An Enhanced Data Integrity Model In Mobile Cloud Environment Using Digital Signature Algorithm And Robust Reversible Watermarking

Boukari Souley, Ismail Abdulkarim Adamu

Abstract: the increase use of hand held devices such as smart phones to access multimedia content in the cloud is increasing with rise and growth in information technology. Mobile cloud computing is increasingly used today because it allows users to have access to variety of resources in the cloud such as image, video, audio and software applications with minimal usage of their inbuilt resources such as storage memory by using the one available in the cloud. The major challenge faced with mobile cloud computing is security. Watermarking and digital signature are some techniques used to provide security and authentication on user data in the cloud. Watermarking is a technique used to embed digital data within a multimedia content such as image, video or audio in order to prevent authorized access to those content by intruders whereas, digital signature is used to identify and verify user data when accessed. In this work, we implemented digital signature and robust reversible image watermarking in order enhance mobile cloud computing security and integrity of data by providing double authentication techniques. The results obtained show the effectiveness of combining the two techniques, robust reversible watermarking and digital signature by providing strong authentication to ensures data integrity and extract the original content watermarked without changes.

Index Terms: Cloud computing, mobile computing, Digital signature and Digital Watermarking

1 INTRODUCTION

The use of mobile device to access and share multimedia content such as images, video, download of software applications, pay online bills and communicate on the cloud over the internet is increasing with the drastic growth in multimedia technology [1]. However, the inefficiency of the mobile devices to hold and handle large size of data due to its limited storage capacity and limited battery life, the need to move and store the multimedia data on the cloud becomes necessary to the users [22], [13], [7], [14]. Mobile cloud computing embeds the component of mobile networks and cloud computing to effectively serve it users. The fascinating thing about mobile cloud computing is that both data processing and storage take places outside of the mobile devices [15], [24]. But, in order to communicate efficiently with the multimedia contents stored on the cloud over a communication network, the need to secure and protect these contents becomes paramount important and concern to the users since the data is vulnerable to intruders attack [8]. Cloud computing provides a lot of shared configurable resources to the user payable on demand according to the size of the resources utilized by the user [12], [4]. The resources provided by cloud computing include software applications, servers, network, storage space, and computer processing power [1], [9]). All the services and resources provided by cloud computing are managed and handled by third party [19].

As a result, the need to protect user data when utilizing the cloud resource becomes very important in order to protect it against unauthorized access or malicious users [20]. This is because user data on the cloud are sensitive and private. Furthermore, any illegal access to these data may lead to privacy violation, leakage or damage of sensitive data. To achieve data confidentiality, integrity and availability of the multimedia data in the cloud the use of security techniques such as cryptography, steganography and watermarking are employed to protect the data from illegal access by malicious users and hackers [2]. The use of all these security techniques individually to provide security to the data in cloud is good but the combination of each of the two techniques in terms of having a hybrid security techniques provides a more strong security to the data in cloud during communication and storage [5], [23]. Several techniques have been employed by different researchers to address security challenge in mobile cloud computing and provide solution to these challenges. However, in this work we employed the use of Digital signature algorithm and robust reversible watermarking technique to improve the integrity of data stored in the cloud during communication and download by users and guarantee data integrity by providing double authentication on the multimedia data to be accessed.

2 LITERATURE REVIEW

2.1 Digital Signature Algorithm (DSA)

Digital signature algorithm is an asymmetric encryption algorithm also known as public key encryption algorithm. It is used in today's modern computing in various ways such as software distribution and financial transactions to verify the identity of a message or transaction in order to ensure that it is from a valid source. The digital signature is just like the hand writing signature but when properly implemented becomes more difficult to forge [3]. Digital signature algorithm uses two keys, private and public keys. The public key is used to verify the document which is known by every user while the private key is used to generate the signature which can only be done by the valid user. Furthermore, the existence of the private key is difficult to be discovered from the public key [16]. Digital

