International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 4, pp: 11-17 www.ijaem.net ISSN: 2395-5252

A Paper on "layered Security 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,
[2]Asstt. Professor, CSE Department, Kalinga University, Raipur (CG) India,
corresponding author: Nikita Chhabada

Date of Submission: 30-07-2020 Date of Acceptance: 09-08-2020

ABSTRACT-
The expansion utilization of hand held gadgets comprising of sharp telephones to get admission to interactive media content in the cloud is expanding with upward push and development in measurements innovation. Versatile distributed computing is progressively utilized today because of the reality it permits clients to have get right of section to kind of advantages in the cloud, for example, picture, video, sound and programming bundles with least utilization of their inbuilt assets, for example, stockpiling memory by utilizing the use of the one accessible in the cloud. The significant strategic with cell distributed computing is insurance. Watermarking and computerized mark are a few techniques used to give security and confirmation on client records inside the cloud. Watermarking is a technique used to insert virtual realities inside a media content alongside photo, video or sound so as to spare you approved get admission to the ones substance material through interlopers though, computerized mark is utilized to distinguish and check client records when gotten to. In this work, we executed virtual signature and solid reversible picture watermarking all together brighten versatile distributed computing security and honesty of realities by utilizing introducing twofold confirmation systems. The results acquired showcase the viability of consolidating the two strategies, solid reversible watermarking and computerized signature by providing tough validation to guarantees records uprightness and concentrate the true substance material watermarked without changes.

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

I. INTRODUCTION

The improvement of the Fifth Generation (5G) wi-fi systems is picking up force to interface almost all components of life by means of the network with tons higher speed, exceptionally low inactivity and pervasive availability. Because of its basic situation in our carries on with, the network should stable its clients, segments, and administrations. The assurance danger scene of 5G has developed gigantically in view of the phenomenal increment in sorts of administrations and inside the wide assortment of gadgets. 5G will offer omnipresent broadband types of assistance, empower network of huge wide assortment of devices inside the shape IoT, and engage clients and devices with high portability in a ultra trustworthy and reasonable way. The improvement toward IP-based absolutely correspondence in 4G has just extended new venture openings; be that as it may, 5G is viewed as another condition associating about all elements of the general public; vehicles, residential apparatuses, wellness care, industry, organizations, and so forth., to the system. This turn of events, nonetheless, will present a fresh out of the box new cluster of dangers and assurance weaknesses as an approach to represent a significant errand to each blessing and future systems. With 5G innovation cell devices can have limited carport and simultaneously it can't strategy other mixed media (video) application in light of little RAM. In this way we are the utilization of cloud for putting away our data. In any case, we can't ensure the wellbeing of our put away data in the cloud. The safeguarding gathering of cloud environmental factors may offer copyright assurance yet there's a danger of taking/hacking our own special classified realities by them. Powerful reversible Robust watermarking and RSA advanced mark can take care of this issue. These two procedures have been utilized after the encryption calculation and is utilized to watch the records in cell cloud condition. It offers higher wellbeing execution, blast the first records extraordinary and secrecy. A refusal of transporter ambush (DOS) is any type of assault on a systems administration shape to incapacitate a worker from overhauling its customers. Assaults assortment from

sending a great many solicitations to a worker in an attempt to continuous it down, flooding a worker with huge bundles of invalid records, to sending demands with an invalid or satirize IP address.

Cross-layer security a bound together system is expected to organize unique wellbeing techniques for each security layer, along with programs or the IoT. In remarkable network layer a few security choices are accessible for video. By the utilization of RSA virtual mark we will validate and make sure about most minimal layer from forswearing of transporter assault. The mark will incorporate open key with encoded video insights utilizing RSA virtual signature and Robust Watermarking. The beneficiary must have the certainty that the open key has a place with the originator in any case any replacement by a copy open key would allow a "man inside the center assault" to arrange the information. One component for referencing the authority of the relationship a large portion of the originator and their open key depend upon endorsements. Strategies will enrich the video insights security between portable client and versatile cloud environmental factors. The mix of RSA computerized signature and Robust Reversible watermarking is utilized to upgrade the measurements secrecy and security for sending data to the cell cloud transporters. The fast improvement of sight and sound bundles, for example, advanced distributing, digitized photographs and films and so on., brings about the prerequisite of more noteworthy stockpiling in cell phones.

