Scientific and Practical Cyber Security Journal (SPCSJ) 3(2): 1- 17 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

Securing User's Attributes on Transit to the Cloud using AES-128 bits Cryptography and DCTM3 Steganography Techniques

Maria M. Abur, Sahalu B. Junaidu, Saleh E. Abdullahi and Afolayan A. Obiniyi
Department of Computer Science, Ahmadu Bello University, Zaria.

ABSTRACT. Cloud adoption is increasing day by day as such, more and more trades and enterprises are moving their vital IT structure and data to the cloud. This move is driven by the remarkable potential of cloud platforms that promise exceptional functioning, efficacy, productivity, agility, elasticity and cost-effectiveness. Although every technology has its strengths and weaknesses, the nature of the cloud makes it vulnerable to the following issues: Performance, Security and Cloud Interoperability with the main problem being security and to be even more specific are the privacy concern which cloud users really fear. The lack of privacy is the inability to protect user's attributes (or Personal Identifiable Information (PII)) as a result of data leakage, breaches and loss of data. This had made users' sceptical about sending their sensitive data to the cloud. Although there are other solutions to protect user's data during transit such as securing user's attribute with the Rivest–Shamir–Adleman (RSA) cryptography. However, RSA have been practically broken and user's sensitive information compromised. Also data leakages still hamper the security of user's data during transmission on the network to the Identity provider (IdP) on the Cloud. This paper presents an Enhanced PII Privacy Protection solution using Advanced Encryption Standard AES-128 and Discrete Cosine Transform Modulus Three (DCT-M3) Steganography techniques in order to protect user's attributes from being leaked when it is being transmitted and stored on the IdP in the cloud. The supremacy of the proposed model over the existing model was also measured based on the encryption techniques used, undetectability and robustness of the Stego image.

KEYWORDS*:* Cloud, Personal Identifiable Information, Security, Identity provider, Network, Steganography, Cryptography techniques and Transit

I INTRODUCTION

Identity Management refers to set of principles, policies, procedures, and technologies that offer automated identifications to persons and preserve confidential facts about the owners of those identifications and help in finding out and allowing access to resources. Identity Management System defines a system that contains information and group of technologies that can be used for innovativeness or inter-network identity management. Examples of Identity Management Systems (IMS) are Shibboleth, OpenID, OpenAm, CardSpace, Liberty Alliance and OAuth (Chadwick (n.d.); Suriadi *et al.,* (2007) and Teena *et al.,* (2017)). The features of IMS includes: Undetectability, Unlinkability and Confidentiality. These features are related with each other due to the fact that they deal with the descriptive actions involving parties in access to a range of private and sensitive data Teena *et al.,* (2017). The undetectability feature shields communications done by the user and prevents the exposure of the user actions in a given system. While the unlinkability feature hides the communication between user identities and history of transactions (e.g., subjects, messages, events, actions) and then the confidentiality feature enables users exercise control over the dissemination of their attributes.

Shibboleth as an Identity Management System (SIMS) is liable for forming the identity of a user, i.e. creating, maintaining and managing identity information for the user, and also managing access to services by the user. It involves the: Identity Provider and Service Provider, (Hogan (n. d.); Chadwick (n. d.); Suriadi *et al.,* (2007); Weingartner & Westptall (2014) and Abur *et al.,* (2018)). Important concepts on SIMS based on this research are: User's attributes, Service Providers (SPs) and the Identity Provider (IdP). The user's attributes which refers to any information usually used to uniquely identify a person whether alone or by combination with other public data that could be connected to a particular person. It is also called Personal Identifiable Information (PII). In this paper, PII is interchangeably used with the user's attributes. Examples of user's attributes are: first name, dates of birth, addresses, student number and the likes. The service providers denotes organizations that provide services or resources desired by a user, by requesting for the submission of valid credentials such as attributes or pseudonyms from the user's IdP. Finally the Identity Provider is "the entity that creates, maintains and manages identity information for the users and provides users' authentication to other service providers within IMS.

Cloud adoption is increasing day by day as such, more and more trades and enterprises are moving their vital IT structure and data to the cloud. This move is driven by the remarkable potential of cloud platforms that promise exceptional functioning, efficacy, productivity, agility, elasticity and cost-effectiveness. Although every technology has its advantages and weaknesses, the nature of the cloud makes it vulnerable to the following issues: Performance, Security and Cloud Interoperability with the main problem being security and to be even more specific are the privacy concern (i.e. data leakage, breaches and loss of data) has made Cloud users' sceptical about sending their sensitive data to the Cloud. Although there are other solutions to protect user's data during transit to IdP such as securing user's attribute with the Rivest–Shamir–Adleman (RSA) cryptography. However, RSA have been practically broken and user's sensitive information compromised. Also data leakages still hamper the security of user's data during transmission on the network to the IdP in the cloud.

Securing of user's attributes in the cloud environment must comprise of definite features that consider the intricacy of the environment. If the security of user's attributes is not guaranteed in the cloud, users will remain sceptical about transferring data to the cloud. This paper presents an Enhanced PII Privacy Protection solution using Advanced Encryption Standard AES-128 and Discrete Cosine Transform Modulus Three (DCT-M3) Steganography techniques in order to protect user's attributes from being leaked when it is being transmitted and stored on the IdP in cloud. The supremacy of the proposed system over the existing system was also measured based on the encryption techniques used, undetectability and robustness of the Stego image. This paper proposes to ensure that user's attributes is secured during transit and when stored in the IdP on Cloud.