- Boukari Souley , Supervisor, Department of Mathematical Sciences, Abubakar Tafawa Balewa University Bauchi, Nigeria. Email: bsouley2001@yahoo.com
- Ismail Abdulkarim Adamu is currently pursuing his Master Degree in Computer science, Department of mathematical science, Abubakar Tafawa Balewa University (ATBU), Bauchi, Nigeria. Email: psalmlisticforlife@yahoo.com

signature is used to detect message or data alteration by the recipient. The digitally signed document whispered a signal to the recipient that the message was sent from a valid source. It is used as a non-repudiation communication medium because the person that sent the message cannot deny that he signed the message in the future. Digital signature uses a specific hash function such as SHA-1 and SHA-2 to generate its hash value unlike RSA digital signature in which any hash function can be used to generate the hash value. The process of generating Digital signature as described in [16] is illustrated as follows:

Key Generation Phase

In the key generation phase, both the public and private key are generated. Where, the private key is used for signing the message and the public key is used for verifying the message. The algorithm parameters (p, q, g) for key generations are:

I. Per user keys:

Public key: y

Private Key: x

II. Signature Generation Phase

The signature phase consists of hashing the message using SHA-1 or SHA-2 hash function to create a hash value. After which, the generated hash value is signed using the generated private key. The signature is (r, s). Where r and s and computed numbers used to sign the message M.

III. Verification Phase

The verification phase involves comparing the hash value with the original content to see if they matched each other. The signature is valid if v = r. where v is the original value and r is the signed value.

IV. Correctness of the algorithm:

The signature scheme is correct in the sense that the verifier will always accept genuine signatures. Figure1 and 2 below, describe the way digital signature is created and verified:

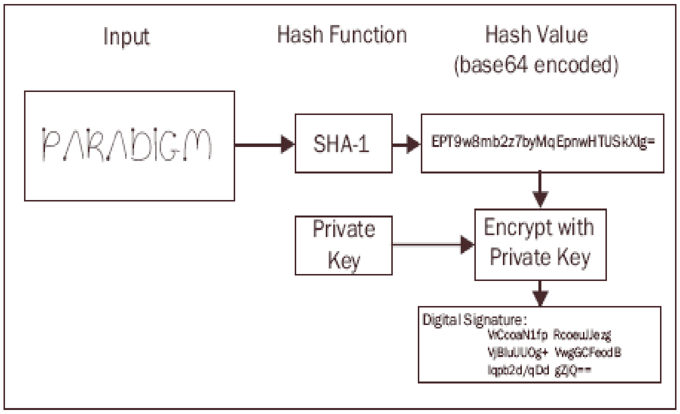

Figure1. *Creating Digital Signature as In [21]*

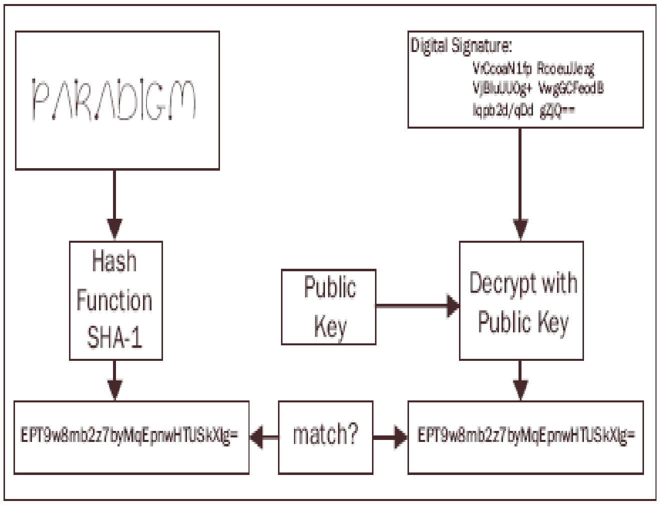

Figure2: *Verifying Hash Value as in [21]*

Considering the above figure2, if the hash value generated matches the extracted content then, the message was not altered in the process of the communication and its integrity is maintained. But, if the hash value generated did not match the extracted content, it can be suspected that the content has been altered with during the transfer and so the integrity of the message cannot be validated.

