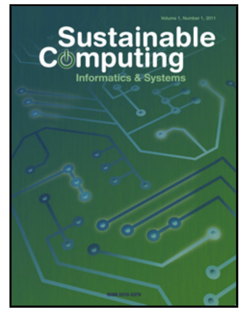
Accepted Manuscript



Title: Security, Privacy and Efficiency of Sustainable Cloud Computing for Big Data and IoT

Authors: Christos Stergiou, Kostas E. Psannis, Brij B. Gupta, Yutaka Ishibashi

PII:	S2210-5379(18)30049-0
DOI:	https://doi.org/10.1016/j.suscom.2018.06.003
Reference:	SUSCOM 255

To appear in:

Received date:	9-2-2018
Revised date:	23-5-2018
Accepted date:	14-6-2018

Please cite this article as: Stergiou C, Psannis KE, Gupta BB, Ishibashi Y, Security, Privacy and Efficiency of Sustainable Cloud Computing for Big Data and IoT<CHK-Error value=Ärticle Title is Mismatching from Order.̈/>, *Sustainable Computing: Informatics and Systems* (2018), https://doi.org/10.1016/j.suscom.2018.06.003

Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT

Christos Stergiou[1], Kostas E. Psannis[1,*], Brij B. Gupta[2], Yutaka Ishibashi[3]

[1]Department of Applied Informatics, School of Information Sciences, University of Macedonia, Thessaloniki, Greece
[2]National Institute of Technology Kurukshetra, India
[3]Department of Scientific and Engineering Simulation Nagoya, Japan

[*]Corresponding author: Kostas E. Psannis,
E-mail address: kpsannis@uom.edu.gr (K.E.Psannis).
URL: http://users.uom.gr/~kpsannis

Highlights

- Cloud Computing System integrated with IoT as a base scenario for Big Data.
- Establish an architecture relaying on the security of the network.
- Install security “wall” between the Server of Cloud Computing & the Internet.
- Cloud provides efficiency regarding privacy issue of bits transferred through time.

Abstract

With the significant advances in communication technologies and in many other sectors, also are growing up security and privacy issues. In our research, is introduced a base technology called Cloud Computing (CC) to operate with the Big Data (BD). CC is a technology which refers to the processing power of data in the fog, providing more “green” computational and sustainable computing. Since it is a recently investigated technology, it has many gaps in security and privacy. So, in this paper, we proposed a new system for Cloud Computing integrated with Internet of Things as a base scenario for Big Data. Moreover, we tried to establish an architecture relaying on the security of the network in order to improve the security issues. A solution proposed is installing a security “wall” between the Cloud Server and the Internet, with the aim to eliminate the privacy and security issues. As a result, we consider that CC deals more efficient with the privacy issue of bits transferred through time. Through our proposed system, the interaction and cooperation between things and objects communicate through the wireless networks in order to fulfil the objective set to them as a combined entity. Regarding the major goal of our research, which is the security, a sort survey of IoT and CC presented, with a focus on the security issues of both technologies. In addition to this, we try present the security challenges of the integration of IoT and Cloud Computing with the aim to provide an architecture relaying on the security of the network in order to improve their security issues. Finally, we realize that through our study Cloud Computing could offer a more “green” and efficient fog environment for sustainable computing scenarios.

***Keywords* – Efficiency, Cloud Computing, Big Data, Internet of Things, Topology, Security, Privacy.**

I. INTRODUCTION

The problem with security and privacy in everyday life could be solved or could be minimized by the use of Big Data (BD) analysis tools and services. Big Data is a new popular term, used to describe the surprisingly rapid increase in volume of data in structured and unstructured form [1]. Accuracy in big data may lead to more confident decisions making, and better decisions can result in greater operational efficiency, cost reduction, and reduced risk [2] [3]. BD usually uses Cloud Computing (CC) as a base technology in order to operate.

In addition to this, CC could be used as a base technology for another relative to communications technology, Internet of Things (IoT). The basic idea of the IoT is the diffuse presence of a variety of things or objects used by people such as radio-frequency identification tags, sensors, actuators, and mobile phones. Through unique addressing schemes, these things interact with each other and cooperate with other things near them in order to reach the common goals [4] [5]. The IoT can defined as “*the network of physical objects, devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity, permitting these objects to gather and interchange data*” regarding the bibliography [6] [7] [8]. Some examples include the restrictions of storage, communication capabilities, energy and processing offered to IoT devices. Those inefficiencies motivate us to combine the functionality of CC and IoT technologies [6] [9] [10].

IoT security is the area of strive concerned with safeguarding connected devices and networks in the IoT. The IoT involves the raising dominance of objects and entities, provided with unique identifiers and the ability to automatically transmit data over a network. Much of the increase in IoT communication comes from computing devices and the embedded sensor systems used in sectors such as industrial machine-to-machine (M2M) communication, smart energy grids, home and building automation, vehicle to vehicle communication and wearable computing devices [11] [12] [13] [14].

Furthermore, the new technology called Cloud Computing could be defined as "a distributed information technology (IT) architecture in which client data is processed at the periphery of the network, as close to the originating source as possible" [15] [16] [17]. The move toward Cloud Computing is driven by mobile computing, the decreasing cost of computer components and the absolute number of networked devices in the IoT. More specifically, CC refers to data processing power in a fog network instead of holding that processing power in a cloud or a central data warehouse [15] [18] [19] [20].

CC storage solutions offer users and enterprises with various capabilities to store and process their data in third-party data centers [16] [21] [22] [23] [24]. With the aim to offer safer communication over the network, encryption algorithm plays a vital role. It is a valuable and fundamental tool for the protection of the data. Encryption algorithm converts the data into scrambled form by using "a key" and only the user have this key to decrypt the data. Regarding the researches which have been carried out, an important encryption technique is the Symmetric key Encryption. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. In this encryption technique the most used algorithm is the AES [22] [25] [26] [27] [28].

Table 1 lists the basic characteristics of CC technology as regards the convenience this technology offers. Also, it enumerates the basic characteristics of the IoT technology. The main purpose of Table 1 is to demonstrate which of the specific characteristics of CC technology, related more and improve the characteristics of IoT technology. As we could realize by observing Table 1, the characteristics of IoT that affected more by the characteristic of CC is "*Sensors in homes and airports*". Regarding the CC, the characteristics that affected more are "*Service over Internet*" and "*Computationally capable*". As a general conclusion, we can observe that those two technologies contribute more each other in many of their characteristics.

In this work, we present a sort survey of IoT and CC with a focus on the security issues of both technologies. Specifically, we integrate the two aforementioned technologies with the aim to examine the common features, and in order to discover the benefits of their integration. Concluding, we present the contribution of CC to the technology IoT, and it shows how the CC technology improves the function of the IoT. Finally, we survey the security challenges of the integration of IoT and CC with the aim to provide an architecture relaying on the security of the network with the aim to improve the security issues. Concluding, Cloud Computing could offer a more "green" and efficient fog environment for sustainable computing scenarios.

The rest of the paper is divided as follows. In section 2 there is a review of the background research that deals with the technology of BD and the integrated model of CC in IoT. Moreover, Section 3 describes and introduces the security issues of CC and IoT, and their integration model. Section 4 presents and illustrates the proposed network system and how operates compared to similar types of networks. Furthermore, Section 5 demonstrates our experimental results and Section 6 displays the advantages and benefits of the proposed model. Finally, Section 7 provides the conclusions of the current paper and offers new possibilities for the development of future work.

II. Literature Review

For the purpose of this paper we study and analyze previous literature which has been published in the field of Big Data, CC and IoT. The following paragraphs present the papers which contributed significantly in our study.