The subsequent sections are organized as follows: Section II describes related work; Section III illustrates the PII privacy protection model; Section IV discusses models for formalizing attributes protection on IdP; Section V presents a comparative analysis of the prototype model versus existing model; Finally, section VI concludes the paper.

II RELATED WORK

Shibboleth is a joint project of Internet2 and IBM. It is open-source based system that supports inter-institutional resource sharing with access. Shibboleth enables the secure exchange of interoperability of services. It employs the idea of federated identity and Single Sign-On (SSO) authentication where there is interaction between the IdP, SP and User. However, there are still limited features and functionality that threatens user's privacy and identity if they store and process personal information with inadequate protective measures Aldeen *et al.,* (2010). Usually user's attributes are entered as plaintext when they sign up into the system and when these attributes passes through the network they become exposed to data leakage and network issues such as sniffing, spoofing, eavesdropping and malicious insider attack, Asha *et al.,* (2016) & CSA, (2016). This is not healthy for the privacy of the user when their data are transmitted to the cloud.

Switch *et al.,* (2010) added uApprove plugin – a user consent module for shibboleth identity providers to address problem of the existing system. The uApprove plugin displays to the user, the Personal Identifiable Information (PII) that the IdP shall release to the requesting SP on behalf of the user. It also offers awareness of data release when accessing some services. However, users cannot make a choice of data that should be divulged to the Service Provider. Similarly, the client has no option assenting/dissenting with His/her PII disclosure. During the dissemination of user's attributes to SPs on the network, data leakage is envisaged as user's attributes are usually exposed to security threat such as spoofing, sniffing, eavesdropping, malicious attack, Asha *et al.,* (2016) & CSA, (2016) and the SPs having received these attributes use them maliciously either directly or indirectly against the users without their consent and then leading to collusion. This way, the users' privacy is being threatened. Also during signup by users into their IdP, through the network, user's attributes are transmitted as plaintext which are prone to data leakage and network issues.

Orawinwaltakul *et al.,* (2010) added "uApprove.jp, a user consent acquisition system (UCAS) with an attribute-filter mechanism for a Shibboleth based SSO system". uApprove.jp request the "user's consent and enable the user control the release of his/her original attributes" values or PII values whether mandatory/optional from the IdP to the SP and then allows the user to determine which of his/her original attributes values are meant to be sent to the SP in order to access services provided by Service Providers. The uApprove.jp is an extension of uApprove Switch *et al.,* (2010). However, the user's control of his/her PII is ineffective making them vulnerable as there is still data leakage. Also original users' attributes values are released to the SP by the IdP are sometimes maliciously shared among other SPs or even used without the user's consent to either harm the user directly or indirectly hence leading to violation of the user's privacy and causing collusion problem. Similarly, during signup by users into their IdP, through the network, user's attributes are transmitted as plaintext which are prone to data leakage and network issues, Asha *et al.,* (2016) & CSA, (2016).

Weingartner & Westptall (2014) improved on the research of Orawiwattanakul *et al.,* (2010) by adding two objects namely: Template Data Dissemination and Cryptography Encryption Key Technique on Shibboleth/uApprove.jp framework. The former object helps users during the course of dissemination of their attributes from the IdP to the

SPs; while the later enable users enter their attributes as plaintext and then get them encrypted with Key I before sending them to IdPs. During a transaction when some PII data is needed by SPs, users would be entreated to open that encrypted data with key II in order to disseminate them to the requesting SP for the release of resources back to user. The Cryptography Encryption Key Technique used by Weingartner & Westptall (2014) is the Rivest–Shamir–Adleman (RSA). However, three basic weaknesses were identified on this system. The first is centred on the encryption techniques used i.e. the RSA which have been be practically broken and user's sensitive information compromised Kumar *et al.,* (2011); Tripathi & Agrawal, (2014) and Hackers News, (2017). The second weakness identified is the exposure of the transmitted attributes on the communication medium, which attracts potential hackers due to data leakage, Asha *et al.,* (2016) & CSA, (2016) when transmitting to the IdP. Thirdly, SPs having received these attributes may keep them and use them without the users consent or even maliciously use them against users in the future. This leads to collusion.

Leandro *et al.,* (2014) demonstrated the flow of operations of the Shibboleth architecture and discussed its main components in details. It was observed that the flow of information from user to SP, then to IdP and then back to the user is lengthy and thereby exposing users to security threat such as data leakage on the network. Secondly, there is delay in WAYF populating the IdP for User's selection. Thirdly, during dissemination of user's attributes from the IdP to the SP, the original user's attributes value are sent to the SP. This attributes may be kept or further reused again by the SPs without the consent of the user for malicious purposes and thus, violating the user's privacy. Furthermore, during signup by users into their IdP, through the network, user's attributes are transmitted as plaintext which are prone to data leakage and network issues.

In comparison with existing system of Weingartner & Westptall (2014), based on the features in the proposed system it is expected that this will outperform the existing system in the area of securing users attributes on the IdP. This is as a result of the fact that the AES-128 is more secured than RSA encryption techniques and further hiding of the encrypted attributes in the Stego image provides additional security. Hence, joining both of them will provide a stronger security solution. This paper aims at providing a better solution of securing users attributes on transit to the IdP on cloud and ensuring that the privacy of the user is preserved. Figure 1(a) depicts the existing PII privacy model used for securing user's attributes and Figure 1(b) illustrates insecure communication between user & IdP and then IdP & SP on the Cloud in the existing system. This paper is focused on the insecure communication between user & IdP.

