International Journal of Engineering & Technology, 7 (4) (2018) 3936-3940

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet. v7i4.20600
Research paper

Big data in cloud computing and the related security issues

Bajes Zeyad Aljunaedi [1] *, Mohammad Bani Younes [1]

[1] *faculty of information and technology, Ajloun National University, Jordan*

Abstract

This paper discusses the security issues associated with cloud computing environment. Additionally, big data, Map Reduce and Hadoop environment have also been catered through this research. The use of big data applications is rising over time because of the benefits of managing massive amount of data easily. Both small scale and large scale organizations use the big data application. Furthermore, the solutions of the problems of cloud computing have been discussed along with Hadoop. This security is developing rapidly and it includes security of the information, computer security, security of the network, and data privacy. The use of cloud computing is evident in policies, technologies, controls, and big data tools that are being used currently. The technology of Cloud computing, big data and its applications are going to form the future of science.

Keywords: *Big Data; Security; Cloud Computing; Hadoop Component; Challenges.*

1. Introduction

The security of data is important for analysing the complex data patterns but Cloud is associated with immense security challenge. This includes the control issue i.e. the owner of the data is not able to control the space where the data is placed or in other words lack of control availability to manage the data. The controls of space provide the benefits of cloud computing by allocating and scheduling resources according to their will and the user is expected to abide by them. [1] This is why the lack of trustworthiness involved in the process of cloud computing requires protection. As the high complexity is involved in the situation, so it is ideal to enhance the security of the cloud to get an ultimate secure cloud [2].
Google has introduced Map Reduce for processing large amounts of data [1], which is provides an important framework in the cloud environment. At the same time, Apache's Hadoop distributed file system (HDFS) is becoming one of the prominent software for cloud computing. The open-source implementation of Google Map Reduce is provided by it, so that the programmer of the application can get the abstraction of the map. Using Hadoop makes it easier for the organizations to manage large volumes of data easily [3]. However, it can create data security problems, problems with data access, monitoring of data and problems in continuing business.
The purpose of this paper is to discuss the approaches for the provision of security and the development of a system that can handle multiple sites and process large data inputs. The current systems using HDFS and Map Reduce do not serve the purpose as they lack the security element for protecting sensitive data [4]. The combination of technologies like k-means and data mining with Hadoop framework can help in solving data and managing complex problems easily [3].

1.1. Big data

Big Data is defined as the handler of large amounts of structured and unstructured data, which is difficult to process through traditional means that were previously employed. The "Big Data [5]" can be used by the companies where the data is loosely structured but it is present in massive amounts. Following three are the main properties of Big Data:

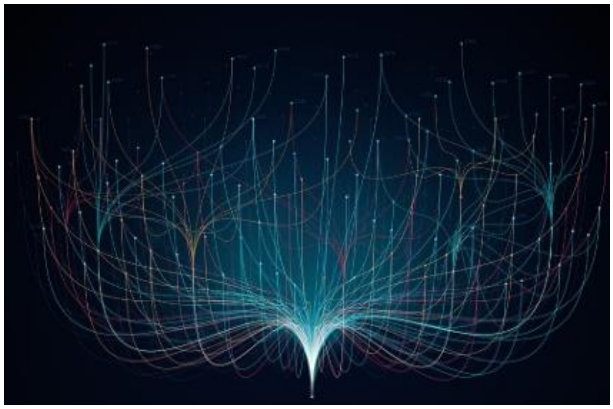


Fig. 1: Big Data Workflow.

a) Volume: The increase in volume is one of the essential features of big data.
b) Variety: Handling variety of formats of data including emails, video, audio, transactions etc. is another characteristic of big data
c) Velocity: the processing speed relative to the demand of data needed is known as velocity Variability and complexity have been chosen as the other two dimensions of Big Data
d) Variability: d-peaks of data along with velocity is known as variability
e) Complexity: The involvement of data from multiple sources is handled by BIG data. It helps in linking, coordinating and integrating the data from a number of sources.