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 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. So as to maintain a strategic distance from this issue, we use cloud for putting away our data. Information (wi-fi interactive media applications) access over remote systems are a lot quicker. Be that as it may, we aren't guaranteed of data assurance. So the RSA

virtual signature and Robust Reversible watermarking is utilized to cure the above alluded to issue. Information wellbeing in cell cloud condition needs to make certain the made sure about and trustworthy media insights transmissions between cell clients and the cell cloud. In any case, the versatile cloud is kept up by means of 0.33 gatherings along with cell cloud specialist co-ops and we can not be acknowledge as evident with them in any regard time. We will have contracts among clients and cell cloud supplier transporters so as to ensure measurements security. This outfit some capacity dangers, along with security assaults or unfortunate behavior of the cell cloud supplier. Be that as it may, clients can concur with themselves rather than cell cloud security suppliers. Our structure is buyer situated, and allows clients to protect their records' wellbeing and security. The beneficiary ought to have the confidence that the overall population key has a place with the originator in some other case any replacement by a copy open key would allow a "man inside the center assault" to arrange the realities. One component for referencing the authority of the relationship a couple of the originator and their open key depend on authentications. They are given by confided in specialists who create and carefully sign authentications needful elements (comprising of individuals and associations) to their open keys. Shockingly, instruments grant us to acknowledge as obvious with the mark of the depended on expert on the testament.

In the event that a carefully marked report is despatched over web, the sent record and the got archive each are veritable. Cryptography is a method of putting away and transmitting realities in a specific shape all together that best for those it's miles pondered can peruse or framework it. This should be possible accurately in shrewd telephones. It is the strategy of encoding the substance all together that for whom it's miles proposed best can analyze it. Computerized mark is a code that is produced by methods for open key encryption and is utilized to verify and affirm the record despatched over a system. It is likewise used to affirm the sender's character. Today advanced marks are being used in numerous particular structures. Some utilization a strict mark of somebody in plain view and recognize it the utilization of photograph preparing methodologies. This isn't in every case truly dependable framework as home made mark would somewhat vary from one another and bring about illegal get right of passage to. Likewise another way is wearing a little USB apparatus containing our computerized signature and interfacing the gadget to machine to insert the virtual mark. The issue for this is our mark totally relies on the gadget we convey with us. On the off chance that the instrument itself is taken or lost, we may land up in a difficult situation. In addition, the gadget is costly. The most made sure about route for usage of advanced marks considered on this date is biometric marks. Be that as it may, once more, all the PDAs aren't furnished with biometric security frameworks. So on this paper we present a worth compelling, basic, exact, especially made sure about Digital Signature validation and check method utilizing sharp telephones. There are unmistakable overview papers that spread extraordinary components of the cryptography innovation. For instance, in we see about the current techniques built up the utilization of cryptography. Additionally the preferences and drawbacks of these methods are seen here. In , we perceive how a minimal effort computerized mark can be created and may irregular conduct inside the gadget be recognized. In addition, paper gives us way to deal with utilize virtual mark structure that might be utilized for web-basically based application. Also, paper mentions to us what the current procedures of the use of virtual marks are in cell gadget frameworks.

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.

