR
PhD. Walter Marcelo Fuertes Díaz	Universidad de las Fuerzas Armadas ESPE. ECUADOR
PhD. Jorge Ramió Aguirre,	Universidad Politécnica de Madrid. ESPAÑA

CHAIR SESIONES

PhD, Angelica Flórez,	Universidad Pontificia Bolivariana, COLOMBIA
PhD. Walter Marcelo Fuertes Díaz	Universidad de las Fuerzas Armadas ESPE. ECUADOR
PhD, David García Rosado,	Universidad de Castilla – La Mancha, ESPAÑA
PhD, Pedro Hecht,	Universidad de Buenos Aires, ARGENTINA
PhD, Leobardo Hernández,	Universidad Nacional Autónoma de México, MÉXICO
PhD. Luis Enrique Sánchez Crespo,	Universidad de Castilla – La Mancha, ESPAÑA
	Universidad de las Fuerzas Armadas ESPE. ECUADOR
PhD. Jorge Ramió Aguirre,	Universidad Politécnica de Madrid. ESPAÑA

INDICE

PRESENTACIÓN

El VIII Congreso Iberoamericano de Seguridad Informática CIBSI 2015, tuvo lugar entre los días 10 al 12 de Noviembre de 2015 en la ciudad de SanGolqui (Quito), siendo organizado por el Departamento de Ciencias de la Computación de la Universidad de las Fueras Armadas y la Universidad Politécnica de Madrid, España, a través de la Red Temática de Criptografía y Seguridad de la Información Criptored.

Las jornadas se desarrollaron en el Auditorio de la Universidad de las Fuerzas Armadas y en el Salón de Conferencias del Edificio de Postgrado.

El evento está pensado desde la perspectiva de compartir experiencias a nivel de investigación en tecnologías de la seguridad informática, imprescindible actualmente para el desarrollo del conocimiento humano y del estado de bienestar de la sociedad. De esta manera, el propósito de CIBSI es promover y desarrollar el área de la seguridad de la Información, creando para ello un espacio tecnológico que facilite el intercambio de conocimiento y la formación de redes de colaboración en el ámbito de la investigación, el desarrollo y la innovación tecnológica.

Así mismo, se llevó a cabo el III Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información TIBETS. Desarrollado como un espacio propio dentro del congreso CIBSI, su objetivo es la presentación de experiencias en la enseñanza y formación en seguridad de la información, innovación educativa en dichas áreas, nuevas propuestas docentes y análisis de proyectos de colaboración académica y de programas de postgrados, de forma que fomente el planteamiento de posibilidades reales de colaboraciones docentes entre países.

A partir de los objetivos antes mencionados, la participación giró en torno a los siguientes ejes temáticos: Fundamentos de la seguridad de la información; Sistemas de gestión de seguridad de la información; Riesgos, recuperación y continuidad del negocio; Normativas y legislación en seguridad; Algoritmos y protocolos criptográficos; Vulnerabilidades y criptoanálisis; Técnicas de control de acceso e identificación; Técnicas de intrusión y análisis forense; Infraestructuras de clave pública; Seguridad en redes; Hacking; Ciberdelitos.

Para esta edición del CIBSI, se recibieron 49 trabajos, de los cuales solo el 30 fueron aceptados como “Full Paper”. En estas actas se recogen los 24 trabajos para el congreso CIBSI y 6 para el taller TIBETS, seleccionados como “Full Paper” por un Comité de Programa compuesto por 58 especialistas de una docena de países Iberoamericanos. Así como 8 artículos que se aceptaron como “Short Paper”. No se incluyen, sin embargo, la conferencia magistral inaugural de CIBSI 2015 "Seguridad de la Información, ¿en quién podemos confiar?" del Dº. David Barroso, la conferencia magistral "Metodología de Experimentación para la Ciberdefensa" de Dª. Esther Álvarez Gonzalez, y la conferencia magistral inaugural de TIBETS 2015 "Lecciones aprendidas en MESI 2.0 al horizonte de la enseñanza en ciberseguridad" del Dr. Jorge Ramió Aguirre.

