Review Article

International Journal of Advanced Technology and Engineering Exploration, Vol4(30)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2017.430003

A review and analysis on text data encryption techniques

Sonu Kumar[1*], Kailash Patidar[2], Rishi Kushwah[3] and Sudeesh Chouhan[3]
M.Tech Scholar, Department of Computer Science & Engineering, SSSUTMS, Sehore, India[1]
Head and Assistant Professor, Department of Computer Science & Engineering, SSSUTMS, Sehore, India[2]
Assistant Professor, Department of Computer Science & Engineering, SSSUTMS, Sehore, India[3]

©2017 ACCENTS

Abstract
In the current age there is need of data security in every field. This paper deals with text data security. In this area there are several research works have already been done and some in progress. But, there is still the need of data security is required in this field. The aims of this paper are to explore the text data security area, discussed the method used and find the capability of the algorithm used. Based on the analysis and discussion finding the gaps and identify it is the goal. So that proper exploration of this field has been done to find out the better way to secure the text data.

Keywords
Cryptography, Steganography, Data security, Encryption methods.

1.Introduction
Information security has turned into a critical concern today for the fruitful operations of various prerequisite of any association. The data security is the genuine concern and protecting an affiliation's information asset from security dangers [1, 2]. With an eye to scene division techniques are ensign for countermeasures against different security perils of the definitive information. The fluctuated points of view of perils and vulnerabilities make undermining condition for the information executive [3, 4]. It is currently a testing assignment for the ventures as all the correspondence and business depends on the information as it is the center piece of any association [5, 6].

There are a few cryptography strategies, which are helpful in information security, for instance, private or mystery key cryptography, open key cryptography, advanced mark and hash work [7]. Private key cryptography, a private key is utilized. Progressed encryption standard (AES), Blowfish, CAST5, Grasshopper, RC4, RC5 and 3DES are the cases of private key cryptography.

This requires wander as a last resort part pass on offering a pantomime of the key and the key be struck by be passed manage without a sheltered channel to the next individual [8].

Private-key cryptography is level indestructible and adequately completed for information security. Along these lines they are more than once for mass estimations encryption. Open key cryptography utilizes an open and private combine for information encryption. RSA, elliptic curve cryptography (ECC) also, Diffie–Hellman key trade. There are other strategies jump at the chance to deliver process hashing the message and can encode the process to create computerized signature [9, 10].

Because of by and large using content as a piece of correspondence strategy, it is fundamental to shield the mystery content data from others that is most certainly not approved for the worry information [11] [12]. To scramble content data one needs to encode the information that is germane to each pixel, since pixels are the basic building bit of picture information [13, 14]. The encoded substance could contain extraordinary properties that pass most by far of the testing criteria so technique for content encryption should be adequately solid. The encoding strategy will change the data into confused structure and decreasing the degree of the data, archive or extend the traverse of the record [15].

Different papers are analysed, discussed and findings have been explored.

*Author for correspondence

2.Related work

In 2009, Juan et al. [16] suggested that the Bluetooth is a low-cost short-range wireless communications medium. Thy suggested security is greater concern in these devices. They have applied DES algorithm to enable Bluetooth technology for military purposes.

In 2011, Murthy et al. [17] focused on encrypting the data based on stream cipher method. The data considered was between the mobile stations and base stations. The keys are generated using genetic algorithm. This genetic algorithm technique gives the best or optimal key for encryption. Before we single point cross over technique is used in generating optimal key for encryption but this paper emphasizes on genetic algorithm technique for different sizes of population and different number of iterations considering multi point crossover. The plain text which is to be encrypted along with the key are encoded using the arithmetic coding technique. Encryption is done to convert the plain text into cipher text.

In 2012, Kester et al. [18] contributed in the area of cryptography application. They have developed a cipher algorithm to produce the ciphered image and also to decrypt ciphered image. The calculation at last makes it feasible for encryption and unscrambling of the pictures in light of the RGB pixel the calculation was actualized utilizing MATLAB.

In 2012, Jing et al. [19] suggested that the text encryption method is capable in information security. On the premise of dissecting the parallels between content watermarking and content encryption, a content encryption calculation in view of common dialect handling is proposed. Three semantic changes in normal dialect preparing are presented. At long last, the necessities and the procedure of the content encryption calculation are given.

In [20-22] authors have suggested different encryption techniques with different file formats have been applied in server and client communication security and provided a practical overview and their implications. The results suggest that their techniques are capable in securing server data.