To begin with, there are several works for the Big Data technology. In recent years several studies for BD technologies have been devised [29-34]. The authors of [29] introduce a multi-objective approach using genetic algorithms. The goal of this is to minimize two objectives, the execution time, and the budget of each node executing the task in the cloud. The contribution of [29] research is to propose an innovative adaptive model to communicate with the task scheduler of resource management. The proposed model periodically queries for resource consumption data and uses to calculate how the resources should be allocated to each task. Through this work, the authors believe that the proposed solution is timely and innovative as it provides a robust resource management where users can perform better scheduling for BD processing in a seamless manner. Furthermore, in [30] the important concepts of BD technology are highlighted and also there is a discussion about the various aspects of BD. Furthermore, the authors of [30] define what BD and discuss the various parameters of its definition. Finally, in [30] there is a look at the process that involved in the data processing and then reviewing the security aspects of BD and as a result, propose a new system for security of BD. Additionally, an offer of six provocation with the aim to spark conversations about the issue of BD technology shown in [31]. These provocations are the cultural, technological, and scholarly phenomenon that rests on the interplay of technology, analysis, and mythology that dares extensive utopian and dystopian rhetoric. Finally, a multi-stakeholder approach for developing a suitable privacy regulation in the age of BD presented in [32]. This argument developed in five steps: 1) A review of the current academic debate on privacy regulation. 2) An argue that the framework for developing a suitable privacy regulation should not only focus on formal and procedural but should additionally include some important essential aspects to guard users and promote socially beneficial BD applications. 3) An examination of how the process leading to an appropriate regulation might be organized. 4) A discussion of the potential structure of a privacy organization which might conduct multi-stakeholder-dialogues as a preliminary step. 5) A discussion of their findings and suggestions.

Moreover, there are several works for the BD technology in regard with new technologies. A literature review of BD and its related technologies, such as Cloud Computing (CC) and Hadoop presented in [33]. Also, the [33] focuses on the five phases of the value chain of BD technology and as a result examines the several representative applications of BD technology. Furthermore, in [34] the important concepts of BD technology are highlighted and also there is a discussion about the various aspects of BD. Furthermore, the authors of [34] define what BD and discuss the various parameters of its definition. Finally, in [34] there is a look at process that involved in the data processing and then reviewing the security aspects of BD and as a result propose a new system for security of BD. Also, an introduction to the MIS Quarterly Special Issue on Business Intelligence Research which first offers a framework that identifies the evolution, applications and emerging research areas of BI&A presented in [35]. Moreover, a definition and description of BI&A 1.0, BI&A 2.0 and BI&A 3.0 in terms of their key characteristics and capabilities are presented in [35]. Also, there is a report of a biometric study of critical BI&A publications, researchers and research topics which based on more than a decade of related academic and industry publications are presented in [35].

As regard the Sustainability of the Cloud Computing, also, there are various works and researches that have been made in the field. We try to present those researches from oldest to newest. Initially, through the [36] the authors strive to compare and contrast Cloud Computing with Grid Computing from different angles, and in addition to give insights into the essential characteristics of both. Another research regarding the open challenges in the field presented in [37]. The [37] presents vision, and architectural elements, except for the challenges, for energy-efficient management of Cloud computing environments. The authors focus on the development of dynamic resource provisioning and allocation algorithms which consider the synergy between different data center infrastructures, and holistically work to boost data center energy efficiency and performance. More specifically, the [37] proposes three things. At first, architectural principles for energy-efficient management of Clouds is proposed. Secondly, proposed some energy-efficient resource allocation policies and scheduling algorithms considering quality-of-service expectations, and devices power usage characteristics. And finally, the authors proposed a novel software technology for energy-efficient management of Clouds. Furthermore, the authors of [38] through their work state some major challenges in the field of Sustainable Cloud Computing, count on recent researches that have been made. One of these challenges is that it is unclear which application areas of IT can and will be outsourced to a Cloud. In a more recent work, and as a newer version of [37], the [39] defines an architectural framework and principles for energy-efficient Cloud computing. The authors, based on this proposed architecture, present their vision, open research challenges, and resource provisioning and allocation algorithms for energy-efficient management of Cloud computing environments. Additionally, the authors conduct a survey of research in energy-efficient computing and propose three things that have discussed in their past work [37]. At the end, the author of [40] discusses a thorough introduction to cloud computing which is realized with emphasis on its advantages for environmental sustainability. Also, a list of challenges in relation to the use of the technology as green technology is presented, and the reasons for using cloud computing for sustainability are explained in his work. And finally, a detailed list of the applications of Cloud Computing focusing on social, business, and environmental sustainability are listed, and a number of conclusions are provided in this work.

III. Security issues in IoT & Cloud Computing integration

There is a quick and independent evolution considering the two words of IoT and CC. Initially, the virtually unlimited capabilities and resources of CC with the aim to compensate its technological constrains, such as processing, storage and communication, could be a benefit for the Internet of Things technology. Also, the IoT technology spins out its scope to deal with real world things in a more distributed and dynamic manner and by delivering new services in a large number of real life scenarios, might be beneficial for the use of CC technology. On several occasions, CC can offer the intermediate layer between the things and the applications, hiding all the complexity and functionalities necessary to implement the latter [41].

Through the integration of IoT and CC could be observed that CC can "complete" some gaps of IoT, such the "*limited storage*" and "*applications over internet*". Also, IoT can "complete" some gaps of CC, such the main issue of "*limited scope*". Based on motivations such those referred beforehand, and the important issue of security in both technologies we can assume some motivations for the integration. The security issue of this integration has a serious problem. When critical IoT applications move towards the CC technology, concerns arise due to the lack of trust in the service provider or the knowledge about service level agreements (SLAs) and knowledge about the physical location of data. Consequently, new challenges require specific attention as mentioned in surveys [42] [43]. Multi-tenancy could additionally conciliate security and lead to sensitive information leakage. Furthermore, public key cryptography cannot be applied at all layers due to the computing power constraints imposed by the things. These are examples of topics that are currently under investigation with the aim to tackle the big challenge of security and privacy in CC and IoT integration [41].

Subsequently, some challenges about the security issue in the integration of two technologies are listed below [42]:

a) *Heterogeneity*. A big challenge in CC and IoT integration is related to the wide heterogeneity of devices, operating systems, platforms, and services available and possibly used for new or improved applications [44].
b) *Performance*. Often CC and IoT integration's applications introduce specific performance and QoS requirements at several levels and in some particular scenarios meeting requirements may not be easily achievable [45].
c) *Reliability*. When Cloud Computing and IoT integration is adopted for mission-critical applications, reliability concerns typically arise. When applications are developed in resource constrained environments several challenges related to device failure or not always reachable devices exists [46].
d) *Big Data*. With an estimated number of 50 billion devices that will be networked by 2020, specific attention must be paid to transportation, storage, access, and processing of the huge amount of data they will produce [47].
e) *Monitoring*. As largely documented in the literature, monitoring is an essential activity in CC environments for capacity planning, for managing resources, SLAs, performance and security, and for troubleshooting [48].

Table 2 lists the two abovementioned technologies that have studied in this research and the challenges of their integration which arising from our study. These challenges are related to the security issue in the integration of those two technologies. As we can observe from Table 2, the both technologies have two common main challenges of their integration which are *Performance* and *Big Data*. Additionally, we can realize that IoT technology related to more challenges (4) than the CC technology (3).

IV. PROPOSED SYSTEM

The study of previous works cites us relevant architecture and topology proposals for a Smart Building network, which on several occasions supported and operated in Internet of Things and Fog environments. In this section we will make a comparative analysis study of the some previous works which we have distinguished. Initially, we analyze what each of them deals with.

Regarding the Literature Review analysis we realize that not enough works deal with security and privacy issues in Cloud Computing for technologies such as Big Data and Internet of Things. Thus, we try to propose a new system for Cloud Computing integrated with Internet of Things as a base scenario for Big Data. In order to improve the security issues we would try to establish an architecture relaying on the security of the network.

As shown in Figure 1, a security "wall" installed between the Cloud Server and the Internet (the various users), with the aim to eliminate the privacy and security issues. This type of network uses all the benefits of the existing topologies (e.g. star, ring etc.) in order to have better communication and to transfer more safely large-scale data (Big Data) through the network.

By applying the proposed model we can extend the advances of IoT and Cloud Computing, by developing a highly innovative and scalable service platform to enable secure and privacy services. Through our research which carried out we can propose the following part of algorithm which extends the security advances of both Cloud and IoT technologies. As a proposal of this work could be this part of algorithm which uses the original key consists of 128 bits/16 bytes which are represented as a 8x8 matrix, represented bellow.

