International Journal of Psychological Rehabilitation, Vol.24, Issue 07, 2020
ISSN: 1475-7192

Using Genetic and Ant Colony Algorithms to Address the Security Issues in Cloud Computing-Based Accounting Systems

Dawood Salman AlFarttoosi[1], Abdalabbas Hassan Kadhim[2]

Abstract: *Due to the recent substantial development in the digital world, transfer data over the network has become more and more critical issue in the context of cloud computing-based accounting systems. This paper discusses the main security mechanisms that could be implemented to fulfill the data protection and confidentiality in cloud computing-based accounting systems. The findings assert the ability to use the computational intelligence techniques (Genetic and Ant colony) to build trust environment in cloud computing. Genetic proposed to apply the Cryptography and achieve data encryption, whereas Ant algorithm combined to add the complexity by creating strong path for each cloud user and this would enable the system to easily detect the unauthorized such as hackers when they try to reach and hack the data.*

Keywords: *Genetic Algorithm, Ant Colony, Cloud Computing, ccounting system, Cryptography*.

I. INTRODUCTION

Cloud computing is a new technology that every organization today aspires to apply to its company in order to obtain greater profitability and expandability [1]. Globalization and increased technology development have imposed the need for economic innovation in order to achieve performance and progress. Nowadays, the impact of globalization and rapid advances in science and technology, the rise of big data, the widespread reach of Internet-based applications and even standardization, have created the appropriate context for the emergence of new, understandable accounting. Business digitization, the increasing capacity of virtual reality, and the shift of traditional computer business diagrams to cloud-based solutions are among the primary drivers of change that are the real principles of the market [2]. On the other hand, accounting is an essential component of the framework that supports the activity of any organization. The focus here is the impact of the cloud computing paradigm on accounting. We highlight various perspectives and definitions dedicated to the concept of "cloud accounting", as well as the potential benefits and risks identified by the adoption of these services, especially with regard to accounting management. Our approach focuses specifically on the security issues of cloud accounting systems and the possible mechanisms for solving these issues in the context of the cloud computing-based accounting systems. Cloud computing is a new computing paradigm in which the third party, cloud service provider, allow users to use different kind of resources on demand [3]. Although there is no universal definition to define the cloud computing, there is a widely accepted definition declared by the United States National Institute of Standard and Technologies (NIST): "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [4]. In 2000, people did not understand the concept of cloud or how it can help their business or organization even nowadays some people still do not know what is the meaning of cloud. Google and IBM initially created the term of cloud when they started to deploy both hardware and software over the network [5]. Cloud vendors are responsible for data processing as well as data saving, clients do not know about the data place and the level of security that used to protect their information, hence cloud providers have to include some assurance in service

[1] [1,2,3]Department of Accounting, Faculty of Administration and Economics, University of Kufa, Iraq

level agreements (SLA) to convince customers that their data will be in safe. For this reason, many approaches and security techniques have been conducted to meet the standards of data confidentiality and security, but hackers already broke some of these strategies to be known and no longer used. This report will discuss the latest security techniques in cloud and attempt to produce a new approach as a suggestion to enhance the data security. Cloud computing can be classified into several models of services as Pearson (2013) [4] indicated in 2013.

- Private: in which one organization or third party can manage and access to the cloud infrastructure.
- Public: Different organizations or individuals have the accessibility to the cloud infrastructure and manage the data.
- Hybrid: Hybrid cloud combine Public and Private Models and this makes it more complex to manage the applications across these two kinds of cloud models.
- Community: This model enables several organizations to share concern applications.
- Partner: specific numbers of parties can be offered with the same services.

II. HYPOTHESIS

Due to the current situation and Internet crimes, data need to be more secure especially when cloud's customers store their information remotely. In addition, lack of full control upon to the user's data makes some costumers do not trust.

III. RESEARCH QUESTIONS

1- Does the security considered as a crucial issue in cloud?

2- Why do companies need to use cloud computing based accounting systems?

3- Do we know about our data storage location?

4- Can be achieved a 100 % data security?

5- What are the techniques that can be used to achieve the data security?