The technologies of the modern world are capable of not only collecting data but also utilization of data is also possible today [5]. Bank is one of the prominent applications of Big Data where the

data is collected and managed for making effective decisions. Additionally, Wal-Mart customer transactions, and Facebook are some of the other examples of usage of Big Data in the practical field. [6] BIG data is closely associated with Hadoop thus it has to be discussed while discussing Big Data "Hadoop" is originated from the Web search Volume [7]. Credit cards are the best example of showing the importance of Hadoop in Big Data.

1.2. Hadoop

Hadoop is a Java-based programming framework - which is available without cost - that helps in processing massive amounts of data in the digital environment. It is sponsored by the Apache Software Foundation. Master/Slave structure is used by Hadoop for its functioning [8]. Hadoop can help in processing large sets of data over a number of servers and the applications of big data can be run with thousands of
Nodes that manage the data of thousands of terabytes through Hadoop. The Distributed file system is responsible for massive file transfers, which allows normal functioning of operations even with the failure of nodes. Such an approach reduces the risk of the failure of entire system. It provides the solution, which is cost effective and scalable thus liked by the businesses and individuals [9]. Furthermore, its flexible and fault tolerant nature is another reason of its success. Google, Yahoo, Amazon, IBM etc., are the companies that use Hadoop to manage huge amounts of data available with these companies. There are two main sub-projects of Hadoop [10]. These include Map Reduce and Hadoop Distributed File System (HDFS).

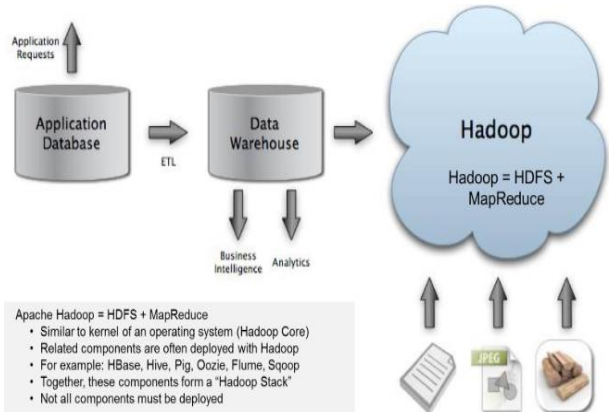


Fig. 2: Hadoop Component.

1.3. Map reduce

Hadoop Map Reduce is a framework [7] that is responsible for writing applications, which could process enormous amount of data on clusters without any faults, thus making it reliable. Map Reduce job splits the available data into smaller pieces, which are then processed parallel. The outputs of the processing process are then used as the input, which reduces the overall tasks. In most of the cases, both the input data and output data are stored in a file-system. Any problem in the tasks performed by Map Reduce includes the problems in Scheduling [11]. The monitoring and re-executing are managed by the framework in an autonomous way.

1.4. Hadoop distributed file system (HDFS)

HDFS [8] is a distributed file system that consists of nodes used for storing the data. It integrates the local nodes to make one larger file, which helps in the improvement of reliability and uses the feature of reliability to fix the failures in the system [12].

1.5. Big data applications

The distributed applications, which require large data process, are known as Big Data Application. Handling this enormous amount of data is often an issue in many sectors. The traditional data processing could not manage the computation easily, thus giving rise to big data applications [13] The defacto software to be used with Big Data are Google's map reduce framework and Apache Hadoop [14]. These software manage the large amount of data that is generated as intermediate data through these applications.
The two big areas of big data applications are Manufacturing and Bioinformatics [15].
The use of big data helps in creating transparency in manufacturing industry as the uncertainties arising because of inconsistent component performance can be managed.
The acquisition of data is in predictive manufacturing is the first step in the process [16]. Various forms of sensory data such as pressure, current, vibration, controller data, acoustics, and voltage are the different forms of data that are collected to be used. Both the sensory data and historical data form the big data in manufacturing organizations. This big data is used as an input to find the precautionary strategies such as prognostics and health management [17].
Bioinformatics is another application of big data. Sequencing and other biological domains are covered in it. Bioinformatics is in need of large scale data analysis, which is easily handled through Hadoop [1].

