Security and Privacy of Big Data for Social Networking Services in Cloud

Christos Stergiou
University of Macedonia
Department of Applied Informatics
Thessaloniki, Greece
c.stergiou@uom.edu.gr

Kostas E. Psannis
University of Macedonia
Department of Applied Informatics
Thessaloniki, Greece
kpsannis@uom.edu.gr

Theofanis Xifilidis
University of Macedonia
Department of Applied Informatics
Thessaloniki, Greece
thxifili@uom.edu.gr

Andreas P. Plageras
University of Macedonia
Department of Applied Informatics
Thessaloniki, Greece
a.plageras@uom.edu.gr

Brij B. Gupta
National Institute of Technology
Kurukshetra, India
bbgupta@nitkkr.ac.in

***Abstract*—Big Data (BD) is of great importance especially in wireless telecommunications field. Social Networking (SNg) is one more fast-growing technology that allows users to build their profile and could be described as web applications. Both of them face privacy and security issues. In this paper, we survey SNg, BD and Cloud Computing (CC) technology and their basic characteristics, by concentrating on the security issues of those technologies. Specifically, we aim at combining the functionality of these two technologies (i.e Big Data and Social Networking) in a CC environment, so that we can analyze the common features and ascertain the advantages of their integration related to security issues. Through this research, we present a new system-framework-network in Cloud Environment through which users of various Social Networks (SNs) will be able to exchange data and information, and primarily large-scale data (Big Data). With our proposed system, we can achive greatly improve of the communication of SN users, and thus become more safe and accurate in a Cloud environment. More specifically, this system could be established as an intermediate communication node that could be utilized in order to improve the security of SNg's users through the use of algorithms that can provide more privacy in the data related to BD technology. Also, in this work we present some measurements and results relative to our proposed system use. Finally, the opportunity to create a database through which each user can view the statistics of his interaction with the SNg is further discussed.**

Keywords— Cloud Computing, Big Data; Social Networking; Framework; System; Security; Privacy;

I. INTRODUCTION

Social Network is a structure consisting of sets of social, dyadic ties, and other social interactions between people. The SN perspective offers a set of methods for analyzing the structure of whole social entities as well as a variety of theories explaining the patterns observed in these structures [1]. SNs are "*self-organizing, emergent, and complex, such that a globally coherent pattern appears from the local interaction of the elements that comprise the system*" [2] (figure 1). Privacy concerns with SNg services is a subset of data privacy, involving the right of mandating personal privacy concerning storing, re-purposing, providing to third parties, and displaying of information connected with oneself through the Internet [3].

Fig. 1. Social Networks Society.

Cloud Computing constitutes a technology of internet services providing remote use of hardware and software. As a consequence, the users of CC could have access to information and data from any place at any time. In recent years, giant companies of the IT and software sectors investigate the services of CC. Furthermore, another technology which generated relaying on CC is "Mobile Cloud Computing" (MCC). MCC based on the concept of the "Cloud" provides any type of information and data by no matter of where and when through mobile devices. Through this relative technology the owners of the data on the internet could manage information everywhere and at any time. Also, MCC could make the mobile devices resourceful in terms such as computational power, memory, storage and energy. Considering this, MCC technology, and furthermore CC technology in general, could be settled as a base technology to operate other technologies such as BD and SNg [4] [5] [6].

A way in which the issues of data security and data privacy in SNs could be solved or could be depleted by the use of "Big Data Analysis Tools and Services". The big data describes the data sets that are large or complex for the traditional data processing applications which are incompetent. "Big Data is often related to the use of predictive analytics or a set of advanced methods (Big Data Analytics) with the aim to extract merit from the collected data" [7] [8]. From this scope it is perceptible that the big data are now equally important for both business and internet. This happens because more data packets demand a more accurate analysis. Data analysis is a do-or-die requirement for today's businesses. The vendor community is responding by providing highly distributed architectures and new levels of memory and processing power [9] [10] [11].

The rest of the paper is divided in sections as follows. Section 2 discusses in detail the technology of SNg and some of its basic characteristics about its security and privacy issues. Moreover, section 3 presents and analyzes the BD technology, and some basic information about its functionality. In Section 4, the proposed method of the paper is presented and some useful information related. Section 5, presents the proposed system-framework-network. Finally section 6 provides the conclusions of the current paper, and sets the issues of future work.