Luis Enrique Sánchez Crespo

Walter Marcelo Fuertes Díaz

Jorge Ramió Aguirre

CIBSI

ECUADOR 2015

CIBSI

FULL PAPER

VIII CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA

III Taller Iberoamericano de enseñanza e innovación educativa en seguridad de la información

10-12 NOV 2015
UNIVERSIDAD DE LAS FUERZAS ARMADAS DEL ECUADOR - ESPE
Sangolquí, ECUADOR

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Con la Organización de

ESPE-Innovativa EMPRESA PÚBLICA

CRIPTORED

Fundación In-n-va Centro de Innovación

Towards a Security Model for Big Data

J. Moreno, D. G. Rosado, I. Caballero, M. Serrano and E. Fernández-Medina

***Abstract*— Big Data technologies describe a new generation of technologies and architectures, designed so organizations can economically extract value from very large volumes of a wide variety of data by enabling high-velocity capture, discovery, and/or analysis. This new technology raises new risks due to more volume and variety of data. Issues related to data security and privacy are one of the main concern in today's era of "big data." It is necessary to know before of involving in big data, which are the most important security needs, requirements and aspects to assure a high security level in our applications, transactions, data processing and decision management. In this paper we analyze the most important privacy and security aspects and requirements found in Big Data and we establish a security model aligned with security quality factor where the most relevant security and privacy aspects considered in Big Data are defined.**

***Keywords*— Big Data, Security, Information Model, security requirements.**

I. INTRODUCCION

THE term Big Data refers to large-scale information management and analysis technologies that exceed the capability of traditional data processing technologies. 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) [1].

The concept of big data can be framed by one of three perspectives. The first is a response to the technology problems associated with storing, securing and analyzing the ever-increasing volumes of data being gathered by organizations. This includes a range of technical innovations, such as new types of database and "cloud" storage, which enable forms of analysis that would not previously have been cost effective. The second perspective focuses on the commercial value that can be added to organizations through generating more effective insights from this data by means of the corresponding analysis. This has emerged through a combination of better technology and greater willingness by consumers to share personal information through Internet. The third perspective considers the wider societal impacts of big data, particularly the implications for individual privacy, and the effect on regulation and guidelines for ethical commercial use of this data [2]. We can see as the security aspects such as privacy is found to be very important in the proper concept of big data. In this position paper we are to discuss what is meant and the corresponding implications about Security when it comes to deal with big data.

Security is the capability of information systems to resist accidents or illegal or malicious actions that compromise the availability, authenticity, integrity and confidentiality of the data stored or transmitted and of the services that these networks and systems offer or make accessible, with a specific level of confidence [3].

Every day, 2.5 quintillion bytes of data are created, and about the 90% of these data in the world has been created in the last two years alone. Security and privacy issues are largely impacted by velocity, volume, and variety of big data, such as large-scale cloud infrastructures, diversity of data sources and formats, streaming nature of data acquisition and high volume inter-cloud migration. The use of large scale cloud infrastructures, with a diversity of software platforms, spread across large networks of computers, also increases the attack surface of the entire system [4].

The relatively less structured and informal nature of many Big Data approaches is their strength, but it also poses a problem: if the data involved is sensitive for reasons of privacy, enterprise security, or regulatory requirement, then using such approaches may represent a serious security breach. Database management systems support security policies that are quite granular, protecting data at both the coarse and the fine grain level from inappropriate access. Big Data software generally has no such safeguards. Enterprises that include any sensitive data in Big Data operations must ensure that the data itself is secure, and that the same data security policies that apply to the data when it exists in databases or files are also enforced in the Big Data context. Failure to do so can have serious negative consequences [5].

Issues related to data security and privacy are of paramount concern in today's era of "big data." Governmental agencies, the health care industry, biomedical researchers, and private businesses invest enormous resources into the collection, aggregation, and sharing of large amounts of personal data [6].

Once we have seen that the security and privacy is an important issue for big data, in this paper we want to define a security model which captures the most important security requirements or aspects for big data which cover with the needs and challenges found for big data.