2.2 Digital Watermarking

Digital watermarking is a security technology that embeds signals and Secret information called watermarked within digital media content such as image, audio and video. It ensures security, privacy and ownership authentication of the media content being watermarked [10], [17]. The idea behind watermarking is related to steganography. Steganography is defined as secret writing, which is used for secret communication in long time history [6]. Digital watermarking is used to hide un-perceptible label or mark on a media content which could later be detected and extracted by an authorized user in order to protect product copyright or media data integrity. There are two types of digital watermarking techniques, the visible and invisible. The visible watermarking technique is the one we can see and notice on product or logo on our television. While, the invisible watermarked is the one that is un-perceptible by human eyes. The invisible watermarking is categorized into fragile and robust watermarking. The fragile watermarking is used to verify the integrity of a media content because any slight change made on fragile watermarking media content create some changes to the original Meanwhile, the robust watermarking technique is used to authenticate the proof of ownership of the said media content [6], [18]. The advantage of the robust reversible watermarking techniques is that it allows the extraction of the full content of the media content being watermarked without affecting it [11]. The process involved in digital watermarking system is described in the figure3 below:

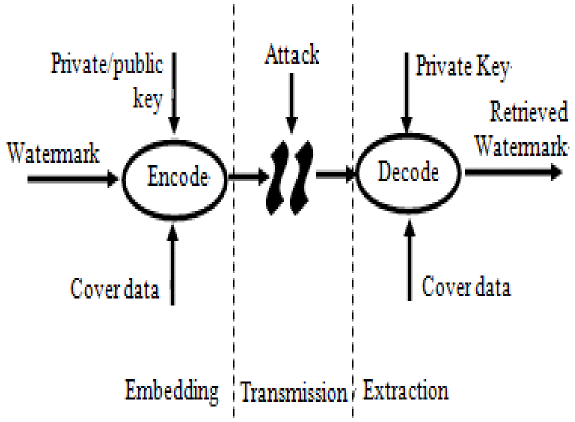

Figure3: *Digital Watermarking system as described in [18]*

2.3 Related Works

[22] Proposed a solution to the security threat and fear faced by cloud users using robust reversible watermarking and RSA digital signature. It was stated in their work that due to the limitation of the traditional watermarking technique in distorting the water marked objects and not able to extract it full content back the need to use the robust reversible watermarking in protecting data on the cloud. Two security methods reversible watermarking and RSA digital signature were used to improve confidentiality and cloud security level between mobile user and mobile cloud environment when sending information to the mobile cloud service providers in their work. Due to rise in technology and increase transfer of multimedia content son the cloud using mobile devices [11] proposed an enhanced security technique to have a secure communication of data in the cloud over the internet using RSA digital signature with robust reversible watermarking algorithm. In their work, RSA was used to encrypt and decrypt the multimedia content using its public and private keys and hash function was used to reduce the size of the multimedia content to any size called hash value and to also, sign the multimedia content for authentication and validation. In order to prevent the security challenge of insider attack on user data in the cloud by cloud service provider administrator [13] proposed an additional layer of security on user data on the cloud using Image Steganography. In their work, they provide security on data by hiding the data in an image cover with secret key that can be used to access the data in the cover in order to achieve data confidentiality. The widespread use of mobile phones and other social network devices has lead to an increase in the use of internet application and bandwith which is gradually exceeding the 3G capability as a result caused the reduction in speed and services of the internet provided in the cloud. To address the issue, [7] proposed an improved identity management protocol system. Their proposed work aimed to minimized the traffic load faced in mobile computing and also provide unique user identification.