IV. LITERATURE REVIEW

Cloud computing is one of the latest trends in the IT world. Cloud computing is a method by which applications and data are hosted and delivered. Instead of dealing with programs and data stored locally, the places they reside are in the cloud. Cloud computing was created to eliminate the need for people to purchase and install software on their computers through the service is any computer or website [6]. Economic uncertainty and IT transformations are the change agents included in this study. Rapid developments in science, the demographic change that globalization determines, and the encouragement of new business models, will collectively shape different economic expectations and values. The increasing complexity of the business environment, coupled with enhanced global competition and reduced business cycles are prerequisites that challenge the accounting profession. On the other hand, the continuing need for global accounting standards and practices also affects the future of accountants with regard to technology development, and therefore accounting management is generally affected by: the digitalization of business, the strong potential created by the Internet, the implications of big data and the increasing importance devoted to data mining. In this context, cloud computing started creating new business models. The impact of cloud computing is undisputed today and will provide the basis for future transformation in the economic sphere. The accounting profession must first achieve insight into these forces that will reshape the future of the organizations that support them. Second, accountants must objectively assess the effects of these changes in relation to the entire accounting system: standards, processes, and staff. Consequently, the effect of change in the future includes all aspects of accounting, from the role of accounting personnel, to the content of financial reporting standards and tomorrow's accountant reform. Next, we will introduce the article in a qualitative manner, the implications of cloud computing in the field of accounting. The study introduces the concept of "cloud accounting" through different definitions and opinions, especially those contained in the field of information technology (which is in fact the origin of the phenomenon of cloud computing) [7].

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019

In order to fully understand the value created by Cloud Accounting, it is necessary to fully realize the potential of Cloud Computing in a commercial landscape. Cloud computing is no longer a new model, and it generally refers to work done online, without the use of computers or software licensing. Cloud computing is defined as "a type of parallel and distributed system consisting of a set of interconnected and virtual computers that are provided dynamically and are presented as one or more unified computing resources based on service level agreements." In fact it could be considered "the next generation of computing". In other words, cloud computing means: providing computers and software applications as online services. It allows users to store data and use applications through different devices located in several locations. After deploying cloud computing to different types of companies, at a certain point, I also reached the field of accounting. Company accounting should not be in isolation from the business itself, but rather be a key component, with a fundamental role in the life of the company. In order to achieve this goal, the accounting model must be "developed", and thus add value to the financial aspects and the business itself. The traditional applications of financial accounting are sometimes very complex and very expensive, especially for small or start-up businesses. It also requires storage, Internet bandwidth, and an IT team to configure, install, and update the accounting software [7].

Cloud security is a fundamental aspect and it is still need to be addressed and improved. Pearson and Yee (2013) [8] claim that the new security techniques need to be ameliorated to fit the new term of cloud. Group (2014) [9] illustrates that identity and authentication are the most notable issues in cloud computing-based accounting system. Data cannot be fully secure as a 100 percent but the security issues can be minimized by some kinds of control such as security incident prevention, risk detection and error correction [10]. According Sharma, Thulasiram, Thulasiraman, Garg, and Buyya (2012) [11] currently up to 50 percent of cloud customers do not trust online shopping because they try to keep their information safe as much as possible, therefore cloud providers have to eliminate the security challenge by using high quality techniques with complexity. In 2008, International Data Corporation (IDC) carried out a survey to measure the most challenges that face the cloud service as a consequence the security was in the top with 74.6% [12]. The risk of data security in cloud can be mitigated by using cryptography technique which means transform the data from readable form to none readable also can be called encrypted data [13]. Project developers in Microsoft Company start designing cloud system that provide confidentiality, integrity and verifiability with high performance by depending on homomorphism encryption technique [14].

