International Journal of Scientific Research and Engineering Development-– Volume 3 Issue 2, Mar-Apr 2020

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

A Survey Paper on "Intermediate Layer Security on Multimedia in 5G Technology using Robust Watermarking with RSA Signatures"

Nikita Chhabada[1], Niraj Kumar sahu[2]

[1]M Tech Scholar Computer Technology (Multimedia)Kalinga University, Raipur (CG) India, 14nikitachhabada@gmail.com

[2]Asstt. Professor, CSE Department, Kalinga University, Raipur (CG) India, nirajsahu86@gmail.com

Abstract-

The increase use of hand held devices consisting of clever phones to get admission to multimedia content in the cloud is increasing with upward push and growth in statistics technology. Mobile cloud computing is increasingly used today due to the fact it allows users to have get right of entry to to type of assets in the cloud such as image, video, audio and software packages with minimum usage of their inbuilt resources such as storage memory by using the usage of the one available in the cloud. The major mission confronted with cellular cloud computing is protection. Watermarking and digital signature are some strategies used to provide protection and authentication on user records inside the cloud. Watermarking is a method used to embed virtual facts inside a multimedia content along with photograph, video or audio in order to save you authorized get admission to to the ones content material through intruders whereas, digital signature is used to identify and verify user records when accessed. In this work, we implemented virtual signature and strong reversible picture watermarking in order decorate mobile cloud computing safety and integrity of facts by using presenting double authentication strategies. The consequences obtained display the effectiveness of combining the two techniques, strong reversible watermarking and digital signature by supplying sturdy authentication to ensures records integrity and extract the authentic content material watermarked without changes.

Keywords- Cloud computing, mobile computing, Digital signature and Digital Watermarking.

I .INTRODUCTION

The development of the Fifth Generation (5G) wi-fi networks is gaining momentum to connect nearly all elements of life via the community with tons higher speed, very low latency and ubiquitous connectivity. Due to its essential position in our lives, the community ought to stable its customers, components, and services. The protection threat panorama of 5G has grown enormously because of the unprecedented increase in kinds of services and within the wide variety of devices. 5G will provide ubiquitous broadband services, enable connectivity of large wide variety of gadgets within the shape IoT, and entertain customers and gadgets with high mobility in an ultra dependable and affordable way. The improvement in the direction of IP-based totally communication in 4G has already helped expand new enterprise opportunities; however, 5G is considered a new environment connecting nearly all factors of the society; vehicles, domestic appliances, fitness care, industry, businesses, etc., to the network. This development, however, will introduce a brand new array of threats and protection vulnerabilities as a way to pose a major task to each gift and future networks. With 5G technology cellular gadgets can have restrained garage and concurrently it cannot procedure other multimedia (video) application because of small RAM. Therefore we are the usage of cloud for storing our information. But we can't guarantee the safety of our stored information in the cloud. The preservation group of cloud surroundings may offer copyright protection but there's a threat of stealing/hacking our very own confidential facts by them. Robust reversible Robust watermarking and RSA digital signature can solve this problem. These two strategies have been used after the encryption algorithm and is used to guard the records in cellular cloud environment. It offers higher safety performance, boom the original records exceptional and confidentiality. A denial of carrier assault (DOS) is any form of attack on a networking shape to disable a server from servicing its clients. Attacks variety from sending thousands and thousands of requests to a server in an try to gradual it down, flooding a server with large packets of invalid records, to sending requests with an invalid or spoofed IP address.