II. Security & Privacy for SNg

Social Networks can be described as web applications that permit users to create their semi-public profile [12] [13]. Most people join SNs to dispense their data and keep in contact with people that they are aware with. The main feature of SNs is a friend finder that allows SN users to search for people that they know and then build up their own online community [14].

Most SN users share a big amount of their private information in their social network space. A large number of users share their information publicly without careful consideration. Consenquently, SNs have become a large set of sensitive data. Moreover, SN users tend to have a high level of trust toward other SN users. They tend to accept friend requests easily, and trust items that friends send to them [15] [16].

Privacy and security issues on SNs are the most popular problems. The web-sites usually suffer from such problems. Meanwhile, security and privacy issues are entirely different problems. On the one hand, security issues occur when hackers gain unauthorized access to a site's protected coding or written language. On the other hand, privacy issues, those involving the unwarranted access of private information, do not necessarily have to involve security breaches. Confidential information such as typing a password can be revealed to anyone. But both types of breaches are often intertwined on SNs, especially "*since anyone who breaches a site's security network opens the door to easy access to private information belonging to any user*" [17] [18].

A. Social Networking Third-Party Output

Simple solutions are proposed for providing privacy when a SN uses third-party output. By these solutions personal data can be protected, but third party applications need direct access to the social graph information embodied in the user's friend list. More specifically, the solutions can be separated in three categories [18]: 1) Data Hiding, 2) User Identification, 3) Public Data.

III. Big Data

BD is a more complicated world because the scale is much larger. The information is usually shared over a number of servers, and the work of compiling the data must be correlated among them. In the past, the work was largely delegated to the database software, which would use its magical JOIN [19] mechanism to compile tables, then add up the columns before handing off the rectangle of data to the reporting software that would paginate it. Database programmers can inform the users about the procedure about complicated JOIN commands that would lock up their database for hours as it tried to produce a report for the boss who wanted his columns just so [19] [20] .

BD sets advanced analytic techniques in which they operate on, that called BD Analytics. Therefore, BD analytics is about two things, BD and analytics, plus how the two have teamed up to produce one of the most profound trends in business intelligence (BI) today. Analytics helps us discover what has changed and how we should react [21] [22].

A. BD Features

Most definitions of BD focus on the size of data in storage. Size matters, but there are other important attributes of BD, namely data variety and data velocity. The three Vs of BD, which are volume, variety, and velocity, constitute a broad definition, and they bust the myth that BD is only about data volume. More specifically, each one of these three Vs has its own ramifications for analytics [21].

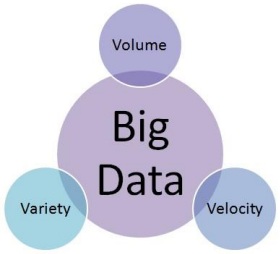

Fig. 2. The Three Vs of Big Data.

1) Big Data Volume

2) Big Data Velocity

3) Big Data Variety

B. BD Analysis Tools and Services

BD is the emerging discipline of capturing, storing, processing, analysing and visualising these huge quantities of information. The data sets may start at a few terabytes and run to many petabytes, far more than traditional data analysis packages can handle [23] [24].

Some BD tools that analyzed bellow are: 1) Jaspersoft BI Suite, 2) Pentaho Business Analytics, 3) Karmasphere Studio and Analyst, 4) Talend Open Studio, 5) Skytree Server, 6) Tableau Desktop and Server, 7) Splunk.

C. Big Data's impact in SNg

As the BD technology grows and spreads on the internet, many web technologies and applications that rely on it are

affected. One of the many applications which are affected by the growth of the BD technology is the SNg.

TABLE I.
Big Data's characteristics affect on Social Networking's third party output.

Big Data Characteristics	Big Data Volume	Big Data Velocity	Big Data Variety
Data Hiding	**X**	**X**	**X**
User Identification	**X**	**X**	
Public Data	**X**		**X**

Table 1 lists the characteristics that the BD technology has, regarding the convenience that this technology offers, and on the other hand lists three categories of the SNg third party output. The aim of the Table 1 is to show how the characteristics of the BD technology are related to the the three categories of Big SNg third party output, and additionally how they affect these three categories. The conclusion that can be drawn from Table 1 is that the BD Volume affects more in the SNg third party output. We reach to this conclusion relying to our study on Big Data technology, and in addition the findings and the conclusions of the related works, which we have studied.