1.6. Advantages of big data

The software package in big data provides a number of tools, which can help an individual to map the data of an organization very easily, making it easier for them to analyse the internal threats being faced. The safety that the Big Data provides is one of the major benefits associated with this technique [3]. The individuals can detect the sensitive information through Big Data and ensure the protection of the unprotected data in an appropriate manner while keeping in account the regulatory requirements. Some of the common characteristics of big data include:

1) Structured and unstructured data both can be covered through big data.
2) Speed and scalability, mobility and security, flexibility and stability are easily managed through big data
3) The time to get information is critical for attracting data from different sources. It is known as realization time. These data sources include mobile devices, web, radio frequency identification (RFID), and other sensory technologies that have gained importance in the market over time.

The businesses can gain value from the speed and capacity that it provides. Additionally, the scalability of cloud and the visualization of data can also be helpful for the business for the identification of newer opportunities. Furthermore, the facility of data analysis can help in personalization of the content so that more
customers can be attracted and retained to the website [1]. The combination of big data with predictive analytics, following four areas can be explored: a. Calculation of the risk of enormous data portfolios, b. Detection, and prevention of financial fraud, c. Improvement in criminal database and d. the execution of high marketing and advertising campaigns

1.7. Security importance in big data

Many organization use big data but the security perspective is not well managed by them. However, if any breach of data occurs in any organization, it can lead to legal problems and loss of reputation of the firms. Moreover [18], the excessive data about the company and customers stored and analysed through technology, makes the classification of information more important. Some of the techniques that can be used for the security of data are encryption [19], logging, and honeypot detection. The use of big data can also be used for detecting frauds. Even the advanced threats of malicious intruders and hackers can be managed easily through Big data style analysis. As through the utilization of these techniques, the threats can be detected at an earlier stage. Even privacy of the company and its information can be managed easily through big data. Usu-

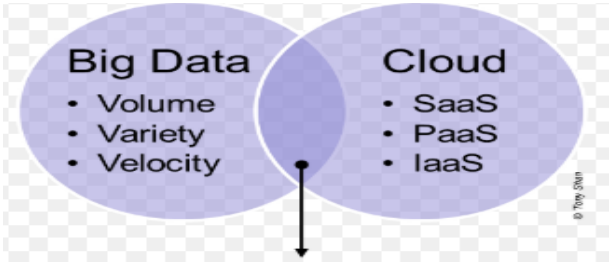
ally, the privacy of data is taken as the liability requiring the companies to act defensive on it. However, with the new technology the privacy of data can also be treated as an asset that provides a competitive advantage to the company [20]. Overall, balance between data privacy and national security must be maintained.

2. Related work

Hadoop is a Java based distributed system, which is currently nascent in the market. It is trying to provide more features and giving high importance to the security element. Some of the notable steps that have been found in this regard are discussed below.
SPARQL has been identified as important tool in diverse data sources by WWW Consortium. Later, the privacy was increased to reduce the privacy utility trade-off being faced by the users. Jelena (from USC Information Science Institute) discussed that the enquiries and probes of the searcher can be managed according to the privacy policy of the searcher that has been set. Similarly, a paper on access control published by Bertino et al highlights that cryptography and digital signature technique can manage the access to XML data document. Another paper on third party XML document distribution [13] published by Bertino, highlighted the presence of another layer of security to enhance the trust for the paradigm. Hamlen et al reiterated individuals can store encrypted data instead of plain data, which can create security issues. One of the benefits of using this technique for storing data is that even in case the storage space is hacked, the data remains safe. This is possible through the storage of data in cryptographic form, thus adding a security layer. IBM researchers have explained the importance of secured query processing as well.
For which Kerberos has been highly effective. It is an authentication system developed by MIT. It is based on an encryption technology that involves an arbitrator, who manages an authentication to open a particular network. In other words, it uses cryptographic tickets so that the text passwords cannot be overwritten. It is based on Needham-Schroeder protocol. Significant advancement in security has been shown by Airavat [14]. Another research work of Roy et al has discussed the differential privacy. The mathematical bound potential privacy violation has been used in this paper [15]. This technology reduces the risk of information leakage. Based on these literature articles, in this research, the different approaches for making the cloud environment secure for transferring data and computation are to be explored.