Cross-layer security a unified framework is needed to coordinate one-of-a-kind safety strategies for every security layer, together with programs or the IoT. In exceptional community layer a couple of security alternatives are available for video. By the usage of RSA virtual signature we will authenticate and secure lowest layer from denial of carrier attack. The signature will include public key with encrypted video statistics using

 ©IJSRED:All Rights are Reserved

RSA virtual signature and Robust Watermarking. The receiver have to have the confidence that the public key belongs to the originator otherwise any substitution by a duplicate public key would permit a "man inside the middle attack" to negotiate the data. One mechanism for mentioning the authority of the relationship most of the originator and their public key rely upon certificates. Methods will decorate the video statistics safety between mobile user and mobile cloud surroundings. The combination of RSA digital signature and Robust Reversible watermarking is used to enhance the statistics confidentiality and protection for sending information to the cell cloud carriers. The rapid development of multimedia packages such as digital publishing, digitized photos and motion pictures etc., results in the requirement of greater storage in mobile phones. In order to avoid this problem, we use cloud for storing our information. Data (wi-fi multimedia applications) access over wireless networks are much faster. But we aren't assured of information protection. So the RSA virtual signature and Robust Reversible watermarking is used to remedy the above referred to problem. Data safety in cellular cloud environment has to make certain the secured and dependable multimedia statistics transmissions between cell customers and the cell cloud. However, the mobile cloud is maintained via 0.33 parties together with cell cloud service providers and we can not be accept as true with them in any respect time. We will have contracts between customers and cellular cloud provider carriers in order to make sure statistics protection. This get up some ability risks, together with security attacks or misconduct of the cellular cloud provider. But customers can agree with themselves instead than cell cloud security providers. Our design is consumer-oriented, and permits customers to defend their records's safety and privacy. The receiver should have the self assurance that the general public key belongs to the originator in any other case any substitution by a duplicate public key would permit a "man inside the middle attack" to negotiate the facts. One mechanism for mentioning the authority of the relationship a few of the originator and their public key rely on certificates. They are issued by trusted authorities who generate and digitally sign certificates needful entities (consisting of people and organisations) to their public keys. Unfortunately, mechanisms permit us to accept as true with the signature of the relied on authority on the certificate. If a digitally signed report is despatched over internet, the sent file and the received document each are genuine. Cryptography is a way of storing and transmitting facts in a particular shape in order that best for those it's miles contemplated can read or system it. This can be done correctly in clever phones. It is the technique of encoding the content in order that for whom it's miles intended best can examine it. Digital signature is a code that is generated by means of public key encryption and is used to authenticate and confirm the document despatched over a network. It is also used to confirm the sender's identity. Today digital signatures are being utilized in many specific forms. Some use a literal signature of someone on display and detect it the use of photo processing strategies. This isn't always very reliable system as home made signature might slightly fluctuate from each other and result in forbidden get right of entry to. Also another way is sporting a small USB tool containing our digital signature and connecting the device to machine to embed the virtual signature. The issue for this is that our signature completely depends upon the device we carry with us. If the tool itself is stolen or misplaced, we might land up in trouble. Moreover, the device is expensive. The most secured way for implementation of digital signatures considered on this date is biometric signatures. But again, all the smart phones aren't provided with biometric safety systems. So on this paper we present a value effective, simple, accurate, particularly secured Digital Signature authentication and verification technique using clever phones. There are distinct survey papers that cover special elements of the cryptography technology. For example, in we observe about the existing strategies developed the use of cryptography. Also the advantages and downsides of these techniques are seen here. In , we see how a low cost digital signature can be developed and may anomalous behaviour within the device be identified. Moreover, paper shows us approach to use virtual signature structure that may be used for web-primarily based application. And paper tells us what the existing strategies of the usage of virtual signatures are in cell device systems.

II. BACKGROUND AND RELATED WORK

The Security is a major task for all the network environments. Image is one of the resources of sending information in all fields like medical image processing, networking, and in cloud environment also.

[1] Suthar et al. introduced an image security method in frequency domain known as mixed hybrid scheme. The method is used to detect the image tamper and also maintains image quality. The experimental results of the scheme represent that method is robust against the different attacks.

The proposed algorithm performs encryption of host image by having a combination of 2D Discrete wavelet transform (DWT), mid band -Discrete cosine transform and a secret key.