TABLE II.
Social Networking's third party output categories affect on Big Data's Analysis Tools & Services.

Big Data Analysis Tools & Services	Data Hiding	User Identification	Public Data
Jaspersoft BI Suite		**X**	**X**
Pentaho Business Analytics	**X**		**X**
Karmasphere Studio and Analyst			**X**
Talend Open Studio		**X**	**X**
Skytree Server	**X**	**X**	**X**
Tableau Desktop and Server	**X**	**X**	
Splunk		**X**	**X**

Table 2 lists three categories of the SNg third party output and on the other hand lists the Big Data's Analysis Tools & Services that we have studied in this paper. The aim of Table 2 is to show how the three categories of the SNg third party output related and affect the Big Data's Analysis Tools & Services. As shown, Table 2 demonstrates that the Public Data category is related more with the Big Data's Analysis Tools & Services which we have studied here. Also, another conclusion that can be drawn from Table 2 is that the Skytree Server was affected more by the three categories of the SNg third party output.

D. BD Security Issues

New challenges and standards developed and created in data security issues through the development and the use of BD technology. This creates a growing need for further research on security technologies in order to make handling the huge amount of data feasible and to ensure effectiveness. Technologies for securing data are slow when applied to huge amounts of data [25].

TABLE III.
Encryption Rates of popular Algorithms.

Algorithm	Key length	MB processed	Block size	Rounds	Time Taken	MB per Second
Blowfish	32-448 bits	256	64 bits	16	3,976	64,386
DES	56 bits	128	64 bits	16	5,998	21,340
3DES	56, 112 or 168 bits	128	64 bits	48	6,159	20,783
AES	128, 192 or 256 bits	256	128 bits	10, 12 or 14	4,196	61,010
RSA	1024-4096 bits	300	512 bits	1	1175,7826	10,900

Regarding Table 3, the conclusion that even the most efficient algorithms give an encryption rate of 64.3MB/s is reached. So, in the sector of BD technology, in which the need of large amounts of data to be transferred, we can confirm a significant bottle neck for encryption such large amounts data. This is detrimental to the nature of BD which have real time processing and results.

IV. EVALUATION EXPERIMENTS

As the BD technology develops and engages with other technologies, established new requirements result relating to operation and needs. Thus there exists a causality of BD technology with an equally growing technology over the last years, which is the the Social Networking.

Having studied some encryption algorithms regarding security issues of BD technology we find that with regard to security issues involving BD technology in SNg technology, there are some issues which can be combined in a Cloud Environment. Selecting two of the encryption algorithms that were previously studied, we attempt to modify them so they can be use data from the algorithms we use in the SNg technology with the aim to realize some specific measurements of the data can be obtained, and why not do it in a safer way. The two algorithms are selected based on their potential to receive more data per second. The algorithms are the Blowfish (64,386MB/s) and the AES (61,010MB/s).

Regard the Blowfish algorithm we can take the NIter, which is the maximum number of iterations with the aim to use it in the encryption algorithm, and to improve the security of the four different bio-inspired algorithms.

void encrypt (NIter & L, NIter & R) {…}

void decrypt (NIter & L, NIter & R) {…}

Regarding the AES algorithm we can take the same value, the NIter, which is the maximum number of iterations in order to use it in the encryption algorithm, and to improve the security of the four different bio-inspired algorithms.

*int mbedtls_aes_crypt_ecb(NIter *ctx, int mode, const unsigned char input[16], unsigned char output[16]) {…}*

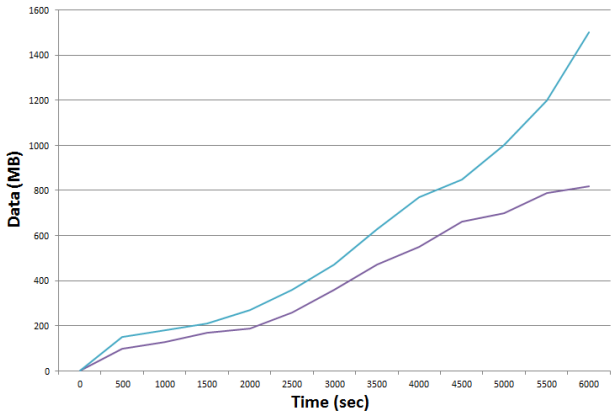

Fig. 3. Security level of encryption algorithms of measurement used for the study of four bio-inspired algorithms.