3. Issues and challenges

The cloud computing involves a number of security issues as it engages with a number of networks, databases, operating systems, virtualization, scheduling the resources, transaction management, balancing the load, concurrency control and management of memory. Thus, the issue related to all these fields can be faced by cloud computing. As an example, it is necessary that the environment that interconnects the systems in a cloud is completely secure. However, at the same time, virtualization paradigm in cloud computing creates a number of security concerns. Particularly, mapping of the virtual machines to the physical machines has to be secure [21].
The issues in data security are not limited to data encryption. They also involve the appropriateness of data sharing policy. Furthermore, memory management and allocation of resources has to be secured. [22]
Some of the industries are more prone to data issues. These include telecoms, financial services and retail sector, marketing and advertisement on web, and government activities. In these industries, the presence of excess data is going to be difficult to handle. The companies, which will manage this data, will be on considerable advantage whereas the ones, which will not manage this data, will face clear disadvantage in the future [2].
Another aspect that has been discussed is the data mining techniques. These techniques can be used for the finding malware in the system. Categorization of challenges can be made to analyse these in a better way. The categorization includes network level, user authentication level, data level, and generic issues.



	Volume	Variety	Velocity
SaaS	Semantics	Visualization	Real-time
PaaS	Distributed processing	Schemaless	Integration on the fly
IaaS	Scalable storage	Federated store	On-demand resources

Fig. 3: Big Data and Cloud Comparison Techniques.

Network level:
The challenges dealing with network protocols, and distributed data, Internode communication are covered in the network level.
Authentication level:
The authentication level challenges deal with encryption/decryption techniques, and authentication methods
Data level:
The issues involved with data integrity and availability such including data protection and distributed data are included in the data level.
Generic types:
Generic type challenges are the challenges that deal with traditional tools for the security and utilization of different technologies

3.1. Distributed nodes

These refer to [15] an architectural issue where computation can be performed in any of the set of nodes. The data with necessary resources is processed in the nodes. As it can be applicable in different locations, the exact location is difficult to find out. It makes the security of computation difficult to maintain.

3.2. Distributed data

The parallel computation of data requires the storage of information in pieces. Additionally, the multiple copies are used in case for maintain the reliability of the data. Even if something is corrupted, the presence of multiple files helps in getting the data. However, in the cloud setting, finding the exact location of the file becomes difficult. These pieces of data can move from one machine to the other based on availability of space and maintenance operations that are carried out by the system. So in centralized data security system, data is wrapped in various security tools [23], providing immense security. It cannot be applied in the case of cloud computing because of changing data environments [24]

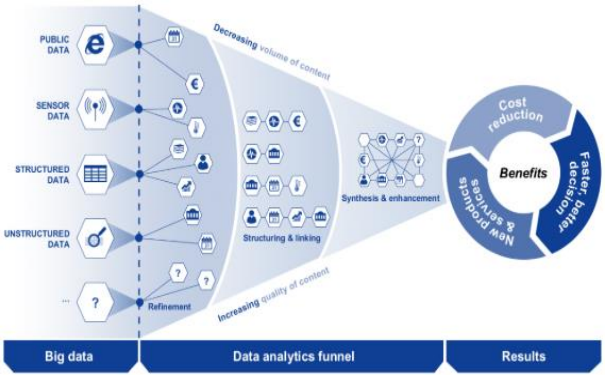


Fig. 4: Big Data Benefits.

3.3. Internode communication

Most of the Hadoop distributions make use of RPC rather than TCP/IP to transfer data between different nodes. Both wired and wireless communication system are involved in making it easier to hack the system [15]

3.4. Data protection

Without encryption, data is stored in cloud environment such as Hadoop in order to improve efficiency. Getting an access to machine by an intruder can result in hacking of the entire data without having any control.

3.5. Administrative rights for nodes

Nodes can access all the data because of the administrative controls available to it [15]. Because of this easy access the data can be easy stolen.

3.6. Authentication of applications and nodes

The parallel operations can be improved through joining of node clusters. This is a problem because any third party can join the system to take away the important data.