The rest of the paper is structured in 3 more sections. The next section, section 2, defines the importance and most important security aspects found in big data. Section 3 presents a model of security factors for the systems information and that will help us to define our model of

J. Moreno, Grupo ALARCOS, Universidad de Castilla-La Mancha, Spain, julio.moreno3@alu.uclm.es

D. G. Rosado, Grupo de Seguridad y Auditoría (GSyA), Universidad de Castilla-La Mancha, Spain, david.grosado@uclm.es

I. Caballero, Grupo ALARCOS, Universidad de Castilla-La Mancha, Spain, ismael.caballero@uclm.es

M. Serrano, Grupo ALARCOS, Universidad de Castilla-La Mancha, Spain, manuel.serrano@uclm.es

E. Fernández-Medina, Grupo de Seguridad y Auditoría (GSyA), Universidad de Castilla-La Mancha, Spain, eduardo.fdezmedina@uclm.es

security for big data which is presented in Section 4. And, finally, we close in section 5 with our conclusions and agenda for future work.

II. Security in Big Data

A. Importance of the Security in Big Data

One of the biggest concerns in our present age revolves around the security and protection of sensitive information. In our current era of Big Data, our organizations are collecting, analyzing, and making decisions based on analysis of massive amounts of data sets from various sources, and security in this process is becoming increasingly more important. At the same time, more and more organizations are being required to enforce access control and privacy restrictions on these data sets to meet regulatory requirements such as HIPAA and other privacy protection laws. Organizations that have not properly controlled access to their data sets are facing lawsuits, negative publicity, and regulatory fines [7]. When big data drives security, the result is a unified, self-evolving approach and a holistic awareness that discrete, stitched-together solutions can't begin to achieve. A big data-driven security model has the following characteristics [8]:

- Diverse data sources – both internal and external – that multiply in value and create a synergistic learning effect as new security-related information is added
- Automated tools that collect diverse data types and normalize them so they are usable by analytics engines
- Analytics engines capable of processing vast volumes of fast-changing data in real time
- Advanced monitoring systems that continuously examine high-value systems and resources and make assessments based on behavior and risk models, not on static threat signatures
- Active controls such as requiring additional user authentication, blocking data transmissions or facilitating analysts' decision-making when high-risk activity is detected
- Centralized warehouse where all security-related data is made available for security analysts to query, either as a unified repository or, more likely, as a cross-indexed series of data stores
- Standardized views into indicators of compromise that are created in machine-readable form and can be shared at scale by trusted sources
- N-tier infrastructures that create scalability across vectors such as geography, storage and databases and have the ability to process large and complex searches and queries
- High degree of integration with security, and risk-management tools to facilitate detailed investigations of potential problems by analysts and to trigger automated defensive measures such as blocking network traffic, quarantining systems or requiring additional verification of user identity.

Privacy protection has become an elusive goal in the big data era as researchers have shown that "linkability threats" can re-identity individuals. Due to the highly personal nature of data of individuals, the policy framework should lead to best practices to store and transmit the data. Existing practices focus on keeping data encrypted at rest and in transit with an infrastructure to ensure proper authorization and authentication of entities to get access to the data [9].

B. Security Challenges and opportunities in Big Data

Security and privacy are a big data concern. Security at each level of architecture is required to preserve data from attacks at each level. Big data has a big issue of storage, computation, data mining, analysis, predictions, transactions and many more and at each point security must be implemented [10]. Big data security challenges can be classified into four categories [4]:

1. Infrastructure security
   (a) Secure computations in distributed programming frameworks.
   (b) Security best practices for non-relational data stores.
2. Data Privacy
   (a) Scalable and composable privacy preserving data mining and analytics.
   (b) Cryptographically enforced data centric security.
   (c) Granular access control.
3. Data Management
   (a) Secure data storage and transactions logs.
   (b) Granular audits.
   (c) Data Provenance
4. Integrity and reactive security
   (a) End-point input validation/filtering.
   (b) Real-Time security monitoring.