Figure 3 shows, the measurements with respect to time. As can be deduced by this figure the more often the combined use of the algorithms, the higher the level of security of the data we achieve every time. The upper line represents the Blowfish algorithm and the other (down line) represents the AES algorithm. More specific, Figure 3 could demonstrate a comparison of the implementation and the use of the two aforementioned encryption algorithms. The graph represents that through time the encryption procedure become more accurate and more efficient.

Regarding the Encryption Rate of the Transmitted Data the following equation is considered:

$$E_n R_a = \frac{\mathrm{R}_e D_{ata} - \left(T_r D_{ata} * NI_{ter}\right)}{T_r T_{ime}} \qquad (1)$$

where,

Acronym	Description
E_nR_a	Encryption Rate of Data
R_eD_{ata}	Received Data
T_rD_{ata}	Transmitted Data
NI_{ter}	Maximum number of iterations
T_rT_{ime}	Transmission Time of Data sent

By applying, so equation (1), the following chart occurs.

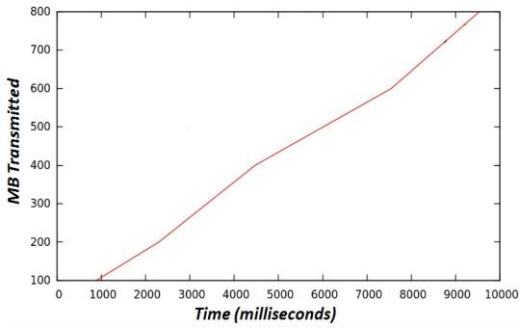

Fig. 4. Encryption Rate (*Data in Time*).

As we can observe from Figure 4, the encryption rate has an upward trend over time, in respect of data transmitted on the network. So, we can conclude that we need a good implementation of the encryption process mainly before sending the data, and then later in the transmission process.

Counting on the data packet switching procedures and use of the data on the internet, one needs to make a further study of additional technologies, such as Internet of Things (IoT), in order to see if combined we can achieve better results on data usage and security issues [26] [27].

V. Proposed System

Considering the study conducted for the related review, we can conclude that creating a system-framework-network in a "safe" Cloud environment through which users of the various Social Networks will be able to exchange data and information, and primarily large-scale data (Big Data), could greatly improve the communication of SN users.

In addition, having studied the available ways of security and authentication offered by social network providers, we reached that the system that we propose should work with authentication (sign in) through the account that will every user have in a SN (e.g. Facebook, LinkedIn YouTube, Instagram). In this way, each user will be able to connect to a more secure "private" network through which the user can exchange data in a "*Safe Cloud Server*" with other SN users, such as photos (mainly high quality) and videos (mostly high quality).

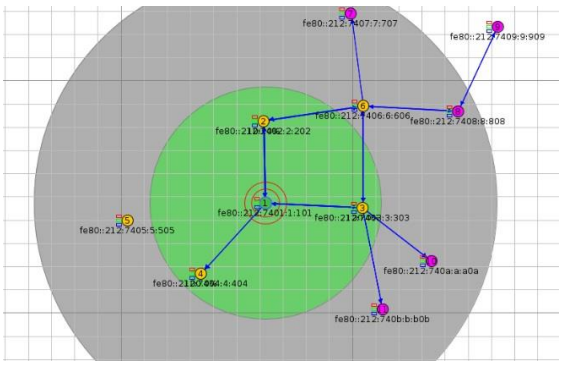

Fig. 5. Propoesd System's Topology.

Having concluded that many similar technologies in the telecommunications sector can be combined with each other from the earlier study we have done, the network we created will be based, in terms of design, architecture, topology, on IoT technology. This type of network that we propose could be count on previous work of C. Stergiou et al [28], where a new type of network topology have been proposed (figure 5) in order to transmit high quality videos. Also, users of this network will be able to exchange and other types of data such as personal files, which can be quite large. Users of the network will also be able to temporarily store data, as well as back up data, during the transmission process in a network space, based on CC technology. For multimedia data (Big Data) transfer within the network a protocol that has been proposed in a previous work of G. Kokkonis et al [29] will be used, the NAMRTP.