3 Methodology

In this model we proposed the use of DSA and Reversible robust watermarking technique. The working procedure of DSA as described in [16] is illustrated below:

p = a prime modulus, where $2L-1 < p < 2L$ for $512 \le L \le 1024$ and L is a multiple of 64. So L will be one member of the set {512, 576, 640, 704, 768, 832, 896, 960, and 1024}

q = a prime divisor of p-1, where $2159 < q < 2160$

g = h (p-1)/ q mod p, where h is any integer with $1 < h < p - 1$such that h (p-1)/ q mod p > 1(g has order q mod p)

x = a randomly or pseudo randomly generated integer with $0 < x < q$

y = gx mod p →1

k = a randomly or pseudo randomly generated integer with $0 < k < q$

The parameters p, q, and g are made public. The users will have the private key, x, and the public key y. The parameters x and k are used for signature generation and must be kept private and k will be randomly or pseudo randomly generated for each signature. This part seems to be straightforward so far. The signature of the message M will be a pair of the numbers r and s which will be computed from the following equations.

r = (gk mod p) mod q →2

s = (k-1(SHA (M) + xr)) mod q →3

K-1 is the multiplicative inverse of k (mod q).

The value of SHA (M) is a 160-bit string which is converted into signature is sent to the verifier.

Verification:

Before getting the digitally signed message the receiver must know the parameters p, q, g, and the sender's public key y. We will let M′, r′, s′ be the received versions of M, r, and s. To verify the signature the verifying program must check to see that $0 < r' < q$ and $0 < s' < q$ and if either fails the signature should be rejected. If both of the conditions are satisfied then we will compute

w = (s′)-1 mod q

u1 = ((SHA (M′)) w) mod q

u2 = ((r′) w) mod q

v = (((g) u1 (y) u2) mod p) mod q

Then if v = r′ then the signature is valid and if not then it can be assumed that the data may have been changed or the message was sent by an impostor.

3.1 PROPOSED WORK

In this work we proposed to improve mobile cloud security using Digital signature algorithm and robust reversible watermarking. The digital signature algorithm will be used to sign the digital data in the cloud watermarked with robust reversible image watermarking technique. The reason behind this method is to guarantee the integrity of digital data being watermarked in the cloud by providing double authentication procedure on the digital data.

3.2 WORKING PROCEDURE OF THE PROPOSED SYSTEM

Encryption Phase

1. Create message
2. Hash the message using SHA-1or SHA-2 hash function
3. Sign the message using DSA private key
4. Watermark the message using robust reversible image watermarking

Decryption Phase

1. Authenticate and extract the watermarked message
2. Verify the message using DSA public key
3. Reverse the hash message
4. Have access to the original message.

3.3 ARCHITECTURE OF THE PROPOSED SYSTEM

The architecture of the proposed system is shown in the figure4 below:

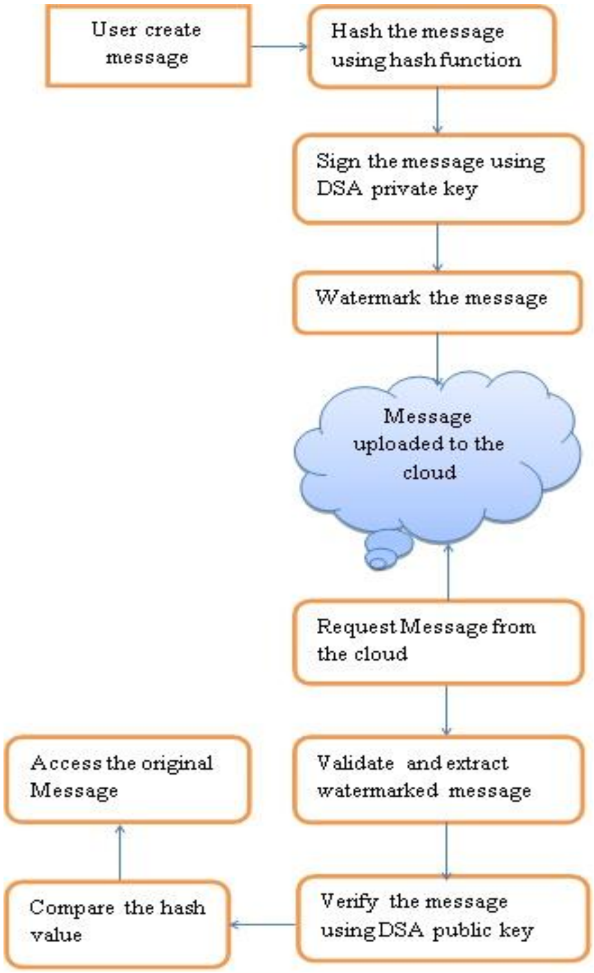
User create message
Hash the message using hash function
Sign the message using DSA private key
Watermark the message
Message uploaded to the cloud
Request Message from the cloud
Access the original Message
Validate and extract watermarked message
Compare the hash value
Verify the message using DSA public key