Algorithm 1

```
Cipher(byte[] input, byte[] output)
{
    byte[8,8] State;
    copy input[] into State[] AddRoundKey
    for (i=8; i<88; i++)
    {
        T = W[i-1];
        if (i mod 8 = = 0)
            T = Substitute (Rotate (T)) XOR RConstant [i/8];
        W[i] = W[i-4] XOR T;
        SubBytes ShiftRows MixColumns
    AddRoundKey
    }
    SubBytes ShiftRows AddRoundKey
    copy State[] to output[]
}
```

The new system architecture provides safer paths between the users of the network. As we can see in Figure 2, the whole connection relaying on wireless communication. The Server connects to the internet through a simple wireless router, where there is installed the "security wall". Through the internet any type of user could have access and manage the transferred data of the network if it meets the requirements.

Figure 3 demonstrates the "*little*" difference between the two models that offers remote access and management of data. As we can see, our proposed model is a little bit better dealing with the privacy issue of bits transferred through time. With the use of Wireshark we test the packets sent and received in our proposed Cloud network and in a conventional Cloud network with the same configuration. The packet loss in the conventional Cloud network is a little bit more in contrast with the our proposed Cloud network. This is demonstrated in Figure 4 below:

where the first output from the ping we made is for the conventional Cloud scenario and the second output from the ping we made is for our proposed Cloud scenario. We used the Contiki operating system and the Cooja emulator for the simulation of the edge computing network. The network and various information about it, are presented in Figure 5 below.

Furthermore, in Figure 6, are shown the packets collected which are stored by a "radio messages" tool in .pcap files for further analysis. Wireshark is a network sniffer and analyzer in which, we can observe in the following Figure 6, various information about the communications.

There are more tools, like Wireshark, available to be used with the Contiki OS, such as foren6 and other packet sniffers and packet analyzers. Also, with the Contiki OS we can handle the security and the privacy of these data collected, but novel ideas and implementations need to be further investigated in order to simulate such solutions in real-time and efficiently.

V. EXPERIMENTAL RESULTS

Through experimental scenarios which we have made we have strengthened our suggestion that our proposed model is more efficient than the conventional Cloud model. We perform a number of simulations and measurements through which we can realize that we have done a good effort.

Figure 7, Figure 8 Figure 9 and Figure 10 describe the better Energy Efficiency offered in a framework implementing by our proposed model. As we can observe our proposed model needs less energy power than the conventional model through the time. This can offer a better option of energy consumption and provide a more environmental friendly framework.

The four Figures above demonstrate the difference between the two models that offers remote access and management of data. As we can see, through the experimental results, our proposed model is a bit better dealing with the privacy issue of bits transferred through time.

Moreover, through Figure 11, Figure 12, Figure 13 and Figure 14 we can observe that through our proposed model we can achieve higher data transmission rate through the time than the conventional model. Due to our efficient settled network our model can transmitted higher amounts of data through time, when the conventional model can transmit fewer amounts of data.

VI. Advantages and Benefits of the Proposed Model

Cloud Computing could offer many benefits to people in general, businesses and Small and Medium Enterprises in particular through our proposed model, but additionally and in general use. The five main reasons for adopting a Sustainable Computational Cloud technology with the aim to give it extra boost and competitiveness are listed below:

- ✓ Offers software and application solutions without greatly increasing costs as applications run on the Cloud and businesses do not need expensive computing systems.
- ✓ Has in a similar size data storage in the Cloud proportional to the package selected by the customer.
- ✓ Gives access to Cloud data from anywhere and any device at any given time, giving portability and flexibility to the business.
- ✓ It is backed by state-of-the-art security protocols that ensure enterprise data protection.
- ✓ Provides optimal business performance due to flexibility, mobility and productivity.

Regarding the efficiency of Cloud Computing in general, and more specific our proposed model, there are in addition economic and efficiency benefits:

- ✓ Reduces labor costs by 50% in the configuration, operation, monitoring and management of business operations.
- ✓ Improves the quality and elimination of software defects by up to 30%.
- ✓ Reduces support costs for end users up to 40%.

All these could consist that Cloud is a “green” computational scenario.

Conclusion

Through our research we found in the conclusion that security and privacy issues grew up by the significant advances in the sector of communications and additionally in other sectors. Relay on this, this work aims to introduce Cloud Computing as a base technology in order to operate and integrate with recent technologies such as Big Data and Internet of Things. The technology of Cloud Computing refers to the processing power of the data at the “edge” of a network. Additionally, we could say that Cloud Computing operates in “fog” environment. Regarding this and relaying on the privacy issues in its operation, we proposed a new system for CC which integrated with IoT and operates as a base scenario for BD.

In our scenario, we tried to make an establishment of an architecture relaying on the security of the network with the aim to improve the security and privacy issues. Thus, through the simulations which have been made, the solution that we proposed installs a security “wall” between the Cloud Server and the different users in the Internet. This proposal aims to eliminate the privacy and security issues which need to be faced. Concluding, we considered that the CC provides efficiency in privacy issues of the network, where bits transferred through time.

The main goal of the interaction and cooperation between things and objects communicate through the wireless networks, in order to fulfil the objective set to them as a combined entity. In this research, a sort survey of IoT and CC was presented, with a focus on the security issues of both technologies. Furthermore, the security challenges of the integration of IoT and Cloud Computing were surveyed through the proposed architecture. At the end, we survey the security challenges of the integration of IoT and Cloud Computing with the aim to provide an architecture relaying on the security of the network in order to improve the security issues. Concluding, we could state that Cloud Computing could offer a more "green" and efficient fog environment for sustainable computing scenarios.

Regarding the future, we plan to make more simulations in order to have a better accuracy in our experimental results. More data transfer scenarios have to be made through the simulators providing results counting not only in data transmission but also in network efficiency and support. Also, considering that CC is a novel technology in the sector of communications, more study need to be made about its operation and how CC interact and integrates in better way with other technologies such as IoT and BD. This can be the field of future research.

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] C. Stergiou, K. E. Psannis, "Efficient and Secure Big Data delivery in Cloud Computing", Springer, Multimedia Tools and Applications, pp. 1-20, April 2017.

[2] 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.

[3] T. Li, J. Li, Z. Liu, P. Li, C. Jia. "Differentially Private Naive Bayes Learning over Multiple Data Sources", Information Sciences, vol. 444, pp. 89-104, 2018.

[4] C. Stergiou, K. E. Psannis, A. P. Plageras, G. Kokkonis, Y. Ishibashi, "Architecture for Security in IoT Environments", in Proceedings of 26th IEEE International Symposium on Industrial Electronics, 19-21 June 2017, Edinburgh, Scotland, UK.

[5] J. M. Batalla, P. Krawiec, A. Beben, P. Wisniewski, A. Chydzinski, "Adaptive Video Streaming: Rate and Buffer on the Track of Minimum Rebuffering", IEEE Journal on Selected Areas in Communications, vol. 34, issue: 8, August 2016.

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

[7] X. Zhang, Y.-a. Tan, C. Liang, Y. Li, J. Li, "A Covert Channel over VoLTE via Adjusting Silence Periods", IEEE Access, vol. 5, pp. 9292-9302, February 2018.

[8] Q. Lin, J. Li, Z. Huang, W. Chen, J. Shen, "A short linearly homomorphic proxy signature scheme", IEEE Access, vol. 6, pp. 12966-12972, February 2018.

[9] A. P. Plageras, K. E. Psannis, C. Stergiou, H. Wang, B. B. Gupta, "Efficient IoT-based sensor BIG Data collection-processing and analysis in Smart Buildings", Future Generation Computer Systems, October 2017.

[10] C. Yuan, X. Li, Q. M. J. Wu, J. Li, X. Sun, "Fingerprint Liveness Detection from Different Fingerprint Materials Using Convolutional Neural Network and Principal Component Analysis", CMC: Computers, Materials & Continua, vol. 53, no. 3, pp.357-371, 2017.

[11] M. Rouse, "IoT security (Internet of Things security)", IoT Agenda, 01/11/2015. [Online]. Available: http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security. [Accessed 27/07/2017].

[12] J. Li, X. Chen, X. Huang, S. Tang, Y. Xiang, M. M. Hassan, A. Alelaiwi, "Secure Distributed Deduplication Systems with Improved Reliability", IEEE Transactions on Computers, vol. 64, issue: 12, pp. 3569-3579, 2015.

[13] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain", IEEE Access, vol. 6, pp. 20632-20640, February 2018.