Localization of the tampered pixels blocks.

Estimation of the five significant bits from the tampered image pixels.

 ©IJSRED:All Rights are Reserved

The method is demonstrated that restoration is achieved by the presented method.

Private Key encryption based network security is discussed in Abusukhon and Talib. The method is described for data encryption among the text file transformation among the server and client machines. The possible key for the permutation helps in analysis of the algorithm.

The immune system based segmentation algorithm for infrared images is discussed in Fu et al. . A novel method is presented by the combination of segmentation and clonal selection algorithm to mitigate the segmentation thresholds.

[2] Singh et al A study on Residue Number System (RNS) and Data Encryption Standard (DES) based reversible watermarking method for image security is discussed. In authors work secret image was passed to the simple-DES based on key image and at last the encrypted image is obtained with the position matrix and watermark image. Later the watermarked image was subjected to RNS that gives the fully encrypted image. The decoding of the image is done by reversible watermarking.

[3] Gupta et al. illustrated an Embedded Zero tree Wavelet (EZW) compression and Chaos-based image security method. The EZW based method was used to achieve image security with compression while the Chaos method offers robustness in security along with mixing property. The EZW sequence is subjected to 2D data conversion and scrambling by Chaos method. The method out forms the more security.

[4] Honggang Wang,Shaoen Wu An active and passive approach is presented in Yanyan et al. to provide security protection for remote sensing images. A high quality of content protection mechanism was adapted to secure, store and transmission purpose. The encrypted image can be decrypted with the key.

The first stage of the proposed method is dividing the image into several sub blocks, and search fingerprinting areas which effects the image with less quality. Then apply DCT transformation to every blocks followed by encryption of DCT coefficients using content encryption scheme.

[5] Jagruti R. Mahajan, A concept of data hiding mechanism is introduced in the Mohan et al. to enhance the image security. The data hiding concept will offer the security and also recover the image with the efficient quality. In the concept of hiding will hide the some portion of the image and encrypt with the key. The hiding concept used in this is reversible that has got the higher capacity of data hiding.

[7] Zefreh et al. The content owner side image is encrypted by chaotic transposition algorithm. As a second level security data hider then hides some data into the encrypted image based on histogram modification by data hiding key. At the receiver end he needs two keys for decrypting it.

A recursive cellular automata substitution and parallelization concept approached in . The method is efficient in test analysis and computational aspects. The method was adopted for half portion of the image to encrypt the image while the half portion of the image mutually. The simulation results of the image concluded that performance in image security is improved.

[8] The related study for medical image security is carried out in Naveen et al. [20] by using the EZW and Chaos mechanism. The security for the digital medical data is much necessary as these data is transmitted among the hospitals and also for health insurance sectors. The enhancement in security by Chaos approach is more useful. By using the EZW approach, the 2D output sequence was converted to 2D and later chaos based scrambling mechanism is implemented in column and row manner. The method out forms with compression and extra security for the image.

[9] Dharini. A, R.M. Saranya Devi An image security and image authentication for the color image is presented in Shefali and Despande known as the Self-embedding mechanism. The method was of Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) combination which simulates the extra security.

[10] Manish gupta, Darpan Anand, This method is used for color images. The technique first converts the host image into YIQ color space followed DCT and DWT transforms.

The Reversible was watermarking, and Arnold's Cat Map approach is presented in Umamageswari and Suresh to provide the security for medical image transmission. In this region of interest and region of noninterest was defined with JPEG 2000 algorithm. The method provides the most secure mechanism in medical image security.

Another medical image security concept is discussed in Nabiyev et al. The survey the method medical image data during the data transmission and also rendered different watermarking techniques.

III. PROPOSED METHODOLOGY

In proposed methodology the improvement of the Fifth Generation (5G) wi-fi networks is gaining momentum to connect nearly all components of life via the community with much higher speed, very low latency and ubiquitous connectivity. Due to its critical function in our lives, the network need to stable its users, components, and offerings. The security hazard panorama of 5G has grown enormously due to the unprecedented increase in sorts of offerings and in the number of devices.