The proposed network system will use existing models of cryptographic algorithms to secure the authentication and data exchange process. Of course, there are some improvements - changes to some pieces of their source code, as we have seen in the previous section. The aim concerning the network will be to offer an alternative and more secure data exchange solution among users of SNs.

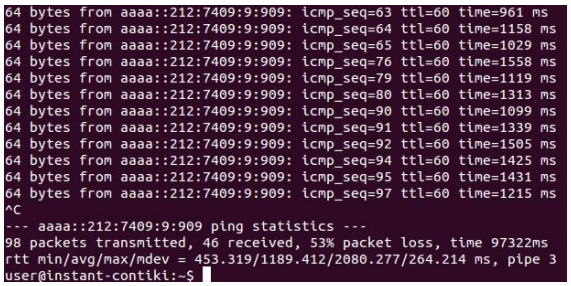

Fig. 6. Packets send through Network (sample node 9).

Figure 6 shows the transmission procedure of packets sent through the network. As easily observed, each file that ends through the proposed network is divided to smaller packets of data in order to be sent. Regarding the large amount of data sent we have a small number of *Packet Loss*. More specifically, the node 9 which is shown in figure 6 is the most distant node of the simulation network.

$$P_aL_o = \frac{\left(P_aT_r - P_aR_e\right) - D_uP_a}{T_rT_{ime}} \qquad (2)$$

$$\frac{P_aR_e}{T_rT_{ime}} = \frac{P_aT_r - P_aL_o - D_uP_a}{T_rT_{ime}} \qquad (3)$$

where,

Acronym	Description
P_aL_o	Packets Loss
P_aT_r	Packets Transmitted
P_aR_e	Packets Received
D_uP_a	Duplicated Packets
T_rT_{ime}	Transmission Time of Packets sent

The (2) shows the *Packet Loss* of the transmission procedure through the proposed network. The rate of the *Packet Loss* differs through time and depends by the various amount of data send each time. While, on the other hand, (3) shows how the *Packages Received* during the Transmission process (Time) depend, from the *Total Packets Transmitted*, removing the *Packet Loss* and the *Duplicated Packets*, and dividing them by the *Transmission Time*.

Fig. 7. Stuck overflow not detected.

Figure 7 demonstrates that there is no stuck overflow during the transmission procedure, so we can deduce that the whole process is smoothly carried out in the network.

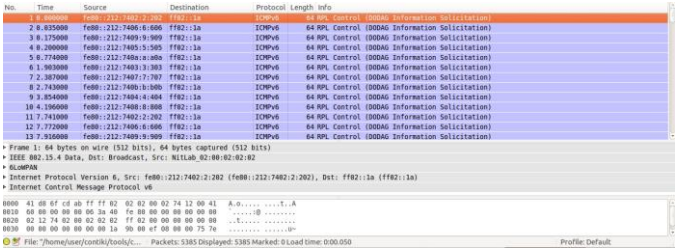

Fig. 8. Transmission proccess (a).

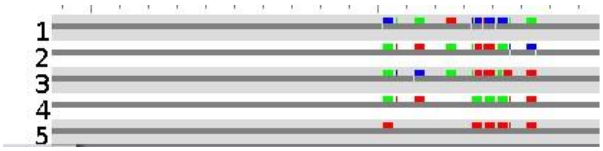

Fig. 9. Transmission proccess (b).

Figures 8 and 9 show the Transmission Packets procedure through the network. As observed, various types of packets were sent in the network by a number of connected users.

VI. CONCLUSIONS

SNg technology offers many possibilities, but also places several limitations as well. Social Networking could be described as web applications that allow users with the aim to create their semi-public profile. In the current work, we survey SNg, BD and Cloud Computing (CC) technology and their basic characteristics, with a focus on the security issues of those technologies. Additionally, we presented the basic characteristics of BD and SNg technologies, and also the major privacy and security issues that both technologies face. Subsequently and in terms of BD technology, we survey the algorithms with big impact to its security, and we present the basic characteristics of them.