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, we improved the security of the Fifth Generation (5G) Wi-Fi networks by using robust watermarking and RSA algorithm. RSA algorithm receives input from mobile user and convert it into cipher text, this text encrypt the information and send it the next point. Finally cipher text can be converted into decimal text; further an algorithm of robust water marking is used to compress the decimal text along with the private and public key and send the compressed text to the next module,. Embedded technology can be used to merge all fields together and send the information to 5G cloud with full security.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 4, pp: 11-17 www.ijaem.net ISSN: 2395-5252

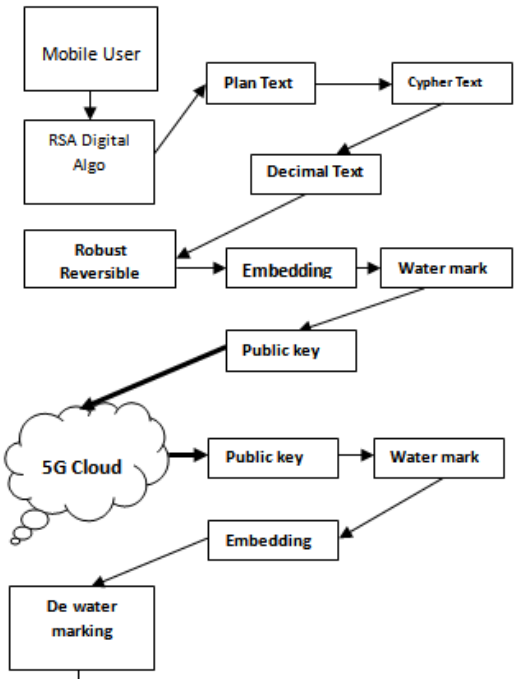
RSA algorithm and watermarking techniques work together to provide strong security in between both the ends, RSA algorithm is a powerful and is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task. As the name describes that the Public Key is given to everyone and Private key is kept private.

One of the significant utilizations of advanced watermarking innovation is copyright insurance and possession recognizable proof for computerized pictures. To accomplish this objective, vigorous watermarking has been quickly evolved in the previous decade or somewhere in the vicinity. Vigorous watermarking is intended to endure different non-geometric controls, for example, JPEG pressure, added substance clamour and separating just as some geometric twists, for example, revolution and scaling. In this section, the crucial idea of advanced watermarking, contrasts among obvious and undetectable watermarking, dazzle and non-daze watermark recognition plans, strong, delicate and semi-delicate watermarking calculations, just as four significant properties for computerized watermarking: intangibility, vigor, limit and security will be portrayed. Various diverse changes and calculations utilized for strong picture watermarking will be checked on in detail.

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 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. 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.. 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.

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.



International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 4, pp: 11-17 www.ijaem.net ISSN: 2395-5252

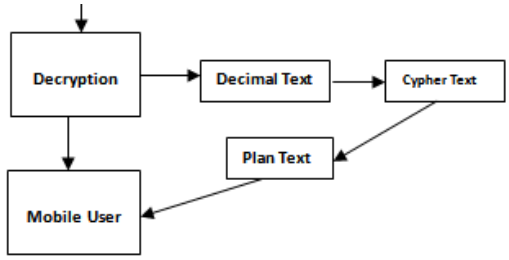


Fig: Block Diagram for 5G cloud Security modules

IV. RESULT AND ANALYSIS

In this section, we display the effectiveness of our proposed methodology. The simulation is achieved on JAVA 2.3.0.04 a & 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.

Result	Attack Number	No Using RSA		Using RSA	
		Attacked Number	Attacked Rate	Attack Number	Attack Rate
Mandatory Access	10	8	0.8	2	2
	20	15	0.75	3	0.06
	30	25	0.80	5	0.6
SQL Injection	10	7	0.7	2	2
	20	16	0.8	4	0.25
	30	26	0.84	7	0.21
XSS ATACKS	10	7	0.7	4	0.4
	20	15	0.75	9	0.44
	30	20	0.70	18	0.6
Bla ck List & White List	10	8	0.8	4	0.4
	20	10	0.5	9	0.44
	30	20	0.70	16	0.6

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 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.

International Journal of Advances in Engineering and Management
ISSN: 2395-5252

IJAEM

Volume: 02 Issue: 01 DOI: 10.35629/5252

www.ijaem.net
Email id: ijaem.paper@gmail.com