5G will offer ubiquitous broadband services, permit connectivity of huge quantity of gadgets inside the form IoT, and entertain users and devices with excessive mobility in an ultra dependable and low-priced way. The development toward IP-based verbal exchange in 4G has already helped broaden new commercial enterprise opportunities; however, 5G is considered a brand new ecosystem connecting nearly all aspects of the society; vehicles, domestic appliances, health

 ©IJSRED:All Rights are Reserved

care, industry, businesses, etc., to the network. This development, however, will introduce a new array of threats and security vulnerabilities so one can pose a major assignment to both gift and future networks. With 5G technology mobile gadgets may have confined storage and simultaneously it cannot method different multimedia (video) application due to small RAM. Therefore we are using cloud for storing our records. But we cannot assure the security of our stored facts within the cloud. The upkeep group of cloud environment may provide copyright protection but there may be a risk of stealing/hacking our own confidential information through them. Robust reversible Robust watermarking and RSA digital signature can remedy this problem. These two techniques have been used after the encryption algorithm and is used to defend the data in cellular cloud surroundings. It offers higher protection performance, boom the original data excellent and confidentiality. A denial of carrier attack (DOS) is any sort of assault on a networking structure to disable a server from servicing its clients. Attacks variety from sending thousands and thousands of requests to a server in an try to sluggish it down, flooding a server with huge packets of invalid information, to sending requests with an invalid or spoofed IP address. Cross-layer safety a unified framework is needed to coordinate distinct security techniques for every security layer, such as programs or the IoT. In extraordinary community layer more than one protection alternatives are to be had for video. By the use of RSA digital signature we can authenticate and steady lowest layer from denial of carrier assault. The signature will contain public key with encrypted video information the usage of RSA digital signature and Robust Watermarking. The receiver ought to have the self assurance that the general public key belongs to the originator in any other case any substitution by using a replica public key would permit a "man in the center assault" to negotiate the records. One mechanism for declaring the authority of the relationship the various originator and their public key depend on certificates. Methods will decorate the video statistics security between cellular user and mobile cloud environment. The mixture of RSA virtual signature and Robust Reversible watermarking is used to improve the data confidentiality and safety for sending information to the mobile cloud providers.

RSA and water marking techniques can provide very secure and encrypted data for any type of system. The algorithm always takes proper way to solve the security problem and after encrypting the text it provides a vice versa process to gather actual data which was encrypted before.