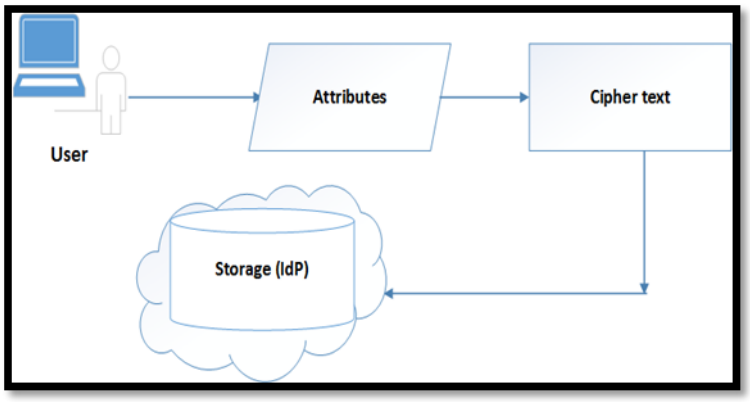


Figure 1(a): Existing PII privacy model for securing user's attributes. Weingartner & Westptall (2014)

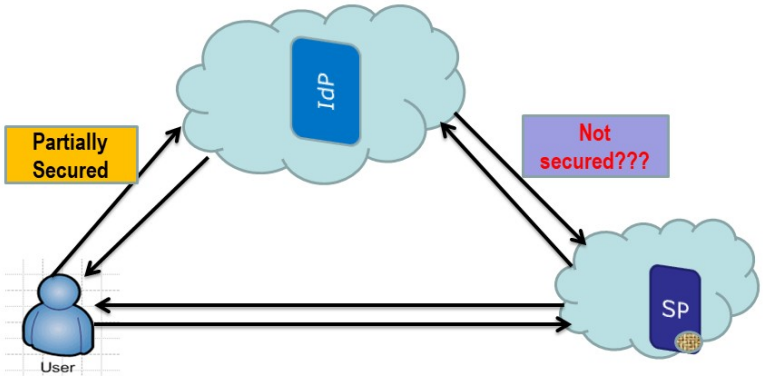


Figure 1(b): Insecure communication between user, IdP and SP on the Cloud on the existing system.

III PROPOSED PII PRIVACY PROTECTION MODEL

This is an improvement on the existing PII privacy protection model of Weingartner & Westptall (2014). Users would enter their attributes as plaintext into identity provider (IdP) in the same way like on the existing model. The proposed system builds a more secured system which will make up for the weaknesses of the existing model discussed in section III. Two basic weaknesses were identified in the existing system. The first is centred on the encryption techniques used i.e. the Rivest–Shamir–Adleman (RSA) which have been practically broken and user's sensitive information compromised. The second weakness identified is exposure of the transmitted attributes on the communication medium, which attracts potential hackers. The proposed model will however address these two basic weaknesses identified with the existing system.

Firstly to take care of the encryption techniques the proposed model uses the AES-128 encryption technique. The use of this encryption technique is hinged on the fact that attributes encrypted with this technique have not been practically broken, though theoretically broken (Kaminsky *et al.,* (2010); Song *et al.,* (2014); Sachdev *et al.,* (2013); Lokhande *et al.,* 2014 and Aleisa (2015)). Although Literature had revealed that AES-128 is yet to be 100% completed and that at year 2020 AES-128 will be completely broken, (Kaminsky *et al.,* (2010); Song *et al.,* (2014). An attempt to wait for the practical breaking of the AES-128 before enhancing the security of user's attributes will create a vacuum in the security of user's attributes on the cloud. It is a wise thing to do by augmenting the weaknesses

of AES-128 on the theoretical aspect and of course to forestall the effect of the practical breaking of AES-128 in the nearest future.

Secondly, to circumvent the exposure to potential hackers on the existing model and to forestall the effect of the practical breaking of AES-128 in the nearest future, the proposed model introduces DCT-M3 steganography technique (Subhedar & Mankar, 2014 and Attaby *et al.,* 2017). This is to ensure that the already encrypted attributes are hidden in a cover image given rise to a Stego image before onward transmission to the IdP. This process has potentials to make the encrypted attributes undetectable while being transmitted to the IdP.

It is expected that this will outperform the existing model in the area of securing users attributes on the IdP. This is as a result of the fact that the AES-128 is more secured than RSA encryption techniques and further hiding of the encrypted attributes in the Stego image provides additional security. Hence, joining both of them will provide a stronger security solution. The supremacy of the proposed model over the existing model shall be measured based on the encryption techniques, undetectability and robustness of the Stego image. MatLab shall be used to test the undetectability and robustness of the proposed model. This shall be presented in section IV B. Figure 2 shows the proposed PII privacy protection model. The procedure for hiding the User's attribute using AES-128 + DCT-M3 techniques and the respective extraction stage as illustrated on Figure 2 are described in a) and b) respectively.