Finally, we discuss the opportunity to create a database through which each user can see the statistics of his interaction with the SNg. The main goal of this paper is to try to combine the functionality of the BD and SNg technologies in a CC environment, in order to examine the common features, and also to discover the benefits related in security issues of their integration. Also, by examining their integration and functionality we could establish a new system-framework-network in Cloud Environment that combines these technologies, and some other technologies (e.g. IoT) related. This could be take place by presenting a new system-framework-network through which users of the various Social Networks will be able to exchange data and information, and primarily large-scale data (Big Data) and greatly improve the communication of SN users, and thus become more safe and accurate in a Cloud environment. Meanwhile, this system could be used for the purpose of improving security of SNg users through the use of algorithms that can provide more privacy in the data related to BD technology in a Cloud Server. This method is presented here and also some measurements results of its use.

This can be a field of future research on the integration of those technologies, and also have a huge improvement of their security and privacy issues. In addition, we can conclude that it would be a useful opportunity to create a database through which each user can see the statistics of his interaction with the SNg. Furthermore, based on the rapid development of network technologies the plethora of new technologies in this field, it would be good a further study to consider related technologies such as IoT, as a new case study.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and feedback which was extremely helpful in improving the quality of the paper.

REFERENCES

[1] S. Wasserman, K. Faust, “Social Network Analysis: Methods and Applications”, Urbana-Champaign: Cambridge University Press, pp. 1-27, March 1995.

[2] M. Newman, A.-L. Barabasi, D. J. Watts, “The Structure and Dynamics of Networks”, ACM, Princeton University Press Princeton, NJ, USA, 2006.

[3] C. Fabiana, M. Garetto, E. Leonardi, “De-anonymizing scale-free social networks by percolation graph matching”, in Proceedings of 2015 IEEE Conference on Computer Communications (INFOCOM), Kowloon, Hong Kong, 26 April-1 May 2015.

[4] C. Stergiou, K. E. Psannis, B.-G. Kim, B. Gupta, “Secure integration of IoT and Cloud Computing”, Elsevier, Future Generation Computer Systems, December 2016.

[5] S. Sakr, A. Liu, D. M. Batista, & M. Alomari, “A survey of large scale data management approaches in cloud environments”, IEEE Commun. Surveys & Tutorials, vol. 13, no. 3, pp. 311–336, 2011.

[6] C. Stergiou, K. E. Psannis, "Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: a survey", Wiley Online Library, International Journal of Network Management, vol. 27, issue 3, pp. 1-12, May 2016.

[7] M. Hilbert, P. Lopez, "The World’s Technological Capacity to Store, Communicate, and Compute Information", Science, vol. 332, issue: 6025, pp. 60-65, April 2011.

[8] Z. Fu, K. Ren, J. Shu, X. Sun, F. Huang, "Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement", IEEE Transactions on Parallel and Distributed Systems, vol. 27, issue: 9, September 2016.

[9] W. Culhane, K. Kogan, C. Jayalath, P. Eugster, “Optimal communication structures for big data aggregation”, in Proceedings of 2015 IEEE Conference on Computer Communications (INFOCOM) , Kowloon, Hong Kong, 26 April-1 May 2015.

[10] A. Detsounis, G. S. Paraschos, I. Koutsopoulos, “Streaming big data meets backpressure in distributed network computation”, Computer Communications, in Proceedings of 35th Annual IEEE International Conference on IEEE INFOCOM 2016, San Francisco, CA, USA, 10-14 April 2016.

[11] Z. Su, Q. Xu, Q. Qi, “Big Data in Mobile Social Networks: A Qof-Oriented Framework”, IEEE Network, February 2016.

[12] T. Ma, J. Zhou, M. Tang, S. Lee, "Social network and tag sources based augmenting collaborative recommender system", IEICE Transactions on Information and Systems, vol. E98-D, no.4, pp. 902-910, April 2015.

[13] L. Bilge, T. Strufe, D. Balzarotti, E. Kirda, "All your contacts are belong to us: automated identity theft attacks on social networks", in Proceedings of the 18th international conference on World Wide Web WWW '09, pp. 551-560, Madrid, Spain. 20-2 April 2009.