3.7. Logging

The lack of logging facility in cloud environment results in lack of recording of data regarding modification and deletion of data. Additionally, the information with joined clusters is also not stored. The lack of these logs of the maintenance of data, there are problems in identifying the problems that could have been created unintentionally. Internal staff can also do malicious activities without being trapped.

3.8. Traditional security tools

The traditional security tools used with traditional networks were important previously when the scope of data was not this broad. Now with the massive data availability, these security tools cannot be applied in the big data.

3.9. Use of different technologies

A number of technologies are included in the cloud environment. Cloud consists of various technologies, which includes interaction between complex components of the system. Database, computing power, network, and much other stuff are some of the different technologies that a cloud is composed of. As a result of this wide technology, a small problem can lead to breaking down of the whole system.

3.10. Nodes authentication

Every time, a node joins a cluster it has to be authenticated. The malicious nodes should not be allowed to join. Kerberos is one of the authentication techniques that can be used to validate the authorized nodes, making the system perform better.

3.11. Rigorous system testing of map reduce jobs

After writing map reduce job a through test must be performed on it. In distributed environment to ensure that the, machine is working properly.

3.12. Honeypot nodes

These nodes should be present in a cluster. These nodes show them to be regular nodes but in reality it is a trap, which finds the hackers and actions, are taken to eliminate the hackers from the system.

3.13. Layered framework for assuring cloud

Secure virtual machine layer, secure cloud data layer, secure layer of cloud storage and virtual network monitor security layer shows the layered framework. Cross cutting services are managed by the security layer policy under consideration, the cloud monitoring layer, the reliability layer and the risk analysis layer [25], [16].

3.14. Third party secure data publication to cloud

The use of cloud computing can be helpful even in storing data from a remote size to ensure resource utilization. So, the data has to be protected in the best way and the access to these locations must be given to authorized individuals. This requires the protection of third party functioning as well. Machines can be treated as third party publishers in cloud computing. [1], [9], [26] Therefore, the third party technique mentioned above can be applied to secure the data [27], [16].

3.15. Access control

One of the efficient security measures that can be taken by the developers in a distributed environment is the collaboration of mandatory access control and differential privacy. The security of sensitive data will be stored by the providers of data. The mathematical bounds for ensuring the security would also be managed by these providers. Such a practice can help in transferring data without any leakage. To avoid the leak of information from the system, SELinux [17] will be used [26]. SELinux is the feature that provides supporting control to the security policy by using Linux Security Modules (LSM) in the Linux Kernel. The enforcement of differential security procedure will require Java Virtual Machine and the Map Reduce framework. Such a framework will have inbuilt application to store the identity pool. Furthermore, third party will support the authentication. This mechanism will be trusted by all the stakeholders [10] [19] [28]. The use of third party authentication will provide an additional layer of security for the whole system. In a cloud environment, real time access control will be responsible for additional security. Furthermore, operational control within a database in the cloud can be utilized by the system to prevent the malfunctioning. Factors like IP address, time of the day, and authentication method are important in this regard. As an example, the access of the system can be made limit to middle tier only [25]. This is because maintain separate identities for security administrator separate and database administrator will ensure better results. The label security method will be used to ensure the protection of sensitive data. The data can be categorized as public, confidential and sensitive based on the label security. On matching the user label with label data, the system can provide access. Numerous data breaches show that using auditing technique could have helped in avoiding problems involved with data security [29] [30].

Big data and healthcare:

The application of big data analytics in healthcare has a lot of positive besides also life-saving outcomes [31], [32] [33] [34]. Big data refers to the huge quantities of information created by the digitization of everything that gets associated and analysed by specific technologies

4. Conclusion

The use of cloud environment is prominent in academic and practical world. Security is essential for all the aspects of cloud environment. With the new technology the privacy of data can also be treated as an asset that provides a competitive advantage to the company. Overall, balance between data privacy and national security must be maintained the utilization of the approaches that have been proposed above, the complex business environments can be protected easily.