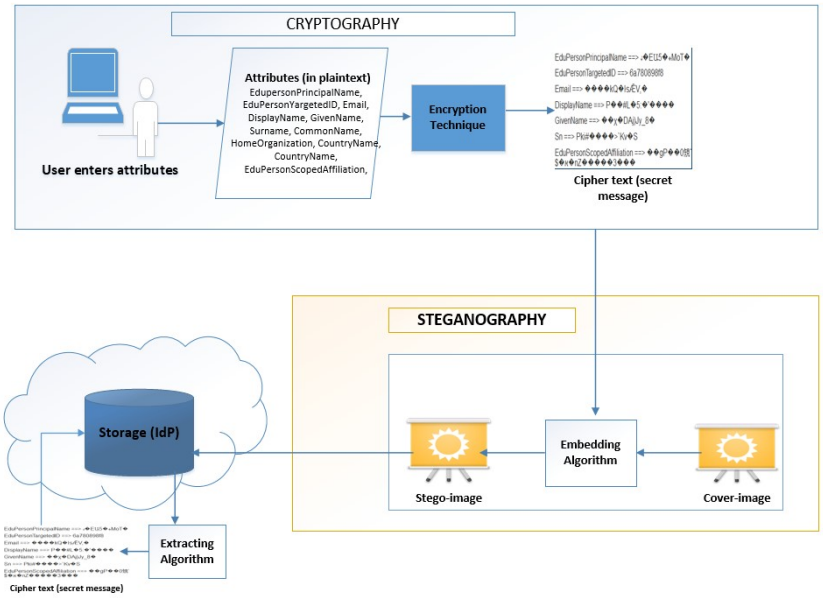


Figure 2: Proposed PII privacy protection model

a) The user's attribute hiding stage can be summarized as:

i. The user's attributes (i.e. secret message) are first received as plaintext and converted to ciphertext by encrypting with the AES-128 encryption algorithm.

ii. Obtain the binary representation of the ciphertext.

iii. Cover image is selected and then "switch the RGB color layers of the cover image into three different components (Y, Cb and Cr)".

iv. After that, translate "the image into transform domain by transforming the pixel data into $8 * 8$ block DCT coefficients" using the equation:

v. $$F(u,v) = \frac{1}{4}C(u)C(v)\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) * \cos\left[\frac{(2x+1)u\pi}{16}\right] \times \cos\left[\frac{(2y+1)v\pi}{16}\right]$$

vi. Produce a "randomized" order with secret key, "K using pseudo random method".

vii. Select a static "place of two DCT coefficients which" shall be changed to implant cipher (thereby avoiding "the DC component of each DCT coefficients block").

viii. Inside every block of 64 coefficients implant "only two bits (Pair) as follows:

i.) Compute the difference between non-overlapping pair of AC coefficients which are selected.

ii.) Change DCT coefficients values based on the original values and the message bits accordingly".

ix. Conclude the implanting till the message bit stream is ended.

x. Reinstate original order "of the DCT blocks using the key, K".

xi. "Quantize the image using a quantization table.

xii. Re-order the values using Zig-Zag ordering".

xiii. "Use Huffman lossless compression coding to compress the image."

b) The decoding phase can be condensed as:

i. Alter the stego-image into transform domain by changing the pixel data into $8 * 8$ block DCT coefficients.

ii. Produce randomized order "with key, K using pseudo random method".

iii. Inside every block of 64 coefficients decode two bits (Pair).

iv. Join the decoded sub message pairs to get a stream of bits.

v. "Uncompressing the stream of bits to get the original message (ciphertext)."

IV MODELS FOR FORMALIZING ATTRIBUTES PROTECTION ON IDP

A. Formalising Shibboleth User's attributes Protection:

In the rest of the paper, the symbol **"→"** shall be used to denote mathematical function, the symbol **"⟹"** shall be used to denote transmission between two entities, the symbol " ⟺ " will be used to denote two-way transmission between entities and the symbol **"↓"** represents constraint on the transmission between two points.

A. Formalising the Existing PII privacy model:

Let α_f be a function that is used for encrypting user's attributes with public key and passphrase of the existing model. Let set $\mathbf{A} = \{a_1, a_2, a_3 \ldots a_n\}$ represent user's attributes needed to be secured; where **n** is a positive integer ≥1. Let $\mathbf{B} = \{b_1, b_2, \ldots, b_n\}$, be a set of encrypted values where $b_i = \alpha_f(a_i)$, $a_i \in A$. Now the encryption can be defined in (1) as:

$$\alpha_f: A \rightarrow B \quad (1)$$

Let **F** be a function representing the communication channel that transmits B to the storage C on the IdP in the Cloud. **Let** c_i be the elements of B that are stored in C, as shown on (2):

$$F: B \Longrightarrow C \quad (2)$$

Since **B** must pass through **F** inorder to get to **C**, data leakage through the communication medium, F has been identified by Asha *et al.,* (2016) and CSA, (2016) as a challenge that needs to be addressed when **B** travels to **C**. Let $\mathbf{W_q}$ be the data leakage problem that may occur between **B** and **C**, which can be modeled as shown in (3):

$$F: B \underset{\downarrow W_q}{\Longrightarrow} C \quad (3)$$

The (1) to (3) which were conceptualized by this research have been able to reveal each of the critical stages required for transmission of attributes (A) to the storage C on the IdP in the cloud. The challenge of data leakage and several network attacks are things that should not be ignored. Hence, there is the need to increase the security of the system in order to be able to minimize the influence of network attacks on the transmitted data. To increase the security "of the existing system" in order to prevent $\mathbf{W_q}$, (4) is then introduced.