Figure 4: *Architecture of the proposed system*

4 EXPERIMENTAL RESULT

This model was implemented using java programing language on HP Pavilion 15 notebook computer system. The result in table1 below: shows the analysis performed using image of different pixel size and kilobyte size used to watermark the digital content. The result was used to verify the kilobyte size and the pixel size of the image after being watermarked. The results in the table1 show that, the image still maintains their pixel size and color quality after being embedded with a digital data but the difference is the kilobyte size of the image that changed because of the size of the digital data watermarked in the image.

Table1: *Image with different pixel and size*

Orinal Image	Watermarked Image with DSA
 259X195 Pixel, Size: 6.88kb	 259X194 Pixel, Size: 147kb
 284X177 Pixel, Size: 8.88kb	 284X177 Pixel, Size:147kb
 300X1648Pixel, Size:14.3kb	 300X168 Pixel, Size: 147
 251X201 Pixel, Size: 8.74kb	 251X201 Pixel, Size: 148kb

The result of the proposed system, provide a strong verification and validation of user and data in the cloud in order to ascertain the integrity of the data. The system is considered to provide a more validation technique using a non-repudiation measure in order to ensure that, the accessed message on the cloud was not modified or changed by intruders when accessed by the intended user. The proposed system guarantees that, once there is a change in the pixel size and distortion in color quality of the image when accessed by the user, then, the integrity of the message will not be accepted because the message must have been tempered with before being accessed.

6 CONCLUSION

The use of mobile devices to access multimedia data such as image, video, audio and software application in the cloud is increasing tremendously with the day to day growth in information technology known as mobile computing. The major challenge with mobile computing is security; where by the integrity of the data being requested and validity of the user accessing the data is always not guarantee. In this work, we proposed a security measure in order to overcome such challenge using Digital signature and robust reversible image watermarking technique. The adopted technique ensures the integrity of data to be accessed on the cloud by providing double authentication on the data. Even though, the procedure adopted in this work, increased the computational complexity on mobile cloud computing, it provides a strong authentication medium for the media data and enhanced its integrity. In the future, we will implement this same technique on video watermarking technique and evaluate the performance of the system with other proposed techniques by other researchers.

REFERENCE

[1] Anuradha, A., & Pandit, H. .. (2017). Biometric Based Security Model for Cloud Computing Using Image Steganography. International Journal of Advanced Research in Computer Science and Software Engineering, 7(1), 42-51.

[2] Apau, R., & Adomako, C. (2017). Design of Image Steganography based on RSA Algorithm and LSB Insertion for Android Smartphones. International Journal of Computer Applications, 164(1), 13-22.

[3] Bhosale, P., Deshmukh, P., Dimbar, G., & Deshpande, A. (2012). Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption. International Journal of Engineering Research & Technology, 1(8), 1-8.

[4] Chintawar, N. N., Gajare, J. S., Fatak, V. S., Shinde, S. S., & Virkar, G. (2016). Enhancing Cloud Data Security Using Elliptical Curve Cryptography. International Journal of Advanced Research in Computer and Communication Engineering, 5(3), 94-97.

[5] Dhamija, A., & Dhaka, V. (2015). A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration. International Conference on Green Computing and Internet of Things (pp. 346-351). IEEE.