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019

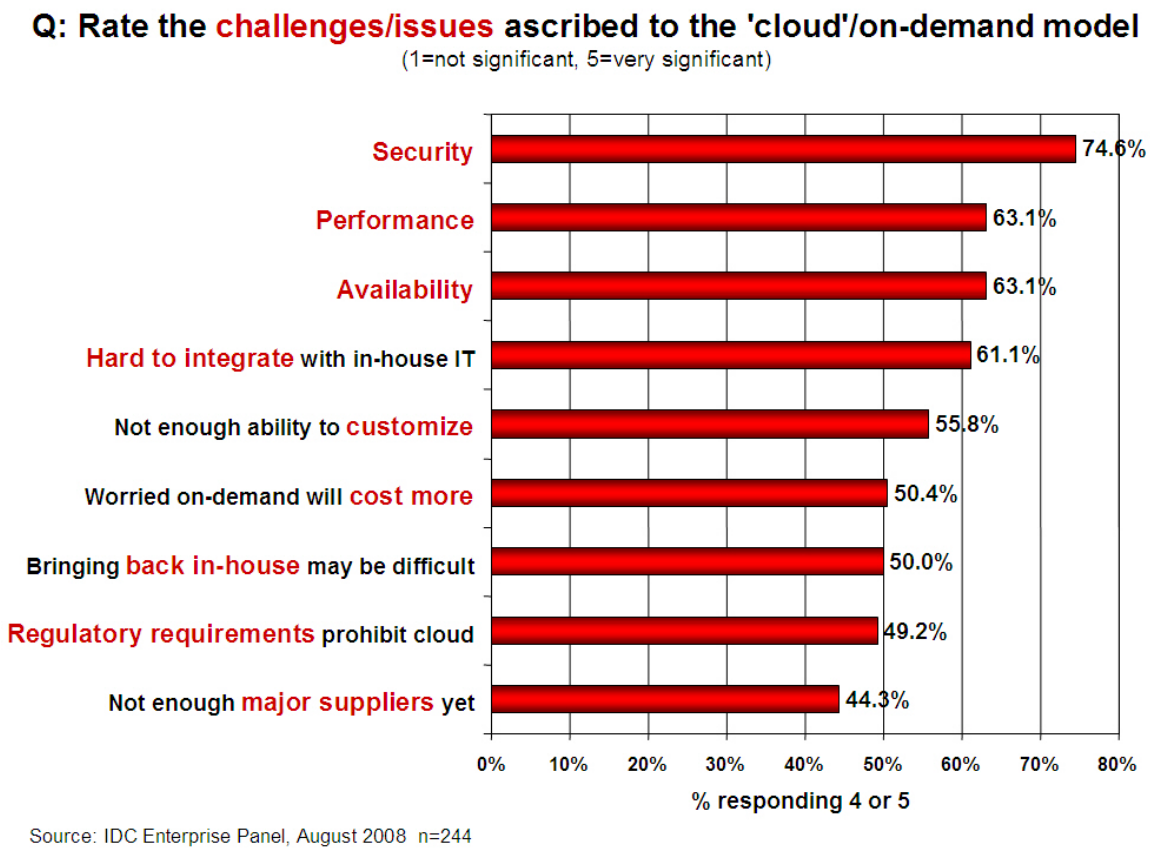


Figure (1) Rate the challenge / issues

3. ADVANTAGES AND DIS-ADVANTAGES OF CLOUD

Cloud technology has both positive and negative sides, however it is widely accepted that benefits outweigh the drawbacks. In bellow there are a list of advantages and disadvantages as mentioned in many recent studies and papers such as (Carolan et al., 2009), (Sokol & Hogan, 2013), (Pearson, 2013), (Pearson & Yee, 2013) [15], [16], [4], [8].

1 Cloud benefits

- Low cost (pay as you go)
- Flexibility
- Scalability
- Makes some new innovations success such as IPad and IPod
- Store data remotely and share resources and applications over the network

2 Cloud dis-advantages

- Security
- Trust and Privacy

V. METHODOLOGY

In order to gauge the security impact factor in case of cloud computing service and how the service providers convince the cloud customers about data insurance and how it would be more secure in their servers. Different materials such as conference articles, scientific reports, books and articles will be the primary source in this report to conduct the information that requires to stand on and high light the current security issues. After compiling the gathered information in report discussion, new security approach will be proposed as a technique to mitigate the vulnerability of security.

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019

VI. CASE STUDY

The main aim of reports that exerted in data protection of cloud computing is to build a robust security environment, which provides confidentiality to the cloud customers as well as seeking to meet the standards in this new technology. Many enterprises used the traditional techniques to achieve data security such as firewalls and intrusion detection systems but these approaches do not perform sufficient protection due to the current security attack [3].There are two powerful strategies that can be implemented to get rid of angst about different kind of security attack: Cryptography and Steganography.