B. Mathematical model for the proposed PII privacy protection

Let set **A** represents user's attributes to be secured, the proposed model employs encrypting function which is based on the symmetric encryption technique. Let α_z be a function denoting the AES-128 cryptography technique of the proposed system that is applied to the elements of **A** to produce elements of **Y**, where **Y** is the set of ciphertext in the proposed solution. Literature have shown that the AES-128 techniques has been theoretically broken, and has not been practically broken (Kaminsky *et al.,* (2010), Song *et al.,* (2014), Sachdev *et al.,* (2013); Lokhande *et. al.,* (2014) and Aleisa, 2015) hence, the preference for this encryption technique in the proposed system. This is illustrated in **(**4):

$$\alpha_z: A \rightarrow Y \quad (4)$$

However, it has been mention in Kaminsky *et al.,* (2010) that at year 2020, AES-128 will be completely broken. The introduction of Steganography is to shield the encrypted information and increase the rigor of breaking the AES-128 cryptography technique. The next step is to introduce a function **β** representing the DCT-M3 Steganography Technique which will embed the ciphertext in Y into an image. Let v be the image that has the capacity to accommodate all the encrypted attributes which is to be stored in K, where K is a set of the Stego-images. This step is as described by equation (5):

$$\beta: Y \rightarrow K \quad (5)$$

In summary, Let **U** be the composition of $\boldsymbol{\alpha_z}$ and **β**which will take the user attributes from set A to the set of stego images K. This is shown in (6):

$$U: A \rightarrow K \quad (6)$$

where $U=\beta \circ \alpha_z$

The next step is to transmit the stego image from **K** to through **F** to the storage **C** on the IdP in the cloud. Let **F** be a function representing the communication channel that transmits **K** to **C**. This is demonstrated on (7) as:

$$F:K \rightleftharpoons C \quad (7)$$

So that for the stego image $\mathbf{k_i}$ in the set **K** there is an element $\mathbf{c_i}$ in **C** such that $\mathbf{c_i=F\ (k_i)}$ to be stored in **C** on the IdP.

V COMPARATIVE ANALYSIS OF THE PROPOSED MODEL VERSUS THE EXISTING MODEL

The comparison analysis of the proposed model over the existing model shall be measured based on the encryption techniques used and then the undetectability and robustness of the Stego image of the proposed model.

A. Comparative analysis based on the complexity of the existing and proposed model with respect to the Wq attack on the Cloud C.

Comparison of the proposed model with the existing model is based on the security of the transmitted data through F (communication channel which is the network) to the storage C in the cloud. This comparison is based on the encryption technique used i.e. the RSA verses AES-128 which were employed in the existing technique and the proposed technique respectively. The RSA is an asymmetric technique which is a two key method which uses one of the keys for encryption and the other for decryption. This method is susceptible and has been known to be broken (Kumar *et. al.,* 2011; Tripathi & Agrawal, 2014 and Hackers News, 2017). The method is slow in computation and inefficient in terms of implementation (Kumar *et. al.,* 2011; Tripathi & Agrawal, 2014 and Hackers News, 2017). Also, longer key generation time and high computational overload characterize the method. On the other hand, the AES-128 technique uses a single key for encryption as well as decryption. It is characterized by the following advantages: has not "been practically broken in reality"; very easy to design; stronger and faster in nature; efficient in Speed and code compactness on a wide range of platforms, has low computational overload, effective generation time and has short key size (Smith,2003; Sachdev *et al.,* 2013; Lokhande *et al.,* 2014 and Aleisa, 2015).

The introduction of DCTM3 Steganography technique is an additional security measure taken to further enhance the security of the encrypted attributes. This hides the ciphertexts in Stego-image so that in case of data leakage and network attacks (sniffing, spoofing and malicious attack); the encrypted attributes are hidden from the prying eyes of the attacker.

Let W_q (b) represent W_q attack as shown on (3). Since $b = \alpha_f(a)$ then the attack launched on b shall be $W_q(\alpha_f(a))$

On the other hand, from (7) representing the proposed system, the attack is carried out on the Stego-image ***k***.

To successfully attack the transmitted data, the Stego-image has to be broken first so that $W_q(k) = W_q(\beta(y))$, which needs to be broken further to access the ciphertext becomes $W_q(\beta(\alpha_z(a)))$.

In summary, the decrypted attributes in the existing model is given as:

$$a = \alpha_f^{-1} b \tag{8}$$

This shows that W_q needs only to employ α_f^{-1} to successfully attack the transmitted attributes. In the proposed model however, the W_q attack is carried out on the Stego-image *k* using the key β^{-1} to set the ciphertext y then use the key α_z^{-1} on y to successfully decrypt the data. Hence W_q needs to combine α_z^{-1} and β^{-1} keys to successfully attack the data. So that,

$$a = \alpha_z^{-1}(\beta^{-1}(k)) \tag{9}$$

Comparing the W_q attack as presented in (8) for the existing model and (9) for the proposed model, one could see that recovering the original attributes is easily achievable in the existing model since only one key α_f^{-1} is required to successfully attack and obtain the original attributes.

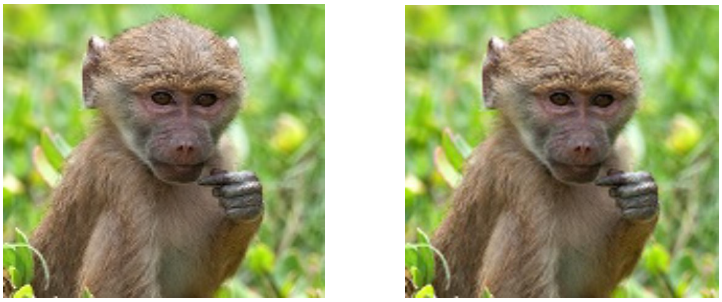
However, the task of W_q attack on the proposed model requires a composition of two keys; $(\alpha_z^{-1} \circ \beta^{-1})$ which is more difficult than the existing model. This is so due to the fact that α_z^{-1} has not been practically obtained. Hence, the security of data transmitted over the proposed model is more guaranteed in comparison to that of data transmitted over the existing system.