5. Funding

The Deanship of Research and Graduate Studies in Ajloun National University Ajloun, 26810, Jordan, fund this research

References

[1] J. W. Lichtman, H. Pfister, N. Shavit, C. Biology, and C. Science, "The big data challenges of connectomics," vol. 17, no. 11, pp. 1448–1454, 2015.

[2] A. Katal, M. Wazid, and R. H. Goudar, "Big data: Issues, challenges, tools and Good practices," 2013 sixth Int. Conf. Contemp. Comput. IC3 2013, pp. 404–409, 2013.

[3] C. L. Philip Chen and C. Y. Zhang, "Data-intensive applications, challenges, techniques and technologies: A survey on Big Data," Inf. Sci. (Ny). vol. 275, pp. 314–347, 2014. https://doi.org/10.1016/j.ins.2014.01.015.

[4] M. Batty, "Big data, smart cities and city planning," Dialogues Hum. Geogr, vol. 3, no. 3, pp. 274–279, 2013. https://doi.org/10.1177/2043820613513390.

[5] A. A. Tole, "Big Data Challenges," Database Syst. J. vol., vol. IV, no. 3, pp. 31–40, 2013.

[6] J. Singh, "Big Data: Tools and Technologies in Big Data," Int. J. Comput. Appl., vol. 112, no. 15, pp. 975–8887, 2015.

[7] D. Che, M. Safran, and Z. Peng, "From Big Data to Big Data Mining : Challenges, Issues, and Opportunities," 18th Int. Conf. DASFAA, pp. 1–15, 2013. https://doi.org/10.1007/978-3-642-40270-8_1.

[8] H. R. Varian, "Big Data: New Tricks for Econometrics," J. Econ. Perspect., vol. 28, no. 2, pp. 3–28, 2014. https://doi.org/10.1257/jep.28.2.3.

[9] R. Kitchin, "The real-time city? Big data and smart urbanism," GeoJournal, vol. 79, no. 1, pp. 1–14, 2014. https://doi.org/10.1007/s10708-013-9516-8.

[10] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. Ullah Khan, "The rise of 'big data' on cloud computing: Review and open research issues," Inf. Syst., vol. 47, pp. 98–115, 2015. https://doi.org/10.1016/j.is.2014.07.006.

[11] A. B. Wei Fan, "Mining big data: current status, and forecast to the future," ACM SIGKDD Explor. Newsl, vol. 14, no. 2, pp. 1–5, 2012. https://doi.org/10.1145/2481244.2481246.

[12] G.-H. Kim, S. Trimi, and J.-H. Chung, "Big-data applications in the government sector," Commun. ACM, vol. 57, no. 3, pp. 78–85, 2014. https://doi.org/10.1145/2500873.

[13] O. Tene and J. Polonetsky, Big data for all: Privacy and user control in the age of analytics, vol. 11, and no. 5. 2013.

[14] H. V Jagadish, J. Gehrke, A. Labrinidis, Y. Papakonstantinou, J. M. Patel, R. Ramakrishnan, and C. Shahabi, "Big Data and Its Technical Challenges," Assoc. Comput. Mach. Commun. ACM, vol. 57, no. 7, p. 86, 2014. https://doi.org/10.1145/2611567.

[15] H. Hu, Y. Wen, T. S. Chua, and X. Li, "Toward scalable systems for big data analytics: A technology tutorial," IEEE Access, vol. 2, pp. 652–687, 2014. https://doi.org/10.1109/ACCESS.2014.2332453.

[16] S. Kaisler, F. Armour, J. A. Espinosa, and W. Money, "Big Data: Issues and Challenges Moving Forward," 2013 46th Hawaii Int. Conf. Syst. Sci., pp. 995–1004, 2013. https://doi.org/10.1109/HICSS.2013.645.

[17] F. Provost and T. Fawcett, "Data Science and its Relationship to Big Data and Data-Driven Decision Making," Big Data, vol. 1, no. 1, pp. 51–59, 2013. https://doi.org/10.1089/big.2013.1508.

[18] V. Inukollu, S. Arsi, and S. Ravuri, "Security Issues Associated With Big Data in Cloud Computing," Int. J. Netw. Secur. It is Appl., vol. 6, no. 3, pp. 45–56, 2014.