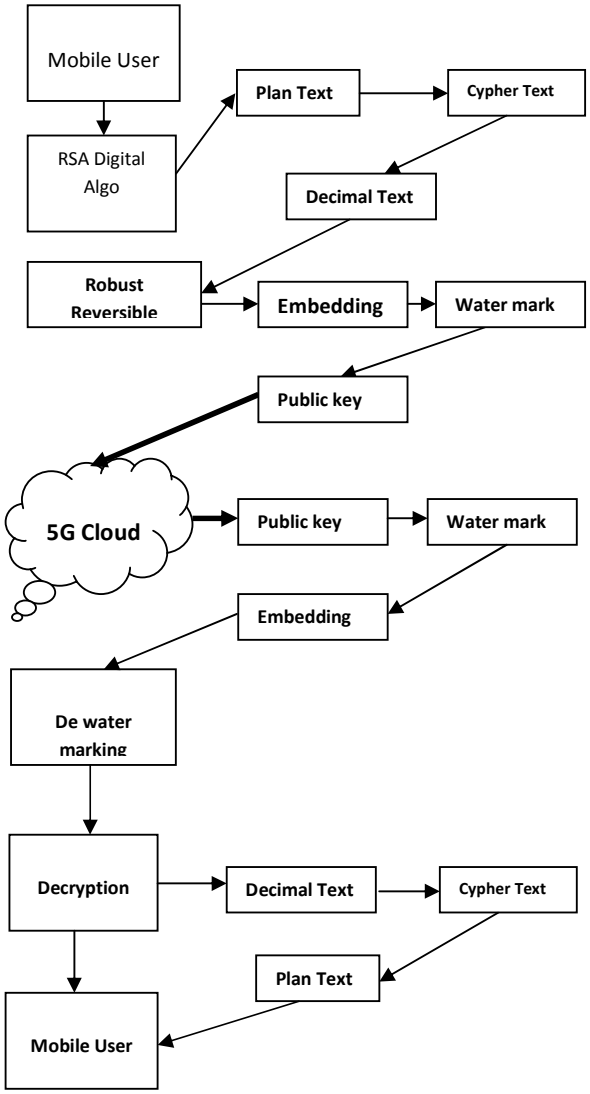

Fig: Block Diagram for 5G cloud Security modules

IV. RESULT AND ANALYSIS

In this section, we display the effectiveness of our proposed methodology. The simulation is achieved on MATLAB2012a & analysis of PSNR and robustness of picture. This technique is carried out to several pix having different varieties of pixels. The first parent in Table-1 is a 512X512 photograph which is encrypted and embedded the usage of 128 bytes of undeniable text and 128 bytes of original photo in our experiment. In the PSNR fee for the equal image is 34.1 dB. In our proposed technique, the performed PSNR price 43.626 dB. At the receiver side, information is extracted no longer with records loss. Other than this, PSNR values are calculated the use of different images having numerous pixel size.

V. CONCLUSION

In this paper, the proposed method has greater the facts safety between mobile person and mobile cloud environment. The mixture of RSA virtual signature and Robust Reversible watermarking is used to enhance the statistics confidentiality

 ©IJSRED:All Rights are Reserved

and security for sending facts to the cell cloud providers. Along with this, technology of an photograph key from the encrypted watermarked photo will increase the security. Surely the complexity of the system will increase but at the identical time an improved protection is achieved. Future scope is to check enforce the same set of rules on video and other multimedia contents. We also exchange the combination of encryption algorithms with different watermarking algorithms to improve the output message with none loss.

REFERENCES

[1] Deepika Verma, Er. Karan Mahajan,(December 2014), 'To Enhance Data Security in Cloud Computing using Combination of Encryption Algorithms', International Journal of Advances in Science and Technology (IJAST) ,Vol 2, Issue 4.

[2] Ankita Ojha, Tripti Sarema, Dr.Vineet Richariya, (May 2015),'An efficient approach of sensitivearea watermarking with encryptionsecurity', International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)Volume 4 Issue 5.

[3] Honggang Wang,Shaoen Wu, Min Chen Wei Wang, (March 2014)'Security protection between users and the mobile media cloud',IEEE communications magazine.

[4] Jagruti R. Mahajan, Nitin N. Patil, (2015) 'Alpha channel for integrity verification using digital signature on reversible watermarking QR', international conference on computing communication control and automation.

[5] A.Khan, A.Siddiqui, S.Munib, and S.A.Malik, (2014), 'A Recent Survey of Reversible Watermarking Techniques', DOI:10.1016/j.ins.2014.03.118, Information Sciences.

[6] Dharini. A, R.M. Saranya Devi, and I. Chandrasekhar, (Nov. 2014), 'Data Security for Cloud Computing Using RSA with Magic Square Algorithm', International Journal of Innovation and Scientific Research,ISSN 2351-8014 Vol. 11 No. 2 pp. 439-444, 2014 Innovative Space of Scientific Research Journals.

[7] Manish gupta, Darpan Anand, Rajeev gupta, Girish parmar,(November 2012), 'A new approach for information security using asymmetric encryption and watermarking technique', international journal of computer applications (0975 – 8887), volume 57– no.14.

 ©IJSRED:All Rights are Reserved