B. Performance evaluation of the security of the proposed model

This section presents further evaluation of the security of the prototype model. The objective of this session is to analyse the cover image and stego-image and then measure the security of the proposed model based on the following metric: undectability and robustness of the Stego image.

1.) *Analysis of the Cover Image and Stego Image*

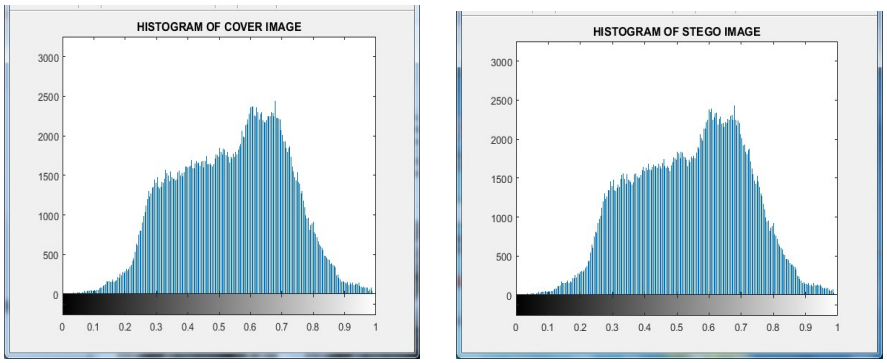
The image baboon.jpg with size of 512*512 was used in the research as the cover image to hide the ciphertext containing user's attribute given rise to the resultant stego- image. This was implemented in Java programing language. The cover and stego image were taken and then processed with Matrix Laboratory (MATLAB) version 2017a on Windows 10 with 8GB RAM size, and the processor of Intel(R) Core(TM), i3-5005U CPU @ 2.00GHz. Furthermore, the computer is a 64-bit operating system and x64-based processor. The cover image and stego image are represented on figure 3 (a) and (b) respectively. From the experimental result, it is difficult to differentiate between the Stego-image from the cover image, since the similarity between them is really high and the closer the stego image is to the cover image implies a greater security.



(a) (b)

Figure 3: (a) Cover Image and (b) Stego Image

Comparing the RGB histogram of both cover image and Stego image shows no significant difference graphically between them as depicted on figures 4 (a) and (b) respectively. Similarly, the closer the stego image is to the cover image implies a greater security.



(a) (b)

Figure 4: (a) Histogram of Cover Image and (b) Histogram of Stego Image

2.) *Mean Square Error (MSE) of the Stego image*

MSE describes a minimal non- perceptual error metric that is acquired from the cover image and Stego image where lesser values for MSE demonstrate negligible detectability on the image processed. In this research the MSE was used to measure the undetectability of the stego image. The smaller the value of MSE the lower the error rate and thus guaranteeing security of the stego image, (*Kamdar et al.,* (2013); Hemalatha *et al.,* (2013) and Attay *et al.,* (2017)). MSE is calculated with the given formula on (10).

$$\text{MSE} = \frac{1}{(M \times N)} \sum_{x=0}^{M} \sum_{y=0}^{N} (Cij - Sij)^2 \qquad (10)$$

"Where C denote the cover image, S is the Stego image, M and N are the width and height (i.e. M * N) of the cover image C and stego image S". When MSE is calculated for baboon.jgp with 36.5 kb of data embedded in the image, the MSE is 0.076248. The MSE measures the undetectability of the proposed model with value falling within the standard range for measuring MSE. The proposed model guarantees security of Cloud user's data.

3.) Peak Signal-to-Noise Ratio (PSNR) of the Stego image

PSNR refers to the ratio between a signal's maximum power and the power of the signal's noise, Seyyed *et al.,* (2014). Signals can have a broad dynamic series, so PSNR is basically measured in decibel (db), which is a logarithmic scale. In this research the MSE was used to measure the robustness of the stego image. A bigger PSNR value specifies a better feature of the Steganography algorithm used. The Human Visual System (HVS) would not be able to discern the images with PSNR greater than 36 db, Seyyed *et al.,* (2014). The PSNR of an image can be calculated using the following formula on (11).

$$\text{PSNR} = 10\log_{10} \frac{Max^2}{MSE} db \qquad (11)$$

Where Max^2 is the maximum pixel intensity that exists in the cover image and the PSNR of the same image, baboon.jgp is 59.308508db. Thus the PSNR of the image for the proposed model falls within the approved value range and proves that the Image quality is conserved at commendable level. Similarly, a high PSNR value is necessary in order to prevent the Stego image to be recognized by intruders that crawl in across the network.

4.) Results of the prototype system with other Images

The proposed model was used on other images such as lena.jgp and pepper.jpg apart from baboon.jpg. The results are shown in table 1 and 2 respectively. Table 1 shows the undetectability of the proposed model with value falling within the standard range for measuring it. Also, Table 2 demonstrates robustness of the proposed system with values falling within the specified standard range. This conserves the quality of the proposed system. Similarly, Figure 5 and 6 shows the respective graphs for the MSE and PSNR for the proposed model.