[19] I. Brief, "Healthcare Cloud Security Healthcare Cloud Security," no. January 2013.

[20] S. Möller, N. Ben-Asher, K.-P. Engelbrecht, R. Englert, and J. Meyer, "Modeling the behavior of users who are confronted with security mechanisms," Comput. Secur. vol. 30, no. 4, pp. 242–256, Jun. 2011. https://doi.org/10.1016/j.cose.2011.01.001.

[21] M. Doheir, B. Hussin, A. Samad, H. Basari, and M. B. Alazzam, "Structural Design of Secure Transmission Module for Protecting Patient Data in Cloud-Based Healthcare Environment," Middle-East J. Sci. Res., vol. 23, no. 12, pp. 2961–2967, 2015.

[22] A Zanella, N. Bui, a Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," IEEE Internet Things J., vol. 1, no. 1, pp. 22–32, 2014. https://doi.org/10.1109/JIOT.2014.2306328.

[23] K. Kambatla, G. Kollias, V. Kumar, and A. Grama, "Trends in big data analytics," J. Parallel Distrib. Comput. vol. 74, no. 7, pp. 2561–2573, 2014. https://doi.org/10.1016/j.jpdc.2014.01.003.

[24] M. J. Khoury, J. P. A. Ioannidis, P. Alto, and J. Snow, "HHS Public Access," vol. 346, no. 6213, pp. 1054–1055, 2015.

[25] M. B. Alazzam, Y. M. Al-sharo, and M. K. Al-, "DEVELOPING (UTAUT 2) MODEL OF ADOPTION MOBILE HEALTH APPLICATION IN JORDAN E- GOVERNMENT," vol. 96, no. 12, 2018.

[26] G. Garrison, C. M. Rebman, and S. H. Kim, "An identification of factors motivating individuals' use of cloud-based services," J. Comput. Inf. Syst., vol. 58, no. 1, pp. 19–29, 2018. https://doi.org/10.1080/08874417.2016.1180653.

[27] M. R. Ramli, Z. A. Abas, M. I. Desa, Z. Z. Abidin, and M. B. Alazzam, "Enhanced convergence of Bat Algorithm based on dimensional and inertia weight factor," J. King Saud Univ. - Comput. Inf. Sci., 2018.

[28] T. Piliouras, V. K. a. Siddaramaiah, N. Sultana, E. Meyer, and R. Harrington, "Trust in a cloud-based healthcare environment," 2011 8th Int. Conf. Expo Emerg. Technol. a Smarter World, pp. 1–6, Nov. 2011.

[29] J. Matysiewicz and S. Smyczek, "Consumer Trust - Challenge for E-healthcare," 2009 Fourth Int. Conf. Coop. Promot. Inf. Resour. Sci. Technol., pp. 333–338, Nov. 2009. https://doi.org/10.1109/COINFO.2009.40.

[30] M. B. Alazzam, A. B. D. Samad, H. Basari, and A. Samad, "PILOT STUDY OF EHRS ACCEPTANCE IN JORDAN HOSPITALS BY UTAUT2," vol. 85, no. 3, 2016.

[31] S. M.Alazzam, BASARI, "EHRs Acceptance in Jordan Hospitals by UTAUT2 Model: Preliminary Result," J. Theor. Appl. Inf. Technol., vol. 3178, no. 3, pp. 473–482, 2015.

[32] A. Bahga and V. K. Madisetti, "A Cloud-based Approach for Interoperable Electronic Health Records (EHRs)," IEEE J. Biomed. Heal. Informatics, vol. 17, no. 5, pp. 894–906, Sep. 2013.

[33] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of Cloud computing and Internet of Things: A survey," Futur. Gener. Comput. Syst., vol. 56, pp. 684–700, 2016. https://doi.org/10.1016/j.future.2015.09.021.

[34] M. Warkentin, S. Sharma, D. Gefen, P. Pavlou, and G. Rose, "Government of the People, By the People: A Look at Trust in eGovernment," 18th Am. Conf. Inf. Syst. (AMCIS 2012), pp. 1–10, 2012.