In 2013, Saraireh et al. [23] proposed a secure system for communication. Their algorithm combined cryptographic algorithm together with steganography. It helps in providing robust and strong communication system to protect from the attackers. Thy have used filter bank cipher to encrypt the secret text message. Then a discrete wavelet transforms (DWT) based steganography is adopted to hide the encrypted message in the cover image by modifying the wavelet coefficients. Their result suggests that it provides high level security.

In 2016, Park et al. [24] deals with two security problems between the cloud computing service and trusted platform module (TPM). They suggested the first problem is the social issues from inside attackers. For this they suggested encrypted DB retrieval system. They suggested the second problem is that cloud computing has limitless computing resources. To conquer the shortcoming and create synergic impacts between the two advancements, we join two applications (cloud datacenter benefit, TPM chip) as a portable concurrent innovation. The principle strategies are TPM-security-customer and veiled keys. With these techniques, the genuine keys are put away in TPM and the faked keys (covered keys) are actualized for calculations rather than genuine keys. Accordingly, the consequence of the faked keys is the same as the genuine keys. So their framework is secure against both of the insiders and pariahs, the distributed computing administration can enhance security shortcomings.

3.Problem discussion

In [23] authors suggest watermarking scheme that has efficient PSNR value and comparable similarity measurer in respect of traditional techniques. The overall comparison is shown in *Table 1*.

Table 1 Overall comparison

S. No	Reference	Method used	Results	Problem definition
1	[25]	Data security and privacy in cloud computing	Their method is capable if the users have control over encryption and decryptions of data that will boost consumer confidence and attract more people to cloud platform.	Practical results are missing to support the statement.
2	[26]	RSA Algorithm	The calculation enables a message sender to produce open keys to encode the message and the collector is sent a created private key utilizing a secured database. A mistaken private key will	Different standard encryption techniques can be applied.

S. No	Reference	Method used	Results	Problem definition
			even now decode the scrambled message yet to a frame not quite the same as the first message.	
3	[27]	Complex encrypting and decrypting data	Their security mechanism "A New Approach for Complex Encrypting and Decrypting Data" which is capable in maintaining the security on the communication channels by making it difficult for attacker to predicate a pattern as well as speed of the encryption / decryption scheme.	Hybridization with other standard encryption algorithm may provide stronger security.
4	[28]	RSA and MD5 algorithm for resource attestation and sharing in java environment	Their approach is mainly divided into two parts. First part is controlled by the normal user which gets permission by the cloud environment for performing operation and for loading data. Second part shows a secure trusted computing for the cloud, if the admin of the cloud want to read and update the data then it take permission from the client environment. This provides a way to hide the data and normal user and can protect their data from the cloud provider. This provides a two way security protocol which helps both the cloud and the normal user.	Results are not validated.
5	[29]	Text steganography	They proposed an unique data security using text steganography (UDSTS) to build a system that is able to transmit and receive encrypted messages embedded in rich text Format: *.DOC, *.RTF, EMAIL /Message Body/, etc. The client can pick the fake content and the program tells whether this fake content can be suited the genuine content. The client is empowered to set distinctive secret word for each message he sends and in this manner two unique messages can be transmitted to two gatherings with two distinct passwords utilizing the same fake content. Instant messages are thought to be innocuous and don't trigger an examination. Henceforth the strategy gives a decent information security plot.	Cryptography with steganography can impact more.
6	[30]	Text data outsourcing	They have explored and analysis's different security breaches in cloud Computing. They have discussed data security along with the access control and authorization and suggest some suggestions.	How it is implemented is missing.
7	[31]	AES and RC6 based cloud-user data security	They proposed an efficient framework for text data security. For data security advanced encryption standard (AES) and RC6 algorithms are used. The information is transferred by the clients so the information of the worry client is the administrator of those information. Cloud servers are likewise not permitted to view or refresh the information without the consent of the worry client. At the point when any client or, then again cloud server needs to get to the information of others, the information can be asked. The encoded information is send after the authorization of the worry client.	How it is implemented without any communication medium.
8	[32]	Compression and cryptography	They have implemented various cryptography algorithms for data security. The information will be first packed utilizing pressure procedures and after that encryption methods will connected and after that relative examination will be done for	Different comparative parameters are missing.

S. No	Reference	Method used	Results	Problem definition
			various blends of pressure and encryption systems. On the off chance that encryption and pressure are done in the meantime then it requires less preparing investment and more speed.	
9	[33]	Review of solutions for securing end user data	They identified end users data security issues when using cloud computing services. It can be addressed using public key cryptography or public key infrastructure (PKI). The information will be first packed utilizing pressure strategies and after that encryption methods will connected and afterward relative investigation will be completed for various mixes of pressure and encryption systems. On the off chance that encryption and pressure are done in the meantime then it requires less preparing investment and more speed.	How it is implemented is missing.
10	[34]	Cybersecurity: risks, vulnerabilities and countermeasures	The objective of their study is to evaluate the vulnerabilities of an association's data innovation framework, which incorporate equipment, and programming frameworks, transmission media, neighborhood, wide range systems, undertaking systems, intranets, and its utilization of the web to digital interruptions.	How it is implemented is missing.

