Critique of academic paper: *A comparative analysis of Encryption Techniques and Data Security Issues in Cloud Computing*

Jaleesa Dmytrow

200300170

The paper “A Comparative Analysis of Encryption Techniques and Data Security Issues in Cloud Computing” by N. Hemalatha, A. Jenis, A. Cecil Donald, and L. Arockiam attempts to show the comparisons of encryption techniques within Cloud Computing. This paper was published in the International Journal of Computer Applications in June of 2014. Hemalatha et al structure the paper into different sections for different topics. To achieve their goal the authors use many sources for different encryption techniques. Although the authors had a structured paper in the layout the content did not fully address the topic of the paper. The paper’s method for collecting data does not look like it was well thought out. The structure of the abstract is disorganised and foreshadows how the paper will be set up.

When reading the paper “A Comparative Analysis of Encryption Techniques and Data security Issues in Cloud Computing” the reader will start to question the structure of the paper. The author’s approach to the subject matter is scattered as they talk about different characteristics of cloud computing, classification of cloud computing and deployment models of cloud computing before encryption techniques. In section six, the paper talks about the security issues of cloud computing. This section is the last section of the paper and should probably be the first or second section. A better structure for Hemalatha et al’s paper would be to briefly describe cloud computing in the first section, describe the security issues with cloud computing in the second section and then discuss and compare encryption techniques. With the current structure a reader is left to guess what security issues cloud computing has and why you may want to use a type of encryption to protect data. Hemalatha et al have also added more information about cloud computing in general than is necessary. By adding too much irrelevant information the topic of the paper becomes unclear and does not line up with the title of the paper. This paper has many grammatical errors and lacks proper sentence structure within the paper. With the grammatical errors and improper sentence structure the paper is hard to read at times which detracts from the topic of the paper. An example of an improper sentence structure is “One of the standard definition National Institute of Standard and Technology (NIST) defined cloud computing as...” [1]. This example shows that if the paper was read out loud the authors would notice the sentence does not flow, the words “from the” should be placed before “National Institute of Standard

and Technology...” to make this sentence clearer. If this example was one of the only mistakes this would not be an issue but the paper is full of errors similar to this example.

While trying to address the subject matter the authors cover topics that are relevant to cloud computing but are irrelevant to security and encryption techniques unless these characteristics or topics relating to cloud computing affects security. For example, in section two the authors talk about essential characteristics of cloud computing [1]. This section could have been useful as characteristics of cloud computing is important but the authors did not specify how the characteristics mentioned related to the security of cloud computing. Section two also mentions different classifications of cloud computing such as public, private and hybrid [1]. This information should have listed the different security issues with the different classifications, such as public cloud computing could be less secure than private or hybrid models. The fourth section of this paper talks about different deployment options for cloud computing such as Platform as a Service (PaaS) and Software as a Service (SaaS) [1]. The paper adds filler information about providers of different deployment options which are completely irrelevant. Once again, there is no tie in for the section topic and the security issues related to cloud computing. Without the security information on these topics the sections about deployment, characteristics, and classifications of cloud computing is nothing more than filler information.

One of the other flaws of the paper “A comparative Analysis of Encryption Techniques and Data security Issues in Cloud Computing” is the sources used for encryption techniques. When looking for encryption techniques a reader would be looking for multiple options, especially when the paper states there will be a comparative analysis of encryption techniques. At the beginning of section five the authors focused on describing different key encryption categories such as asymmetric and symmetric key algorithms [1]. Although these are important encryption categories there are other types of encryptions that do not include a key such as Hash algorithms. Hashing is a good encryption technique for small amounts of data but should have been mentioned as it is an encryption technique that could be used for cloud computing [4]. The paper does not deliver a large amount of techniques, in reality they really only talk about two techniques in a small amount of detail. This paper uses two different

symmetric encryption techniques but what they do not mention is that symmetric key encryption is one key to encrypt and decrypt. This could be a huge security flaw if the key is not kept private. If an unauthorized person gets a hold of your encryption key the security of the data can be compromised [4]. This paper defines two classifications of ciphers: substitution and transposition [1]. These two classifications are mentioned later in the paper, in section 5.4 in the second paragraph, however, the facts sound confusing. In the second paragraph of section 5.4 the authors mention how to improve classical encryption techniques by integrating substitution cipher and transposition ciphers [1]. This fact contradicts the facts stated in section 5 which states that Classical Encryption algorithms are categorized into two principles: Substitution Cipher and Transposition Cipher [1]. How do you integrate encryption techniques into themselves? If an encryption technique is categorized as a Substitution cipher or Transposition cipher integrating Substitution ciphers or Transposition ciphers would not be possible. One of the first encryption techniques the authors mention is the inverse of a Caesar cipher. This is an example of an encryption technique, however, when searched for with a simple Google search no results that relate to this idea are found. The authors also specify that Caesar cipher can be broken by a brute force attack which is true but do not provide an example of the inverse of the Caesar ciper. The second encryption technique mentioned in the paper is called a Playfair cipher [1]. The authors state that Sastry et al, who are authors for one of the references of the paper “A comparative Analysis of Encryption Techniques and Data security Issues in Cloud Computing”, proposed the Playfair cipher [1]. After a quick search on Google I found that the Playfair cipher was not proposed by Sastry et al but invented by Charles Wheatstone [3]. This makes their reference incorrect which eliminates the credibility of this academic paper. When a reader finds a reference is incorrect they start to question whether other facts presented in the paper are correct and the integrity of the paper comes into question.