Table1: Comparison of Mean Square Error (undetectability) of the proposed model with the existing model based on different images

S/No	Name of Image	Image	Image Size (bits)	Mean Square Error	
				Proposed model	Existing model
1.	Baboon.jpg		512*512	0.0762	N/A
2.	Lena.jpg		512*512	0.0794	N/A
3.	Peppers.jpg		512*512	0.0790	N/A

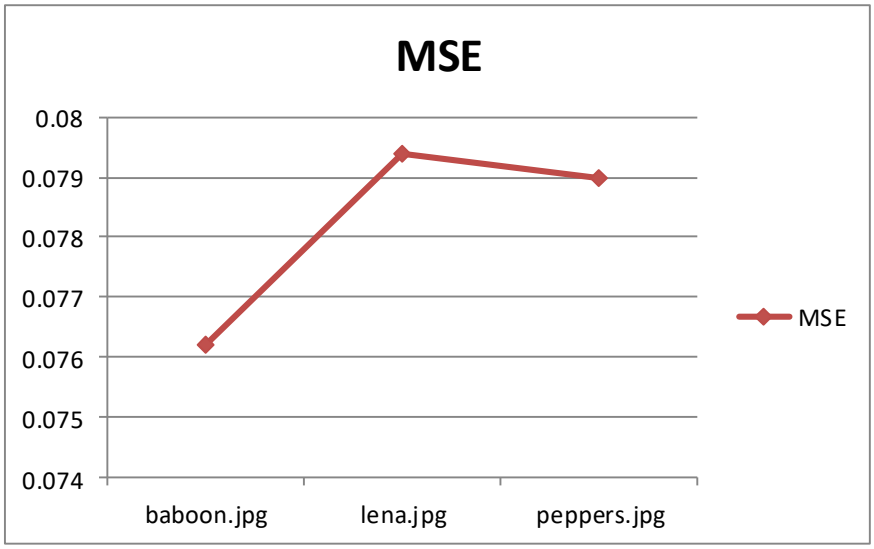


Figure 5: Mean Square Error of the proposed model

Table2: Comparison of Peak Signal-to-Noise Ratio (Robust) of the proposed model with the existing model

S/No	Name of Image	Image	Image Size (bits)	PSNR (db)	
				Proposed model	Existing model
1.	Baboon.jpg		512*512	59.309	N/A
2.	Lena.jpg		512*512	59.134	N/A
3.	Peppers.jpg		512*512	59.157	N/A

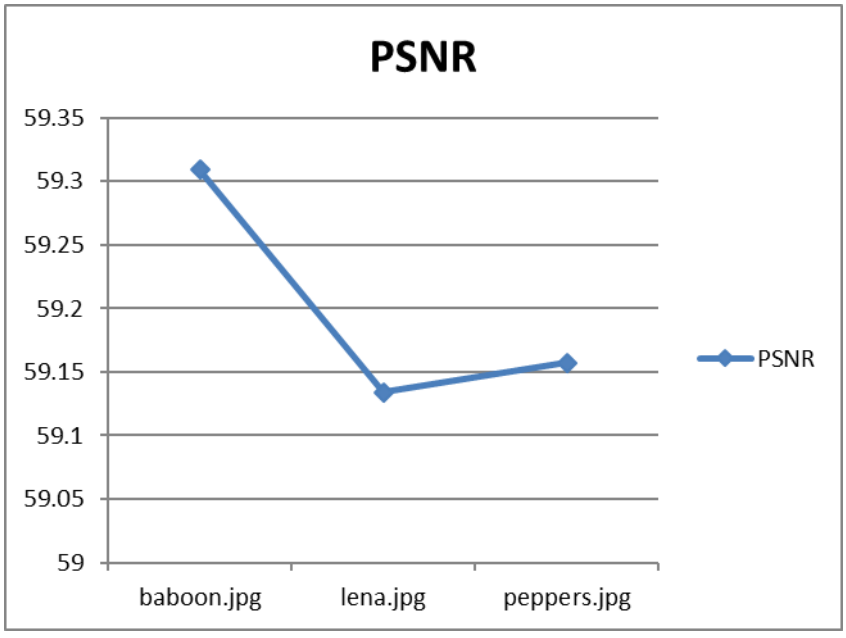


Figure 6: Peak Signal Noise Ratio of the proposed system

5. Discussion

Since the network is usually porous to attacks such as data leakage (sniffing, spoofing and malicious attack) user attributes are hereby endangered. The proposed model has been designed to ensure the security of user's attributes during transmission over the Network. The results of the proposed system have shown that the proposed model have performed more effectively and stronger. The proposed system performance has been evaluated with the performance parameters: Mean Squared Error (MSE) with value of 0.076248 for undetectability and Peak signal to noise ratio (PSNR) with value of 59.308508db for robustness. The performance has shown that the proposed system is undetectable, robust and effective for the security of the user's attributes. The proposed system has been tested on other images and the results have proved the proposed system strong and effective.

VI CONCLUSION

The paper presented an Enhanced PII Privacy Protection solution (using Advanced Encryption Standard AES-128 and Discrete Cosine Transform Modulus Three (DCT-M3) Steganography techniques) for protecting user's attributes from being leaked when transmitted and stored on the cloud. The supremacy of the proposed system over the existing system was also measured based on the encryption techniques used, undetectability and robustness of the Stego image. The result showed that the proposed system is undetectable, robust and effective for the security of the user's attributes on the cloud. Also the proposed system has been tested on other images and the results have proved the proposed system strong and effective for securing user's attributes.

REFERENCES

M. M. Abur, S. B. Junaidu, S. Danjuma, S. Arlis, R. Ritonga, T. Herawan (2018): Towards a Privacy Mechanism for Preventing Malicious Collusion of Multiple Service Providers (SPs) on the Cloud. In: V. Bhateja, B. Nguyen, N. Nguyen, S. Satapathy, Le DN. (eds) Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing, Singapore: Springer, vol 672.

M. M. Abur, O. S. Adewale & S. B. Junaidu, (2015): Cloud Computing Challenges: A review on Security and Privacy issues.Proceedings of the ACM International Conference on Computer Science Research and Innovations (CoSRI), Ibadan pp. 89-92.