5.1 Cryptography

Cryptography is the mechanism that used to resist an authorized party to expose the multimedia contents. Cryptography performs and conforms vary ways to achieve security in communication. This method involves cipher, hash, digital signature and authentication [17]. These ways including Encryption aim to transform readable information to unintelligible as a technique to provide data security [18]. During the last decades, lots of encryption algorithms have been proposed and studied, but most of them breached to be insecure and no more reliable, therefore the complexity of cryptography methods has been increasing [17]. Cloud computing resources can be shared by multiple customers at the same time therefore security, privacy, trust and confidentiality are the main issues that face the wide spread out of this technology; data and application in cloud are typically store in cloud server and the user does not have fully control upon them therefore cloud customers always looking for technique that enable them to be sure about data protection in cloud environment [3]. Cryptography is one solution that enhance the data safety as well as decreasing the risk of security [3]. According to Kaur (2012) [19] cryptographic encryption is widely used and more trusted, hence most of cloud providers in the U.S and many countries around the world nowadays prefer the cryptography as an efficient way to avoid vulnerability, potential risks and integrity. Consequently, new cryptography approach will be proposed in order to mitigate the issues of security in cloud servers.

5.2 Steganography

The term of steganography comes from Greek's word (steganos and graptos), which is mean covered writing, this approach can be traced back since 440 BC [20]. Ancient Greeks used to use steganography to protect their critical information from unauthorized party. This technique was implemented in a different ways such as invisible ink, written on rabbit stomach and used wax to cover the message that written on table [20]. At current time, this technique has been enhanced due to the technology and computer era but the meaning of steganography did not change, which is hide the crucial information inside another information, also it is considered as a powerful factor to achieve data security. Currently, multimedia files such as image, text, sound and video can be hidden and covered by another multimedia content as a part of security level; these hidden data can be recovered by those who have permission to access and view it. Recently, some of cloud providers tend to apply steganography concept to hide the data of their customers from unauthorized parties, in addition to achieve their goals of building trusted environment [14].

VII. ARTIFICIAL INTELLIGENCE

Cloud susceptible to be threaten by different kind of potential attacks. Computational intelligence techniques play an important role in this context such as artificial neural network to detect intruders over the network ,fuzzy logic and genetic algorithm had a good result in data encryption.

6.1 Ant Colony

Ant algorithm proposed by Marco Dorigo in 1992, it has been used to tackle a lot of problems such as travelling sales man and vehicle routing [10]. The main idea behind of this kind of swarm algorithms is the behavior of Ants, which can be summarized with the creation of strong path between the Ant's nest and food source.

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019

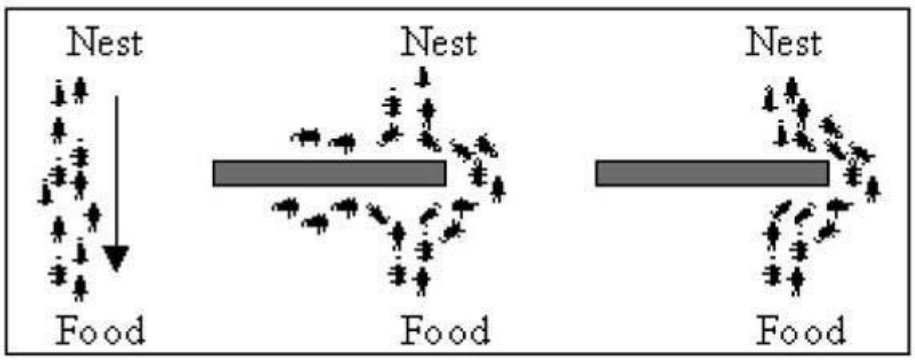


Figure 2: the behavior of ants

Source: Chhikara and Patel (2013) [21]. Enhancing Network Security Using Ant Colony Optimazation. International Journal of Innovative Research and Development, 2(4), 647-655.

6.2 Genetic Algorithm

Genetic algorithms are search techniques, which are based on natural selection and genetics. Holland (1975) [22] proposed the initial framework for this approach and gave an abstraction of biological evolution in his book "Adaptation in Natural and Artificial Systems" [22]. Genetic algorithm based on makes diversity among chromosomes to create new generation with new characteristics that different from both parents.