One of the key security issues involved with big data aggregation and analysis is that organizations collect and process a great deal of sensitive information regarding customers and employees, as well as intellectual property, trade secrets and financial information. As organizations look for identify how to gain value from such information, they are increasingly seeking to aggregate data from a wider range of stores and applications to provide more context in order to increase the value of the data, for example, to provide a clearer picture of customer preferences in order to better target them [11, 12].

- *Data Disposal:* Disposing of business documents from storage systems must also follow certain edicts, such as ensuring that the files are truly unrecoverable [11].
- *Authenticity:* A request to guarantee data authenticity usually emerges during legal investigations or compulsory procedures. The organization must be able to prove that documents have not been altered [11].
- *Access Control:* What about provisions for controlling who has access to data stored? Specific data is subject to strict security measures for access [11].

- *Discovery:* Ensuring quick access to business documents is a priority in discovery situations [11].
- *Encryption:* Data encryption is now integral to today's business processes as a means of ensuring privacy of sensitive or protected information. Strong encryption is a powerful element of data security practices for offering effective, continuous protection of data [11].
- *Data at rest protection:* The standard for protecting data at rest is encryption, which guards against attempts to access data outside established application interfaces [12].
- *Administrative data access*: Each node has at least one administrator with full access to its data. As with encryption we need a boundary or facility to provide separation of duties between different administrators [12].
- *Authentication of applications and nodes*: Hadoop can use Kerberos to authenticate users and add-on services to the Hadoop cluster. But a rogue client can be inserted onto the network if a Kerberos ticket is stolen or duplicated, perhaps using credentials extracted from virtual image files or snapshots [12].
- *Audit and logging*: If you suspect someone has breached your cluster, can you detect it? How could you do this? You need a record of activity. One area which offers a variety of add-on capabilities is logging [12]. The system logs significant events, such as object deletion, for audit purposes [11].
- *Monitoring, filtering, and blocking*: There are no built-in monitoring tools to look for misuse or block malicious queries [12].
- *API security*: The APIs for big data clusters need to be protected from code and command injection, buffer overflow attacks, and every other web services attack [12].
- *Account Monitoring and Control*: Manage accounts for big data users. Require strong passwords, deactivate inactive accounts, and impose a maximum permitted number of failed log-in attempts to help stop attacks from getting access to a cluster [13]
- *Secure processing*: Measures to secure the data within the analysis infrastructure are needed to mitigate potential vulnerabilities and to secure against leakage. These could include disk level encryption and a high level of network isolation. Big data should be secured in transit preferably using encryption [14].

III. Security Quality Factors

Like any other type of quality requirement [15], security requirements should be based on an underlying quality model [16]. Security signifies the degree to which valuable assets are protected from significant threats posed by malicious attackers [15]. As a quality factor (i.e., attribute, characteristic, or aspect), security can be decomposed into a hierarchical taxonomy of underlying quality subfactors [16, 17] as illustrated in the Fig. 1.

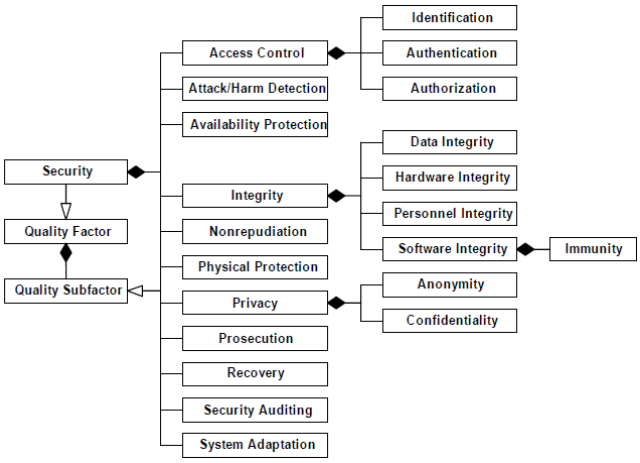

Figure 1. Quality Sub/actors a/the Security Quality Factor.

The security subfactors illustrated in Fig. 1 can be defined as follows [18]:

- *Access control* is the degree to which the system limits access to its resources only to its authorized externals (e.g., human users, programs, processes, devices, or other systems).