[14] L. Fan, X. Lei, N. Yang, T. Q. Duong, G. K. Karagiannidis, "Secrecy Cooperative Networks With Outdated Relay Selection Over Correlated Fading Channels", IEEE Transactions Vehicular Technology, vol. 66, no. 8, pp. 7599-7603, August 2017.

[15] M. Zakarya, L. Gillam, "Energy efficient computing, clusters, grids and clouds: A taxonomy and survey", Elsevier, Sustainable Computing: Informatics and Systems, vol. 14, pp. 13-33, June 2017.

[16] A. Bianco, R. Mashayekhi, M. Meo, "On the energy consumption computation in Content Delivery Netwroks", Elsevier, Sustainable Computing: Informatics and Systems, vol. 16, pp. 56-65, December 2017.

[17] J. Li, Y. K. Li, X. Chen, P. P. C. Lee, W. Lou, "A Hybrid Cloud Approach for Secure Authorized Deduplication", IEEE Transactions on Parallel and Distributed Systems, vol. 26, issue: 5, pp. 1206-1216. 2015.

[18] A. M. Sampaio, J. G. Barbosa, "Chapter Three – Energy-Efficient and SLA-Based Resource Management in Cloud Data Centers", Elsevier, Advances in Computers, vol. 100, pp. 103-159, 2016.

[19] C. Kulatunga, K. Bhargava, D. Vimalajeewa, S. Ivanov, "Cooperative in-network computation in energy harvesting device clouds", Elsevier, Sustainable Computing: Informatics and Systems, vol. 16, pp. 56-65, December 2017.

[20] L. Fan, X. Lei, N. Yang, T. Q. Duong, G. K. Karagiannidis, "Secure Multiple Amplify-and-Forward Relaying With Cochannel Interference", IEEE Journal of Selected Topics in Signal Processing, vol. 10, no. 8, pp. 1494-1505, December 2016.

[21] M. Haghighat, S. Zonouz, M. Abdel-Mottaleb, "CloudID: Trustworthy cloud-based and cross-enterprise biometric identification", Expert Systems with Applications, vol. 42, no. 11, pp. 7905-7916, November 2015.

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

[23] C.-z. Gao, Q. Cheng, P. He, W. Susilo, J. Li, “Privacy-Preserving Naive Bayes Classifiers Secure against the Substitution-then-Comparison Attack”, Information Sciences, vol. 444, pp. 72-88, May 2018.

[24] B. Li, Y. Huang, Z. Liu, J. Li, Z. Tian, S.-M. Yiu, “HybridORAM: Practical Oblivious Cloud Storage with constant bandwidth”, Information Sciences, in press, 2018.

[25] Y. Kumar, R. Munjal, H. Sharma, “Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures”, IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, October 2011.

[26] R. Kaur, S. Kinger, "Analysis of Security Algorithms in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 3, no. 3, pp. 171-176, March 2014.

[27] J. Li, X. Chen, S. S. M. Chow, Q. Huang, D. S. Wong, Z. Liu, “Multi-authority fine-grained access control with accountability and its application in cloud”, Journal of Network and Computer Applications, vol. 112, pp. 89-96, June 2018.

[28] J. Li, Z. Liu, X. Chen, X. Tan, D. S. Wong, “L-EncDB: A Lightweight Framework for Privacy-Preserving Data Queries in Cloud Computing”, Knowledge-based Systems, vol. 79, pp: 18-26, 2015.

[29] I. A., T. Hashem, N. B. Anuar, A. Gani, "Schedule optimization for big data processing on cloud", in Proceedings of 2nd International Conference on Big Data Analysis and Data Mining, San Antonio, USA, 30 November - 1 December 2015.

[30] R. Toshniwal, K. G. Dastidar, A. Nath, "Big Data Security Issues and Challenges", International Journal of Innovative Research in Advanced Engineering (IJIRAE), vol. 2, issue: 2, pp. 15-20, February 2015.

[31] K. Crawford, D. Boyd, "Critical Questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon", Information, Communication & Society Journal, vol. 15, issue: 5, pp. 662-679, May 2012.

[32] M. G. Will, “Privacy and Big Data: The Need for a Multi-Stakeholder Approach for Developing an Appropriate Privacy Regulation in the Age of Big Data”, Ingo Pies, Halle, July 2015 [Available at SSRN: https://ssrn.com/abstract=2634970].

[33] I. Chebbi, W. Boulila, I. R. Farah, "Big Data: Concepts, Challenges and Applications", Springer International Publishing, Computational Collective Intelligence, vol. 2, p. 638–647, October 2015.

[34] R. Toshniwal, K. G. Dastidar, A. Nath, "Big Data Security Issues and Challenges", International Journal of Innovative Research in Advanced Engineering (IJIRAE), vol. 2, no. 2, pp. 15-20, February 2015.

[35] H. Chen, R. H. L. Chiang, V. C. Storey, "Business Intelligence and Analytics: From Big Data to Big Impact", MIS Quarterly, vol. 36, no. 4, pp. 1165-1188, December 2012.

[36] I. Foster, Y. Zhao, I. Raicu, S. Lu, “Cloud Computing and Grid Computing 360-Degree Compared”, in Proceedings of IEEE GCE ’08, Grid Computing Environments Workshop, Austin TX, USA, 12-16 November 2008.

[37] R. Buyya, A. Beloglazov, J. Abawajy, “Energy-Efficient Management of Data Center Resources for Cloud Computing: A Vision, Architectural Elements, and Open Challenges”, in Proceedings of the 2010 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA 2010), Las Vegas, USA, July 12-15, 2010.

[38] G. Muller, N. Sonehara, I. Echizen, S. Wohlgemuth, “Sustainable Cloud Computing”, Business & Information Systems Engineering, vol. 3, issue 3, pp. 129-131, June 2011.

[39] A. Beloglazov, J. Abawajy, R. Buyya, “Energy-aware resource allocation heuristics for efficient management of data centers for Cloud computing”, Future Generation Computer Systems, vol. 28, issue 5, pp. 755-768, May 2012.

[40] K. Domdouzis, “Sustainable Cloud Computing”, Book section in DASTBAZ, Mohammad, PATTINSON, Colin and AKHGAR, Babak, *Green information technology: a sustainable approach*, Waltham, MA, Morgan Kaufmann, pp. 95-110, December 2015.

[41] A. Botta, W. de Donato, V. Persico, A. Pescape, “Integration of Cloud Computing and Internet of Things: a Survey”, Journal of Future Generation Computer Systems, vol. 56, pp. 1-54, March 2016.

[42] T. Bhattasali, R. Chaki, N. Chaki, “Secure and trusted cloud of things”. In Proceedings of Annual IEEE India Conference (INDICON 2013), Mumbai, India, 13-15 December 2013.

[43] Y. Simmhan, A. G. Kumbhare, B. Cao, V. Prasanna, “ An analysis of security and privacy issues in smart grid software architectures on clouds”, In Proceedings of IEEE International Conference on Cloud Computing (CLOUD 2011), pp. 582–589, Washington, DC, USA, 4-9 July 2011.

[44] N. Grozey, R. Buyya, “Inter-cloud architectures and application brokering: taxonomy and survey”, Software: Practice and Experience, vol. 44, issue: 3, pp. 369–390, December 2012.

[45] B. P. Rao, P. Saluia, N. Sharma, A. Mittal, S. V. Sharma, "Cloud computing for Internet of Things & sensing based applications", In Proceedings of IEEE 6th International Conference on Sensing technology (ICST 2012), pp. 374–380, Kolkata, India, 18-21 December 2012.

[46] W. He, G. Yan, L. D. Xu, "Developing vehicular data cloud services in the IoT environment", IEEE Transactions on Industrial Informatics, vol. 10, issue: 2, pp. 1587–1595, May 2014.

[47] C. Dobre, F. Xhafa, "Intelligent services for big data science". Elsevier, Future Generation Computer Systems, vol. 37, pp. 267–281, July 2014.

[48] G. Aceto, A. Botta, W. de Donato, A. Pescape, "Cloud monitoring: A survey", Elsevier, Computer Networks, vol. 57, issue: 9, pp. 2093–2115, June 2013.