Section 5.2 is one of the sections of the paper “A comparative Analysis of Encryption Techniques and Data security Issues in Cloud Computing” that makes the least amount of sense. While reading the first paragraph the reader will notice that the author is stating the same information in about five different ways. One sentence states that a fully Homomorphic encryption is an encryption that allows a person without the

key to decrypt the data. The individual will be allowed to perform operations on the data like they are working with the raw data instead of the actual encrypted data [1]. The second paragraph in this section states that this method ensures data confidentiality, authentication, integrity and availability by using Homomorphic cryptography with Attribute Based Encryption [1]. As a reader, this method does not sound secure at all. If operations can be performed on data without decrypting the data the question of “is the data really encrypted in the first place?” will be asked. The authors of this paper do not explain what Homomorphic cryptography with Attribute Based Encryption is even though they are supposed to be doing a comparative analysis of different encryption techniques. In sections 5.3 and 5.4 the authors continue to mention techniques that their sources describe and propose but do not state the facts of these techniques within their own paper. As the title of this paper is “A comparative Analysis of Encryption Techniques and Data security Issues in Cloud Computing” the techniques that are mentioned should have more information so that comparisons could be made.
One section, which should be the largest section of the paper, that is completely missing is the comparisons of techniques used in cloud computing. This is the actual reason for the paper but the authors chose to just state different techniques from different resources. A comparative analysis should have tables, charts, and graphs depicting the usefulness of an encryption technique, how fast the encryption can be broken in relation to other encryption techniques, and other valuable data when trying to pick a strong encryption technique. This paper does provide a comparison of encryption techniques that were mentioned but the table is missing information. The columns of Table 1 include: Author, Techniques Used, Description, Concepts Used, Security Applied On, and Issues Addressed [1]. This table is stating basic facts about the resources and what the encryption concepts are but has very little comparisons between the techniques. When looking at Table 1 the reader will see that all techniques are symmetric key encryption which is secure only if the key is secure [4], which the authors do not mention.

One of the things I found that this paper was missing was the different versions of symmetric cryptography algorithms and asymmetric cryptography algorithms. To explain this point, I found a paper called “Encryption Techniques in Cloud Computing”

that is not an academic paper but mentions many other algorithms such as RSA, DES, Blowfish, RC5 [2]. This paper gives brief descriptions of the different algorithms and how they work. This paper did not stick with just symmetric algorithms (DES) but also talked about asymmetric (RSA), block cipher algorithms (Blowfish and RC5) [2]. Although these techniques were not compared the fact that the paper mentions them provides more information than Hemalatha et al's paper does.

The conclusion of this paper should summarize what the paper was about but ends up sounding more like an introduction. The last sentence in this conclusion is that Table 1 explains the comparison among various encryption techniques used in the cloud [1]. If someone has read the paper they have already seen Table 1 and know that it explains comparisons of techniques mentioned in the paper. This paper implies the overall goal is to provide readers with different encryption techniques and the comparison of these techniques to point out which would work well, what flaws exist, and how these encryption techniques are used in cloud computing. Overall this paper lacked a large variety of encryption techniques to compare. There were many flaws in the abstract that were contradicted within the paper itself. An example of one of the flaws is that Hemalatha et al state they will compare several encryption techniques; however they only compare a couple of techniques and leave out several important options. The authors had many grammatical and incorrect sentence structure errors that could have been avoided if proof read more than once. The authors also should have checked their sources as a reader might doubt their credibility if an incorrect fact is noticed. This paper should have compared characteristics of encryption techniques not just encryption techniques as general information. Many parts of this paper could have been summarized into smaller paragraphs as the topics did not directly relate to Encryption Techniques in cloud computing.

References

[1] N.Hemalatha, A. Jenis, A. Cecil Donald, and L. Arockiam, "A comparative Analysis of Encryption Techniques and Data Issues in Cloud Computing," *International Journal of Computer Applications*, vol. 96, no. 16, June 2014. [Online]. Available: URSummon, http://research.ijcaonline.org/volume96/number16/pxc3896873.pdf.[Accessed: Jan. 20, 2016].

[2] M. Kumari and R. Nath, "Encryption Techniques in Cloud Computing," *Advances in Computer Science and Information Technology*, vol. 2, no. 3, p. 276-280, January-March 2015. [Online]. http://www.krishisanskriti.org/vol_image/04Jul2015110718zzx%20%20%20%20%2082zMeena%20Kumari%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20276-280.pdf. [Accessed: Jan. 20, 2016].

[3] “Playfair Cipher.” [Online]. Available: http://practicalcryptography.com/ciphers/playfair-cipher/. [Accessed: Jan. 20, 2016].

[4] M. Ciapa, *CompTIA Security+ Guide to Network Security Fundamentals*, 5th ed., Boston: Cengage Learning, 2014.