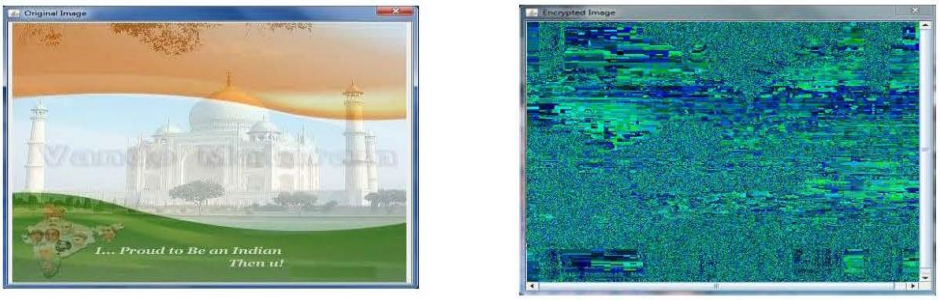
VIII. PROPOSED METHOD

Both Genetic and ant algorithms could be used together in purpose of enhancing the data security and vulnerable detection. The main idea is to build trusted path between the cloud provider and consumer by applying Ant colony algorithm in this context, particularly when Ant algorithm has a good result and evolutionary search and solving a complex problems. In addition, Genetic algorithm and an ant colony optimization will be used to add more complexity by encrypting the data and transform it to non-readable form and that will make the mission of unauthorized party hard to reach and breach this robust system and protected environment.

IX. EXPERIMENTS

In this section will show the experiment result that implement it by using Java programming language at first applied this encryption method on some kind of images and the output was fully non-readable as shown in figure 3.

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019



A B

Figure3: (experiment 1) (India 500 x 500).(A)Original Image (B)Image after encryption

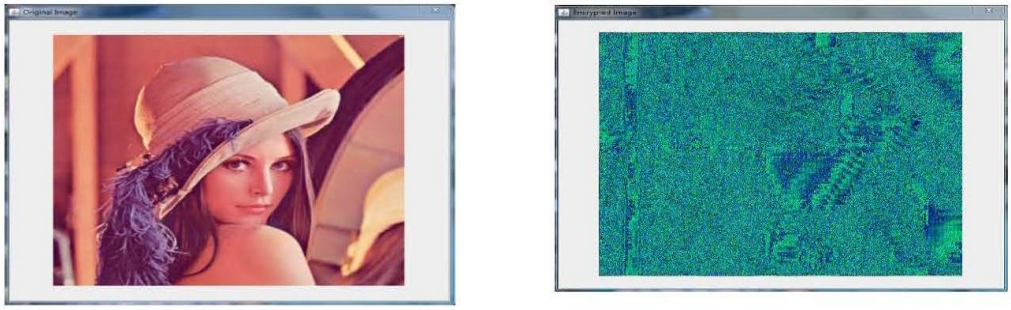
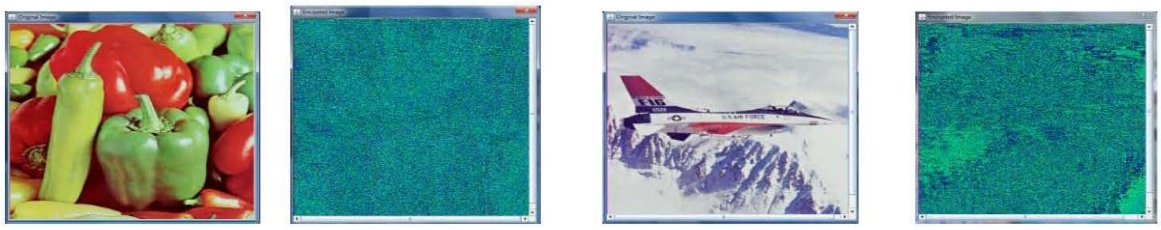


Figure3: (experiment 2) (Lena 512 x 512)



(Pepper 512 x 512) (Air Force 512 x 512)

Figure3: (experiment 3&4)

X. DISCUSSION AND CONCLUSION

Through the case study of this report, it has been found that security and privacy are the most crucial concept in relation with cloud computing. Although, lots of research have been conducted in this area to eliminate the drawbacks, issues have been mitigated but not totally tackled. Two main mechanisms can be applied to achieve data security: Cryptography and Steganography. Hiding the important information by Steganography techniques will protect data from unauthorized access; whereas Cryptography techniques do not prevent accessibility of third party but encrypt the information as a way to make it misunderstand for those who do not have permission to access. New method has been proposed in this report by combining the powerful characteristics of Genetic and Ant algorithms both together to compose new security system, while a good result would be expected. In conclusion, it can be clearly seen that security is an essential factor in cloud computing technology. Efforts have been exerted to decrease the risks of security as well as prohibiting hackers, intruders and crackers to steal the secret information. Cloud has a list of advantages such as low cost, pay as you go, flexibility and makes some innovations to be success such as IPads, but the security issues cause obstacle and service deterioration. Artificial intelligence techniques could play an important role in this context to increase the robustness of security of accounting systems by utilizing the features of Genetic and Ant algorithms.