Brij Gupta received Ph.D. degree from Indian Institute of Technology Roorkee, India in the area of Information and Cyber Security. He has published more than 90 research papers (including 03 book and 14 chapters) in International Journals and Conferences of high repute including IEEE, Elsevier, ACM, Springer, Wiley Inderscience, etc. He has visited several countries, i.e. Canada, Japan, China, Malaysia, Hong-Kong, etc. to present his research work. His biography was selected and publishes in the 30th Edition of Marquis Who's Who in the World, 2012.
He is also working principal investigator of various R&D projects. He is serving as associate editor of IEEE Access, Associate editor of IJICS, Inderscience and Executive editor of IJITCA, Inderscience, respectively. He is also serving as reviewer for Journals of IEEE, Springer, Wiley, Taylor & Francis, etc. Currently he is guiding 10 students for their Master's and Doctoral research work in the area of Information and Cyber Security. He is also serving as guest editor of various reputed Journals. Dr. Gupta is also holding position of editor of various International Journals and magazines. He has also served as Technical program committee (TPC) member of more than 20 International conferences worldwide. Dr. Gupta is member of IEEE, ACM, SIGCOMM, The Society of Digital Information and Wireless Communications (SDIWC), Internet Society, Institute of Nanotechnology, Life Member, International Association of Engineers (IAENG), Life Member, International Association of Computer Science and Information Technology (IACSIT). He was also visiting researcher with Yamaguchi University, Japan in January, 2015. His research interest includes Information security, Cyber Security, Mobile/Smartphone, Cloud Computing, Web security, Intrusion detection, Computer networks and Phishing.

Yutaka Ishibashi received the B.E., M.E., and Ph.D. degrees from Nagoya Institute of Technology, Nagoya, Japan, in 1981, 1983, and 1990, respectively. In 1983, he joined the Musashino Electrical Communication Laboratory of Nippon Telegraph and Telephone Corporation (NTT), Japan. From 1993 to 2001, he served as an Associate Professor of Department of Electrical and Computer Engineering, Faculty of Engineering, Nagoya Institute of Technology. Also, he was a Visiting Researcher, Department of Computer Science and Engineering, University of South Florida (USF) (2000–2001). Currently, he is a Professor of Graduate School of Engineering, Nagoya Institute of Technology. His research interests include networked multimedia, multimedia QoS (Quality of Service) control, and multi-sensory communication. He was the Chair of the IEICE Communication Quality Technical Committee (2007–2009). He also served as the Guest Editor-in-Chief of IEICE Transactions on Communications, Special Section on Quality of

Communication Networks and Services, General Co-Chair of Annual Workshop of Network and Systems Support for Games (NetGames) in 2006, 2010, and 2014, and Technical Program Chair of IEEE International Communications Quality and Reliability (CQR) Workshop in 2010 and 2011. He is a fellow of IEICE and a member of IEEE, ACM, IPSJ, ITE, VRSJ, and IEEJ

Kostas E. Psannis was born in Thessaloniki, Greece. Kostas received a degree in Physics from Aristotle University of Thessaloniki (Greece), and the Ph.D. degree from the Department of Electronic and Computer Engineering of Brunel University (UK). From 2001 to 2002 he was awarded the British Chevening scholarship sponsored by the Foreign & Commonwealth Office (FCO), British Government. He was awarded, in the year 2006, a research grant by IISF (Grant No. 2006.1.3.916). Since 2004 he has been a (Visiting) Assistant Professor in the Department of Applied Informatics, University of Macedonia, Greece, where currently he is Assistant Professor (& Departmental LLP/Erasmus-Exchange Students Coordinator and Higher Education Mentor) in the Department of Applied Informatics, School of Information Sciences. He is also joint Researcher in the Department of Scientific and Engineering Simulation, Graduate School of Engineering, Nagoya Institute of Technology, Japan. He has extensive research, development, and consulting experience in the area of telecommunications technologies. Since 1999 he has participated in several R&D funded projects in the area of ICT (EU and JAPAN). Kostas Psannis was invited to speak on the EU-Japan Co-ordinated Call Preparatory meeting, Green & Content Centric Networking (CCN), organized by European Commission (EC) and National Institute of Information and Communications Technology (NICT)/ Ministry of Internal Affairs and Communications (MIC), Japan (in the context of the upcoming ICT Work Programme 2013) and International Telecommunication Union (ITU) SG13 meeting on DAN/CCN, July 2012, amongst other invited speakers. He has several publications in international Conferences, books chapters and peer reviewed journals. His professional interests are: Multimodal Data Communications Systems, Haptic Communication between Humans and Robots, Cloud Transmission/Streaming/Synchronization, Future Media-Internet of Things, Experiments on International Connections (E-ICONS) over TEIN3 (Pan-Asian), Science Information Network (SINET, Japan), GRNET (Greece)-Okeanos Cloud, and GEANT (European Union) dedicated high capacity connectivity. He is Guest Editor for the Special Issue on Architectures and Algorithms of High Efficiency Video Coding (HEVC) Standard for Real-Time Video Applications (2014), Journal of Real Time Image Processing (Special Issue). He is Guest Editor for the Special Issue on Emerging Multimedia Technology for Smart Surveillance System with IoT Environment (2016), The Journal of Supercomputing (Special Issue). He is Guest Editor for the Special Issue on Emerging Multimedia Technology for Multimedia-centric Internet of Things (mm-IoT) (2016), Multimedia Tools and Applications (Special Issue). He is currently GOLD member committee of IEEE Broadcast Technology Society (BTS) and a member of the IEEE Industrial Electronics Society (IES). From 2017 Prof. Kostas E. Psannis serving as an ASSOCIATE EDITOR for IEEE ACCESS and for IEEE Communications Letters. He is also a member of the

European Commission (EC) EURAXESS Links JAPAN and member of the EU-JAPAN Centre for Industrial Cooperation.

Christos Stergiou is currently a PhD student in the Department of Applied Informatics, School of Information Sciences, University of Macedonia, Greece. His main research interests include Algorithms for Cloud Computing, Big Data and Wireless Communication. In 2017, he was awarded by the conference committee of 19th IEEE Conference on Business Informatics (CBI) for Doctoral Student Work titled "Algorithms for Big Data in Advanced Communication Systems and Cloud Computing".

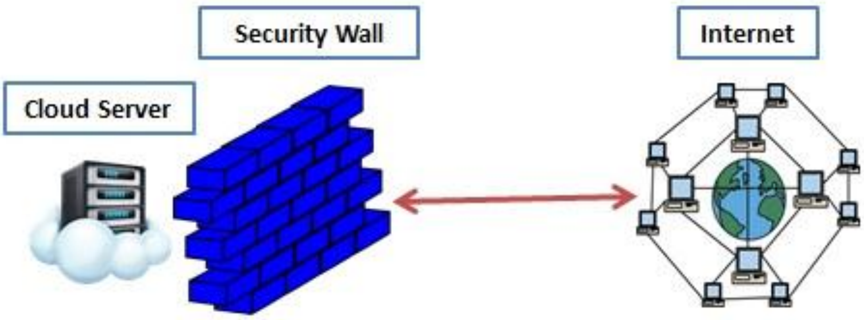


Figure 1: Network Scenario based in “strong” Security Wall.

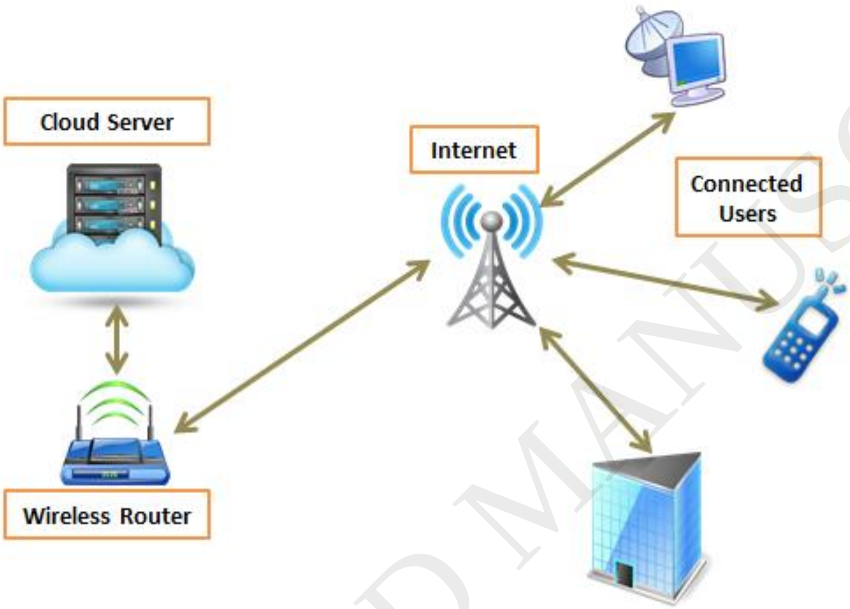


Figure 2: Wide-Range Network of Cloud Computing.