[14] J. L. Z. Cai, M. Yan, Y. Li., “Using crowdsourced data in location-based social networks to explore influence maximization”, in Proceedings of the 35th Annual IEEE International Conference on Computer Communications IEEE INFOCOM 2016, San Francisco, CA, USA , 10-14 April 2016.

[15] P. Chaudhary, B. B. Gupta, S. Gupta, "Auditing Defense against XSS Worms in Online Social Network-Based Web Applications," Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, IGI-Global's Advances in Information Security, Privacy, and Ethics (AISPE) series, USA, 2016.

[16] J. Cheng, Y. Zhang, Q. Ye, H. Du, “High-precision shortest distance estimation for large-scale social networks”, in Proceedings of the 35th Annual IEEE International Conference on Computer Communications, IEEE INFOCOM 2016, San Francisco, CA, USA, 10-14 April 2016.

[17] D. Gunatilaka, "A Survey of Privacy and Security Issues in Social Networks," CSE571S: Network Security, pp. 1-12, November 2011.

[18] L.Yan, H. Shen, K. Chen, “TSearch: Target-oriented low-delay node searching in DTNs with social network properties”, in Proceedings of 2015 IEEE Conference on Computer Communications (INFOCOM) , Kowloon, Hong Kong, 26 April-1 May 2015.

[19] P. Wayner, "7 top tools for taming big data," InfoWorld, 18/4/2012. [Online]. Available: http://www.infoworld.com/article/2616959/big-data/7-top-tools-for-taming-big-data.html. [Accessed 21/5/2016].

[20] A. P. Plageras, C. Stergiou, G. Kokkonis, K. E. Psannis, Y. Ishibashi, B.-G. Kim, B. B. Gupta, “Efficient Large-scale Medical Data (eHealth Big Data) Analytics in Internet of Things”, in Proceedings of 2017 IEEE 19th Conference on Business Informatics (CBI), International Workshop on Internet of Things and Smart, Thessaloniki, Greece, 24-26 July, 2017.

[21] Cloud News Daily, "Guide to Big Data Analytics: Platforms, Software, Companies Tools, Solutions and Hadoop," Cloud News Daily, 12/12/2015. [Online]. Available: http://cloudnewsdaily.com/big-data-analytics/. [Accessed 21/5/2016].

[22] K. Zheng, Z. Yang, K. Zhang, P. Chatzimisios, K. Yang, W. Xiang, “Big Data-Driven Optimization for Mobile Networks toward 5G”, IEEE Network, February 2016.

[23] S. Kaisler, F. Armour, J. A. Espinosa, W. Money, “Big Data: Issues and Challenges Moving Forward”, in Proceedings of 2013 46th Hawaii International Conference on System Sciences (HICSS), pp. 995-1004, Wailea, Maui, HI, USA, 7-10 January 2013.

[24] K. Raichura, N. Padhariya, “BigCache: a cache-based Big Data management in mobile networks”, International Journal in Mobile Communications, vol. 15, no. 1, pp. 49-68, 2017.

[25] C. Stergiou, K. E. Psannis, “Algorithms for Big Data in Advanced Communication Systems and Cloud Computing”, in Proceedings of 2017 IEEE 19th Conference on Business Informatics (CBI 2017), Thessaloniki, Greece, 24-26 July 2017.

[26] C. Stergiou, K. E. Psannis, “Efficient and Secure Big Data delivery in Cloud Computing”, Springer, Multimedia Tools and Applications, vol. 76, issue 21, pp. 22803–22822, November 2017.

[27] K. Yang, X. Jia, K. Ren, R. Xie, L. Huang, “Enabling efficient access control with dynamic policy updating for big data in the cloud”, in Proceedings of 2014 IEEE INFOCOM, Toronto, ON, Canada, 27 April-2 May 2014.

[28] C. Stergiou, K. E. Psannis, A. P. Plageras, Y. Ishibashi, B. B. Gupta, B.-G. Kim, “Architecture for security monitoring in IoT environments”, in Proceedings of 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), Edinburgh, Scotland (UK), 19-21 June 2017.

[29] G. Kokkonis, K. E. Psannis, M. Roumeliotis, D. Schonfeld, “Real-time wireless multisensory smart surveillance with 3D-HEVC streams for internet-of-things (IoT)”, Springer, Journal of Supercomputing, vol. 73, issue: 3, pp. 1044-1062, March 2017.