  The following are quality subfactors of the access-control quality subfactor:
  - *Identification* is the degree to which the system identifies (i.e., recognizes) its externals before interacting with them.
  - *Authentication* is the degree to which the system verifies the claimed identities of its externals before interacting with them.
  - *Authorization* is the degree to which access and usage privileges of authenticated externals are properly granted and enforced.
- *Attack/harm detection* is the degree to which attempted or successful attacks (or their resulting harm) are detected, recorded, and notified.
- *Availability protection* is the degree to which various types of DoS attacks are prevented from decreasing the operational availability of the system.
- *Integrity* is the degree to which components are protected from intentional and unauthorized corruption. Integrity includes the following:
  - *Data integrity* is the degree to which data components (whether stored, processed, or transmitted) are protected from intentional corruption (e.g., via unauthorized creation, modification, deletion, or replay).
  - *Hardware integrity* is the degree to which hardware components are protected from intentional corruption (e.g., via unauthorized addition, modification, or theft).
  - *Personnel integrity* is the degree to which human components are protected from intentional corruption (e.g., via bribery or extortion).

- *Software integrity* is the degree to which software components are protected from intentional corruption (e.g., via unauthorized addition, modification, deletion, or theft).
- *Immunity* is the degree to which the system protects its software components from infection by unauthorized malicious programs (i.e., malware such as computer viruses, worms, Trojan horses, time bombs, malicious scripts, and spyware). Such protected software components include complete programs, partial programs, processes, tasks, and firmware.

- *Nonrepudiation* is the degree to which a party to an interaction (e.g., message, transaction, transmission of data) is prevented from successfully repudiating (i.e., denying) any aspect of the interaction.
- *Physical protection* is the degree to which the system protects itself and its components from physical attack.
- *Privacy* is the degree to which unauthorized parties are prevented from obtaining sensitive information. Privacy includes the following subfactors:
  - *Anonymity* is the degree to which the users' identities are prevented from unauthorized storage or disclosure.
  - *Confidentiality* is the degree to which sensitive information is not disclosed to unauthorized parties (e.g., individuals, programs, processes, devices, or other systems).
- *Prosecution* is the degree to which the system supports the prosecution of attackers.
- *Recovery* is the degree to which the system recovers after a successful attack.
- *Security auditing* is the degree to which security personnel are enabled to audit the status and use of security mechanisms by analyzing security-related events.
- *System adaptation* is the degree to which the system learns from attacks in order to adapt its security countermeasures to protect itself from similar attacks in the future.

IV. Security Model for Big Data

In this section we present our security model that captures the most appropriate security factors defined by Firesmith [18] but focused on big data and the challenges and initiatives presented for this new technology.

Of the most important security challenges found and described in section II, we analyze if there is any security factor defined by the Firesmith model that covers it so if this security factor is implemented on a big data environment, the challenge or possible solution can be carried out with the mechanisms and solutions proposed for assuring the fulfilment of this security factor. So for example, in the Table 1, one of the challenges is Encryption which is covered by the factors: Integrity and confidentiality, which is necessary the use of the encryption to implement this requirement. For the rest of security factors what cover some security challenges can be seen in Table 1.

TABLE I. SECURITY CHALLENGES IDENTIFIED BY SECURITY QUALITY FACTORS.

Security Challenges \ Security Quality Factors	Identification	Authentication	Authorization	Attack/harm detection	Availability protection	Integrity	Nonrepudiation	Physical protection	Anonymity	Confidentiality	Prosecution	Recovery	Security auditing	System adaptation
Authentication		X												
Access Control	X	X	X											
Encryption						X	X			X				
Audit and logging													X	
Confidentiality										X				
Integrity						X								
Discovery					X									
Secure processing					X	X				X				
Data access	X	X	X											
API security					X								X	
Monitoring and filtering													X	
Data management						X				X			X	

Taking into account the results of the table, we can see that some of the security factors do not cover some security challenges, and therefore, these factors are not considered in our security model. Therefore, our security model extracted of the security quality factors defined in [18] is shown in Fig. 2.