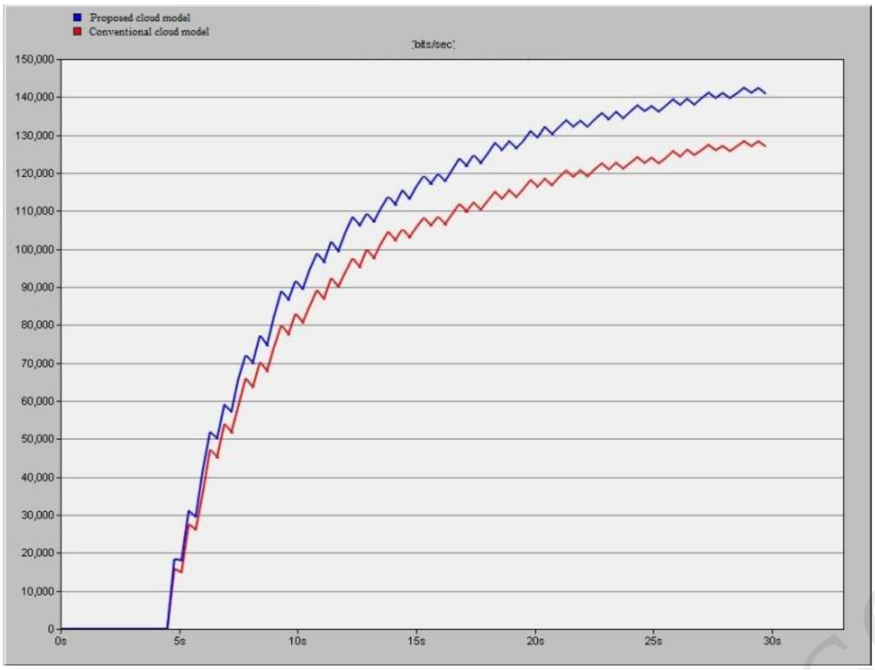


Figure 3: Efficiency comparison proposed model vs. conventional Cloud model.

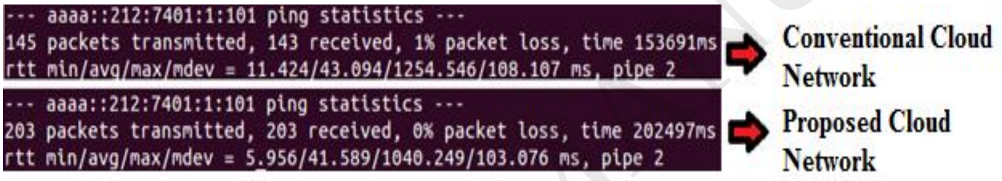


Figure 4: The packet loss for both conventional cloud and proposed cloud computing network respectively.

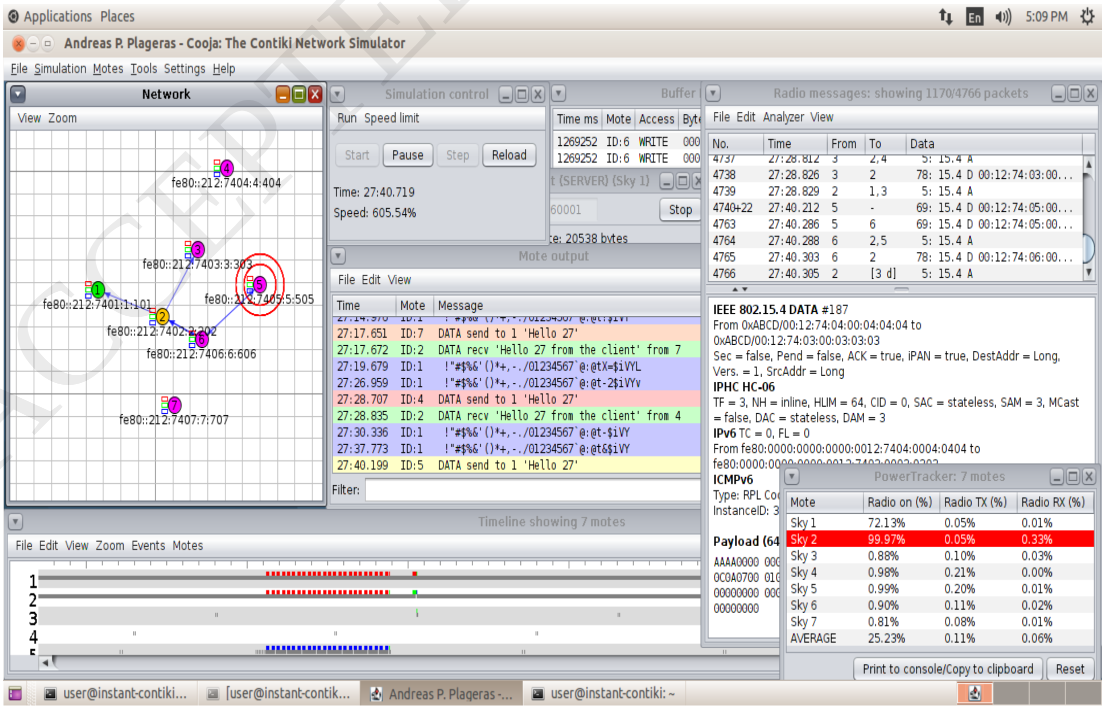


Figure 5: The simulation of the proposed cloud computing network using the Contiki OS.

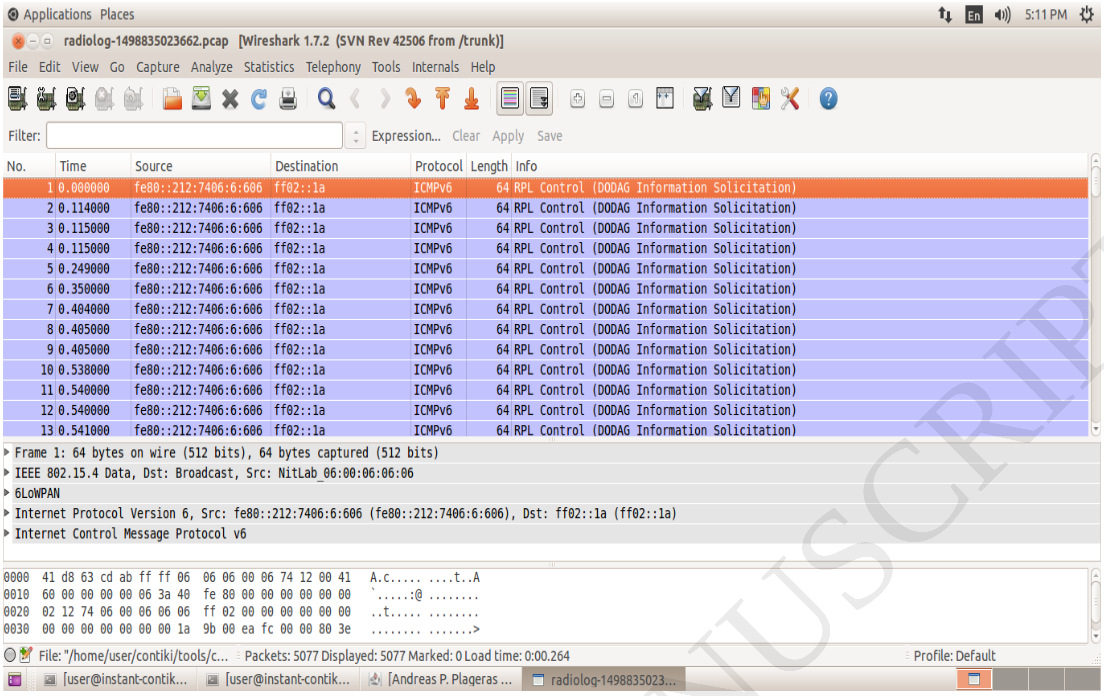


Figure 6: The packets collected and analyzed with Wireshark.