M. M. Abur, S. B.Junaidu, A. A. Obiniyi and S. E. Abdullahi (2018) "Privacy Protection and Collusion Avoidance Solution for Cloud Computing Users", 1st International Conference on Education and Development (ITED 2018), Base University, Abuja

Y. A. Aldeen, M. Salleh & M. Abdur Razzaque, (2015): "A Survey Paper on Privacy Issue in Cloud Computing". *Research Journal of Applied Sciences, Engineering and Technology*, 10 (3): 328-337.

N. Aleisa (2015): A comparison of the 3DES and AES encryption standards. *International Journal of Security and its Applications* 9(7):241-246 http://dx.doi.org/10.14257/ijsia.2015.9.7.21.

P. N. Asha, T. Mahalakshmi, S. Archana and S. C. Lingareddy, (2016): Wireless Sensor Networks: A Survey on Security Threats Issues and Challenges. *International Journal of Computer Science and Mobile Computing*, 5(5), 249-267

Attaby A. A., Mursi Ahmed F. and Alsammak A. K., (2017) Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3. Ain Shams Engineering Journal http://dx.doi.org/10.1016/j.asej.2017.02.003

Chadwick D. W. (n. d.). Federated Identity Management: Computer Laboratory, University of Kent, Canterbury, CT2, &NF, UK.

Chen D. & Zhao H. (2012): Data Security and Privacy Protection Issues in Cloud Computing. *Proc. of the 1st International conference on Computer Science and Electronics Engineering*, Hangzhou China. Doi: 10.1036/0071393722.

Cloud Security Alliance (CSA). 2013: The Nine Notorious Threats. Top threats working group.

Cloud Security Alliance (CSA). 2016: The Treacherous 12 - Cloud Computing Top Threats

Hacker News (2017): Researchers Crack 1024-bit RSA Encryption in GnuPG Crypto Library. Retrieved July 3, 2017 from wiki: https://thehackernews.com/2017/07/gnupg-libgcrypt-rsa-encryption.html

S., Hemalatha, A. U. Dinesh, A. Renuka, & P. R. Kamath (2013). A Secure and High Capacity Image Steganography Technique. Signal & Image Processing: An *International Journal (SIPIJ)* 4(1), 83-89.

N. P. Kamdar, D. G. Kamdar, D. N. khandhar, (2013). Performance Evaluation of LSB based Steganography for optimization of PSNR and MSE *Journal of Information, Knowledge and Research in Electronics and Communication Engineering* 2(2), 505-509.

Kaminsky A., Kurdziel M. & Radziszowski S. (2010). An overview of cryptanalysis research for the advanced encryption standard (AES). Military Communications Conference (MILCOM), San Jose, USA. Pp1-8.

Y. Kumar, R. Munjal and H. Sharma, (2011) Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures. *International Journal of Computer Science and Management Studies (IJCSMS)* 11(3), 60-63.

M. A. P. Leandro, T. J. Nascimento, D. Santos, C. M. Westphall & C. B. Westphall (2014). Multi-Tenancy Authorization System with Federated Identity for Cloud-Based Environments Using Shibboleth. *In proceeding of the Eleventh International Conference on Networks* (NetWare2014), Lisbon, Portugal. pp. 42-67.

U. Lokhande and A. K. Gulve (2014): Steganography using Cryptography and Pseudo random numbers. *International Journal of Computer Applications*, 96 (19), 41-45.

T. Orawiwattanakul, K. Yamaji, M. Nakamura, T. Kataoka & N. Sonehara (2010): "User-controlled privacy protection with attribute-filther mechanism for a Federated SSO environment using Shibboleth," in P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), International Conference on IEEE, pp.243-249.

A. S. Seyyed & N. Ivanov (2014). Statistical Image Classification for Image Steganographic Techniques I.J. Image, Graphics and Signal Processing, 8, 19-24 DOI: 10.5815/ijigsp.2014.08.03

J. Song, K. Lee, and H. Lee, (2014). Biclique Cryptanalysis on the Full Crypton-256 and mCrypton-128. *Journal of Applied Mathematics*. 2014, 1-10, http://dx.doi.org/10.1155/2014/529736.

S. Suriadi, E. Foo and A. Josang (2007). A User-Centric Federated Single-On System. IFIP International Conference on Network and Parallel Computing Workshops.

R. Smith: Understanding encryption and cryptography basics (2003) Retrieved August 15, 2018 from wiki https://searchsecurity.techtarget.com/Understanding-encryption-and-cryptography-basics

SWITCH, (2010). "uapprove - user consent module for shibboleth identity providers," retrieved: [Online]. Retrieved from: https://www.switch.ch/aai/support/tools/uApprove.html/03/03/2016

A. M. Teena and M. Aaramuthan (2017): Federated Cloud Identity Management: A Study on Privacy Tactics, Tools and Technologies. Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, 19(6), 34-40.

R. Tripathi & S. Agrawal (2014). Comparative Study of Symmetric and Asymmetric Cryptography Techniques. *International Journal of Advance Foundation and Research in Computer* (IJAFRC) 1(6), 68-76.

R. Weingartner, C. M. Westphall, (2014) "Enhancing privacy on identity providers", Emerging Security Information Systems and Technologies (SECURWARE). The *Eighth International Conference* Lisbon, Portugal pp. 1-7.

M. Zhou, R. Zhang, W. Xie, W. Quian & A. Zhou, (2010) Security and Privacy in cloud: Survey. In Proc. Of the 6Th *International Conference on Semantics, Knowledge and Grids, IEEE*. Pages 105-112.