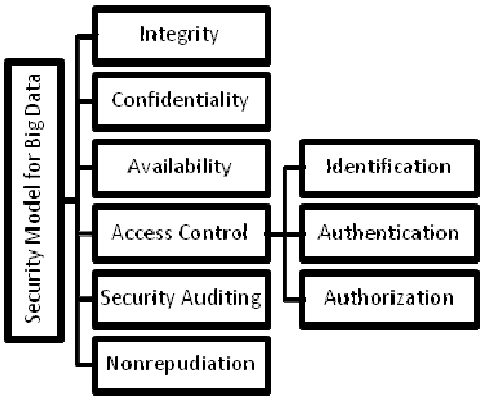

Figure 2. Security Model for Big Data proposed

This model defines the basic security requirements that we think most appropriate and interesting to consider in big data because cover the majority of challenges and needs found that should be solved in the next years. These factors of our model can be considered as security requirements to be taken into account in any big data environment and the implementation and functionality of each one depend of the system or datasets to protect, so as the security mechanisms and technologies to

be used to implement the security service that it is necessary to protect to the big data environment.

IV. CONCLUSIONS

Big data implies datasets having larger volumes, wider range of formats, and different velocities. Therefore, security in these environments has a higher importance than in traditional databases. In this paper we have defined a first security model where the majority of security factors that can be necessary in big data are identified. This security model will help us to define an information model where the security aspects are to be taken into account. This model could be used in the data provenance, related to ISO 8000-100 and to be used for exchanging of data with security indications and preprocessing of secure datasets.

AKNOWLEDGEMENT

This work is partially supported by R&D project SERENIDAD (PEII11-037-7035) funded by "Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla- La Mancha" (Spain), GEODAS (TIN2012-37493-C03-01) and SIGMA-CC (TIN2012-36904), funded by Ministry of Economy and Competitiveness and the Regional Development Fund, FEDER.

REFERENCIAS

[1] D. Laney, 3D Data Management: Controlling Data Volume, Velocity and Variety. . 2001, Stamford, CT: META Group.
[2] D. Nunan and M.D. Domenico, Market research and the ethics of big data. International Journal of Market Research, 2013. 55(4).
[3] MAP, Methodology for Information Systems Risk Analysis and Management. 2006.
[4] Cloud Security Alliance, Top Ten Big Data Security and Privacy Challenges. 2012.
[5] R.L. Villars, C.W. Olofson, and M. Eastwood, Big Data: What It Is and Why You Should Care. 2011, IDC.
[6] RENCI, Security and Privacy in the Era of Big Data. iRODS, a Technological Solution to the Challenge of Implementing Security and Privacy Policies and Procedures, 2013. 1.
[7] K.T. Smith (2013) Big Data Security: The Evolution of Hadoop's Security Model.
[8] S. Curry, E. Kirda, E. Schwartz, W.H. Stewart, and A. Yoran, Big Data Fuels Intelligence-Driven Security. 2013, RSA.
[9] Cloud Security Alliance, Comment on Big Data and the Future of Privacy. 2014.
[10] M. Kaushik and A. Jain, Challenges to Big Data Security and Privacy. International Journal of Computer Science and Information Technologies (IJCSIT), 2014. 5(3): p. 3042-3043.
[11] C. Tankard, Big data security. Network Security, 2012.
[12] A. Lane, Securing Big Data: Security Recommendations for Hadoop and NoSQL Environments. 2012.
[13] J. Markey. How to Manage Big Data's Big Security Challenges. 2013; Available from: http://data-informed.com/manage-big-datas-big-security-challenges/.
[14] M. Small, Securing bigdata: The challenges –malice, misuse and mistake. 2013, The British Computer Society.
[15] W.S. Al-Shorafat, Security in Software Engineering Requirement, in The 8th International Conference for Internet Technology and Secured Transactions. 2013.
[16] D.G. Firesmith. OPEN Process Framework Website. 2003; Available from: http://www.donald-firesmith.com.
[17] ISO/IEC 9126-2, Software Engineering - Product Quality - Part 2: External Metrics 2000.
[18] D.G. Firesmith, Common Concepts Underlying Safety, Security, and Survivability Engineering, in CMU/SEI-2003-TN-033. 2003.