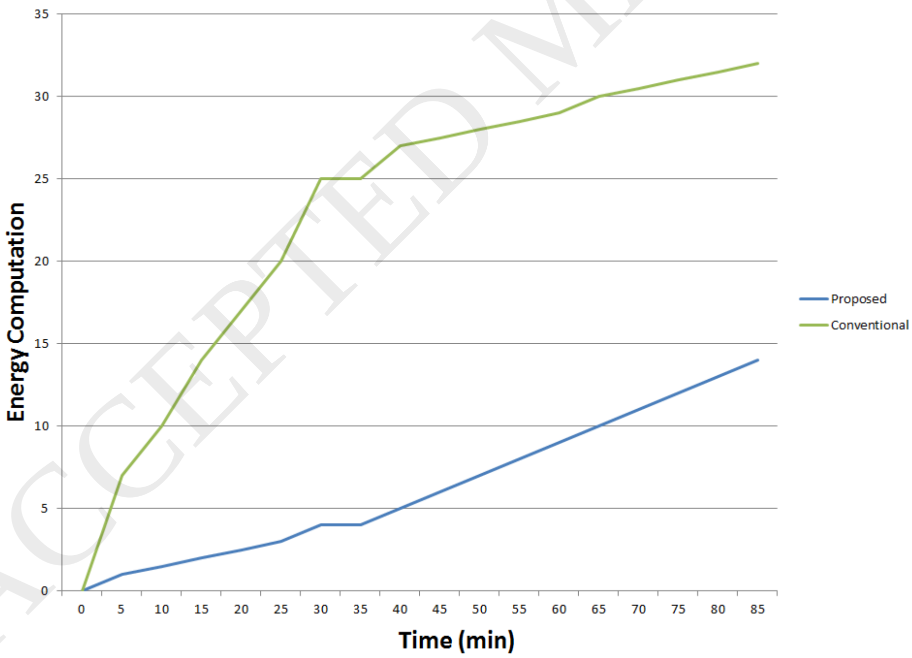


Figure 7: Energy Efficiency Comparison (a).

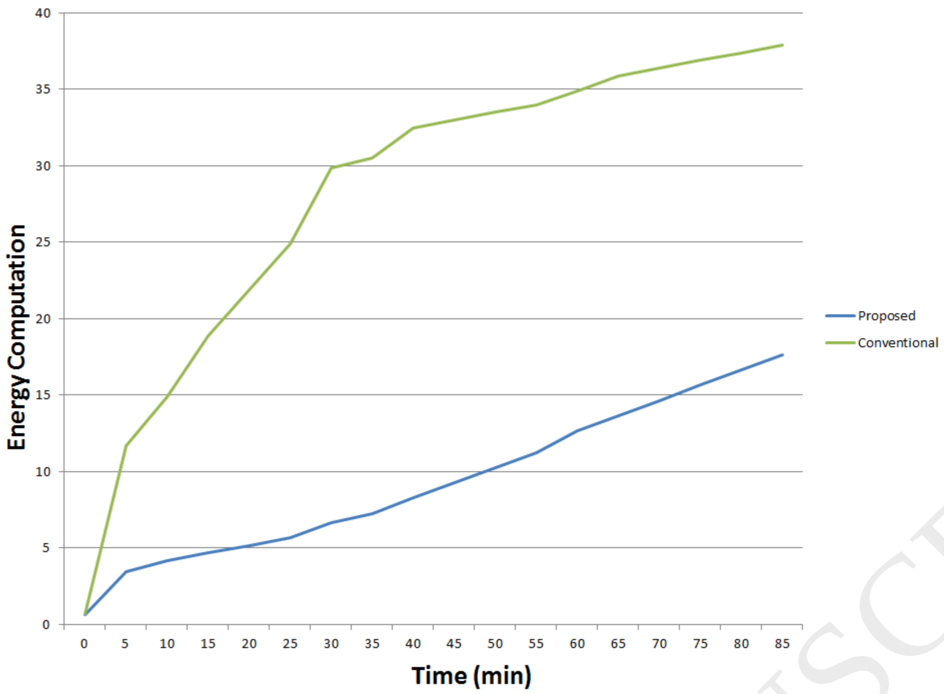


Figure 8: Energy Efficiency Comparison (b).

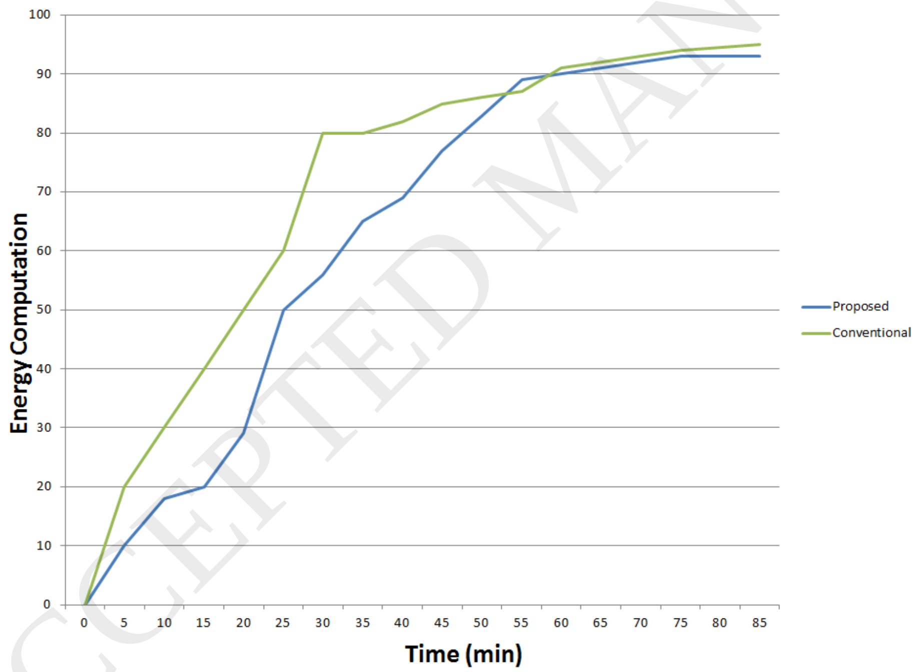


Figure 9: Energy Efficiency Comparison (c).

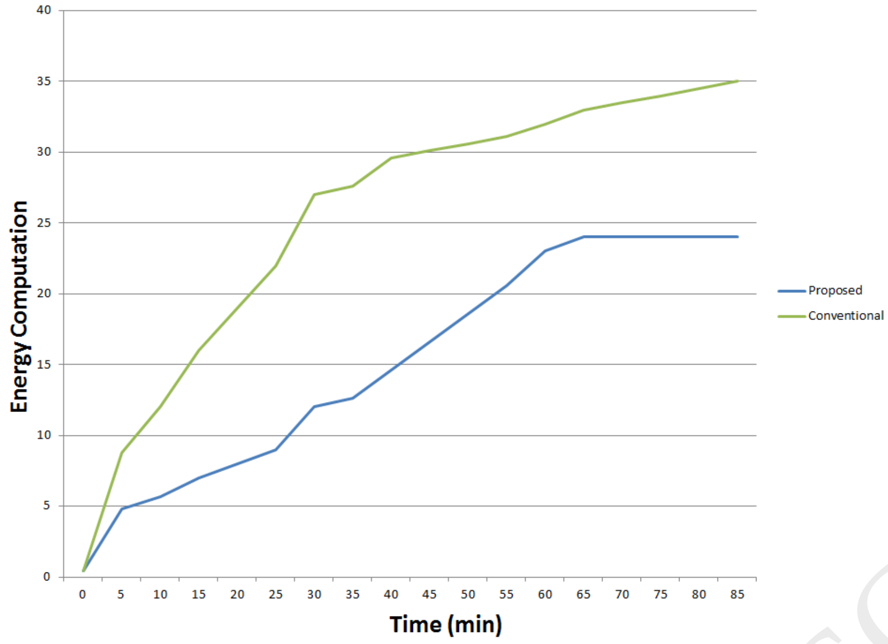


Figure 10: Energy Efficiency Comparison (d).