[6] Guru, J., & Damecha, H. (2014). A Review of Watermarking Algorithms for Digital Image. International Journal of Innovative Research in Computer and Communication Engineering, 2(9), 5071-5078.

[7] Hadole, P. .., Rohankar, J., Priyanka, & Katara, A. (2014). Development of Secure Mobile Cloud Computing Using Improved Identity Management Protocol. International Journal on Recent and Innovation Trends in Computing and Communication, 2(3), 645-650.

[8] Honggang, W., Wu, S. W., Chen, M., & Wang, W. W. (2014). Security Protection between Users and the Mobile Media Cloud. IEEE Communication Magazine, 52(3), 73-79.

[9] Kanthale, A., & Potdar, .. P. (2016). Survey on Cloud Computing Security Algorithms. International Journal of Science and Research, 5(4), 1865-1867.

[10] Kaur, M., Baghla, S., & Kumar, S. (2015). A Review on Watermarking of Digital Images. International Journal of Advances in Science Engineering and Technology, 3(3), 149-153.

[11] Monisha, M., & Chidambaram, S. (2017). Enhanced Data Security using RSA Digital Signature with Robust Reversible Watermarking Algorithm in Cloud Environment. Internation al Journal of Electroni cs & Co mmuni cation Techno logy, 8(1), 20-24.

[12] Neha, M. K. (2016). Enhanced Security using Hybrid Encryption Algorithm. International Journal of Innovative Research in Computer and Communication Engineering, 4(7), 13001-13007.

[13] Reza, H., & Sonawane, M. (2016). Enhancing Mobile Cloud Computing Security Using Steganography. Journal of Information Security, 245-259.

[14] Sagg, K., & Bhatia, S. .. (2015). A Review on Mobile Cloud Computing: Issues, Challenges and Solutions. International Journal of Advanced Research in Computer and Communication Engineering, 4(6), 29-34.

[15] Shamim, S. M., Sarker, A., & Bahar, A. N. (2015). A Review on Mobile Cloud Computing. International Journal of Computer Applications, 113(16), 4-9.

[16] Shiny, R., Shaji, R., & Jayan, J. (2015). Signature Based Data Auditing Under Mobile Cloud System. Proceedings of 2015 Global Conference on Communication Technologies (pp. 565-570). IEE.

[17] Singh, P., & Chadha, R. S. (2013). A Survey of Digital Watermarking Techniques, Applications and Attacks. International Journal of Engineering and Innovative Technology, 2(9), 165-175.

[18] Song, C., Sudirman, S., & Merabti, M. (2009). Recent Advances and Classification of Watermarking Techniques in Digital Images. Proceedings of the 10th of Post Graduate Network Symposium, (pp. 283–288).

[19] Suganya, V., & Shanthi, A. L. (2015). Mobile Cloud Computing Perspectives and Challenges. International Journal of Innovative Research in Advanced Engineering, 7(2), 71-76.

[20] Tawalbeh, L., Darwazeh, S. N., Al-Qassas, S., & AlDosari, F. (2015). A Secure Cloud Computing Model based on Data Classification. First International Workshop on Mobile Cloud Computing Systems, Management, and Security (pp. 1153-1158). Elsevier B.V.

[21] Thomas, S. (2008, January 02). Paradigm . Retrieved September 05, 2017, from Workbook on Digital Private Papers : http://www.paradigm.ac.uk

[22] Uma, B., & Sumathi, S. (2017). An Efficient Approach for Data Security in Cloud Environment using Watermarking Technique and RSA Digital Signatures. International Research Journal of Engineering and Technology, 4(2), 1817-1821.

[23] Varsha, & rRajender, C. S. (2015). Data, Hiding Using Steganography and Cryptography. International Journal of Computer Science and Mobile Computing, 4(4), 802-805.

[24] Yadav, S. D., & Doke, K. (2016). Mobile Cloud Computing Issues and Solution Framework. International Research Journal of Engineering and Technology, 3(11), 1115-1118.