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019

XI. REFERENCES

[1] Elzamly, Abdelrafe, Nabil Messabia, Mohamed Doheir, Samy Abu Naser, and Hazem A Elbaz. "Critical Cloud Computing Risks for Banking Organizations: Issues and Challenges." Religación. Revista de Ciencias Sociales y Humanidades 4, no. 18 (2019): 673-82.

[2] Vasile, Valentina, Călin-Adrian Comes, Beatrice-Anamari Ştefan, and Anca Munteanu. "Emerging Markets Queries in Finance and Business." Procedia Economics and Finance, no. 32 (2015): 1-3.

[3] Chauhan, N Singh, and Ashutosh Saxena. "Cryptography and Cloud Security Challenges." CSI Communications (2013).

[4] Pearson, Siani. "Privacy, Security and Trust in Cloud Computing." In Privacy and Security for Cloud Computing, 3-42: Springer, 2013.

[5] Lohr, Steve. "Google and Ibm Join in 'Cloud Computing'research." New York Times 8 (2007).

[6] Christauskas, Česlovas, and Regina Misevičienė. "Cloud-Computing Based Accounting for Small to Medium Sized Business." Inžinerinė ekonomika (2012): 14-21.

[7] Dimitriu, Otilia, and Marian Matei. "A New Paradigm for Accounting through Cloud Computing." Procedia economics and finance 15, no. 14 (2014): 840-46.

[8] Pearson, Siani, and George Yee. "Privacy and Security for Cloud Computing: Computer Communications and Networks." London, UK: Springer-Verlag, 2013.

[9] Group, NIST Cloud Computing Forensic Science Working. "Nist Cloud Computing Forensic Science Challenges." National Institute of Standards and Technology, 2014.

[10] Shtovba, Serhiy D. "Ant Algorithms: Theory and Applications." Programming and Computer Software 31, no. 4 (2005): 167-78.

[11] Sharma, Bhanu, Ruppa K Thulasiram, Parimala Thulasiraman, Saurabh K Garg, and Rajkumar Buyya. "Pricing Cloud Compute Commodities: A Novel Financial Economic Model." Paper presented at the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012), 2012.

[12] Rittinghouse, John W, and James F Ransome. Cloud Computing: Implementation, Management, and Security. CRC press, 2016.

[13] Mather, T. "Cloud Security and Privacy/Mather T., Kumaraswamy S., Latif S." Sebastopol: O'Reilly, 2009.

[14] Sarkar, Mrinal Kanti, and Trijit Chatterjee. "Enhancing Data Storage Security in Cloud Computing through Steganography." International Journal on Network Security 5, no. 1 (2014): 13.

[15] Carolan, Jason, Steve Gaede, James Baty, Glenn Brunette, Art Licht, Jim Remmell, Lew Tucker, and Joel Weise. "Introduction to Cloud Computing Architecture." White Paper, 1st edn. Sun Micro Systems Inc (2009).

[16] Sokol, Annie W, and Michael D Hogan. "Nist Cloud Computing Standards Roadmap." 2013.

[17] Linda, Ondrej. "Applications of Computational Intelligence in Critical Infrastructures: Network Security, Robotics, and System Modeling Enhancements." University of Idaho, 2009.

[18] Robling Denning, Dorothy Elizabeth. Cryptography and Data Security. Addison-Wesley Longman Publishing Co., Inc., 1982.

[19] Kaur, Simarjeet. "Cryptography and Encryption in Cloud Computing." VSRD International journal of Computer science and Information Technology 2, no. 3 (2012): 242-49.

[20] Wawge, PU, and AR Rathod. "Cloud Computing Security with Steganography and Cryptoghrapy Aes Algorthm Technology." World Research Journal of Computer Architecture, ISSN (2012): 2278-8514.

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019

[21] Chhikara, Parul, and Arun K Patel. "Enhancing Network Security Using Ant Colony Optimization." Global Journal of Computer Science and Technology (2013).

[22] Holland, John. "Adaptation in Natural and Artificial Systems: An Introductory Analysis with Application to Biology." Control and artificial intelligence (1975).

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019