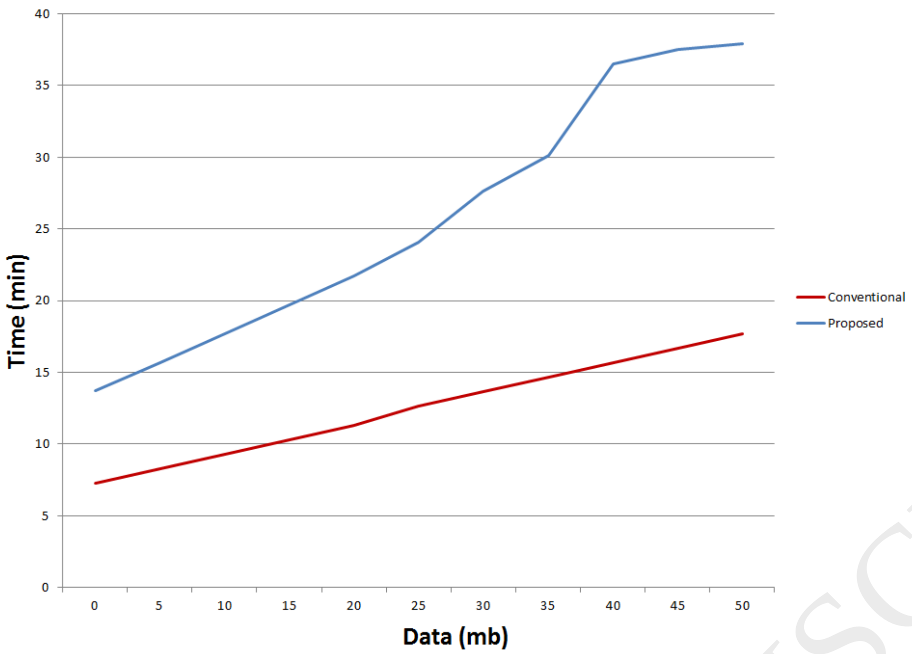


Figure 11: Data Transmission through Time (a).

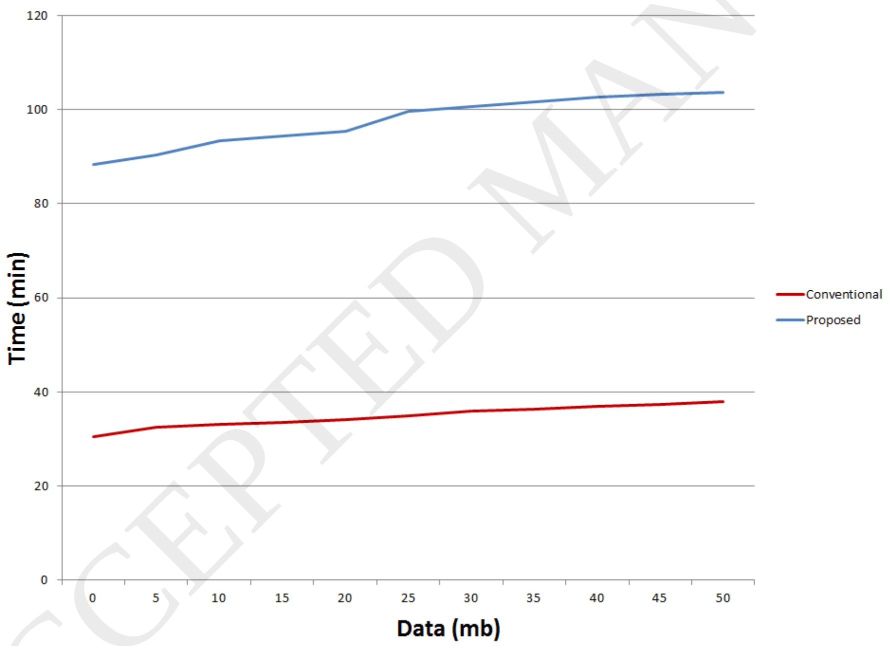


Figure 12: Data Transmission through Time (b).

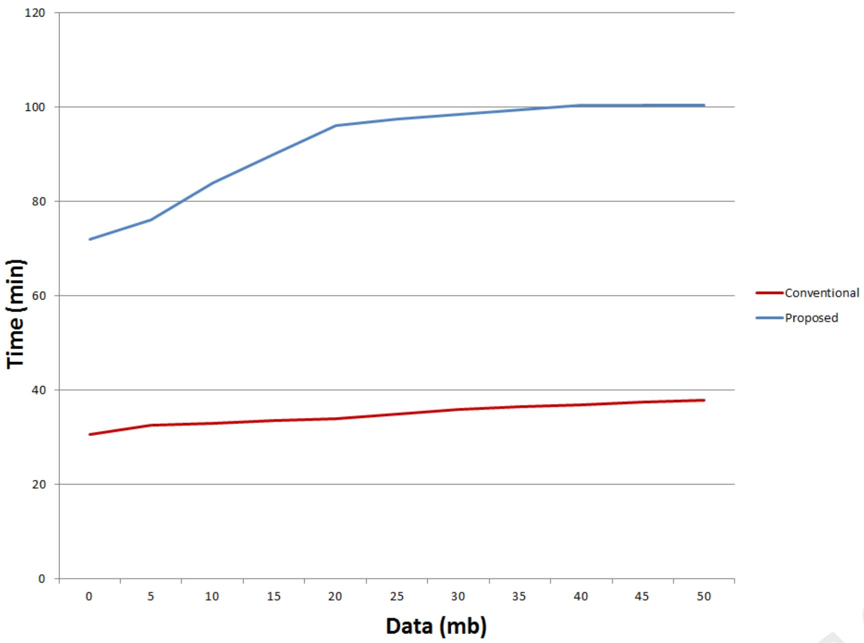


Figure 13: Data Transmission through Time (c).

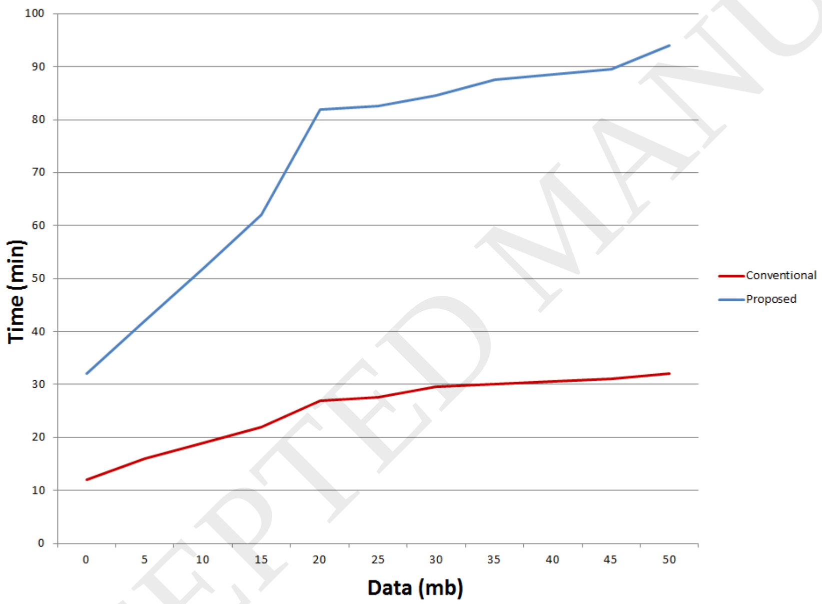


Figure 14: Data Transmission through Time (d).

Table 1: Contributions of Cloud Computing in Internet of Things.

Internet of Things characteristics	*Storage over Internet*	*Service over Internet*	*Applications over Internet*	*Energy efficiency*	*Computationally capable*
Smart solution in the bucket of transport	**X**	**X**	**X**		**X**
Smart power grids incorporating more renewable	**X**	**X**		**X**	**X**
Remote monitoring of patients		**X**	**X**		**X**
Sensors in homes and airports	**X**	**X**	**X**	**X**	**X**
Engine monitoring sensors that detect & predict maintenance issues		**X**	**X**	**X**	**X**

Table 2: Affects of IoT & Cloud Computing security challenges.

IoT & Cloud Computing security challenges	**Heterogeneity**	**Performance**	**Reliability**	**Big Data**	**Monitoring**
Internet of Things		**X**	**X**	**X**	**X**
Cloud Computing	**X**	**X**		**X**	