4.Gap analysis

The following gaps have been identified basis on the review and analysis discussed in the above sections.

1. There is a need of encryption technique which is capable in converting encrypted data in different file formats to enhance the confusion.
2. Different hybridization of encryption technique is also missing.
3. Need to minimize the time differences and allow decrypting it in a shorter time.
4. Cross data conversion is missing like text form is encrypted in images so that the attacker can confuse in handling the data.
5. Data recovery mechanism can be applied to handle the data smoothly. So to minimize the losses.

5.Conclusion and future direction

In this paper a wide exploration has been presented for security methods for text data security. Different analysis has been presented based on different parameters to explore the possibilities in this direction. Based on the discussion it is found that there is the need of data security in the fashion that the original attribution is not shown in the encrypted message so that the attackers not know the identity of the data means the type. Cross data conversion can be a key factor for the future research.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Kumar B, Boaddh J, Mahawar L. A hybrid security approach based on AES and RSA for cloud data. International Journal of Advanced Technology and Engineering Exploration. 2016; 3(17):43.

[2] Kumar B, Boaddh J. A meta-analysis on secure cloud computing. International Journal of Advanced Technology and Engineering Exploration. 2016; 3(15):15.

[3] Lee HM, Lee TY. Analysis of algorithm of cipher text containing data and key in network security. In international conference on innovative computing, information and control 2007 (pp. 439-439). IEEE.

[4] Jaquith A. Security metrics: replacing fear, uncertainty, and doubt. Upper Saddle River: Addison-Wesley; 2007.

[5] Noel S, Jajodia S, O'Berry B, Jacobs M. Efficient minimum-cost network hardening via exploit dependency graphs. In proceedings of computer security applications conference 2003 (pp. 86-95). IEEE.

[6] Ou X, Govindavajhala S, Appel AW. MulVAL: A logic-based network security analyzer. In USENIX security symposium 2005 (pp. 8-8).

[7] Zaidan BB, Zaidan AA, Al-Frajat AK, Jalab HA. On the differences between hiding information and cryptography techniques: An overview. Journal of Applied Sciences. 2010; 10:1650-5.

[8] Singh A, Gilhotra R. Data security using private key encryption system based on arithmetic coding. International Journal of Network Security and its Applications. 2011; 3(3):58-67.

[9] Kumar MK, Azam SM, Rasool S. Efficient digital encryption algorithm based on matrix scrambling technique. International Journal of Network Security & its Applications. 2010; 2(4): 30-41.
[10] Lakhtaria KI. Protecting computer network with encryption technique: A Study. In international conference on ubiquitous computing and multimedia applications 2011 (pp. 381-90). Springer, Berlin, Heidelberg.
[11] Raviraj P, Sanavullah MY. The modified 2D-haar wavelet transformation in image compression. Middle-East Journal of Scientific Research. 2007; 2(2):73-8.
[12] Blackedge JM, Ahmed M, Farooq O. Chaiotic image encryption algorithm based on frequency domain scrambling. School of Electrical Engineering systems Articles, Dublin Institute of Technology. 2010.
[13] Kharate GK, Ghatol AA, Rege PP. Image compression using wavelet packet tree. ICGST-GVIP Journal. 2005; 5(7):37-40.
[14] Walnut DF. An introduction to wavelet analysis. Springer Science & Business Media; 2013.
[15] Ahmad M, Alam MS. A new algorithm of encryption and decryption of images using chaotic mapping. International Journal on Computer Science and Engineering. 2009; 2(1):46-50.
[16] Juan L, Bin C, Kun L. Study on the improvement of encryption algorithm of Bluetooth. In international conference on networking and digital society 2009 (pp. 89-92). IEEE.
[17] Murthy YS, Satapathy DS, Srinivasu P, Saranya AA. Key generation for text encryption in cellular networks using multi-point crossover function. International Journal of Computer Applications 2011.
[18] Kester QA, Koumadi KM. Cryptographie technique for image encryption based on the RGB pixel displacement. In international conference on adaptive science & technology 2012 (pp. 74-7). IEEE.
[19] Jing X, Hao Y, Fei H, Li Z. Text encryption algorithm based on natural language processing. In international conference on multimedia information networking and security 2012 (pp. 670-72). IEEE.
[20] Qadri SI, Pandey K. Tag based client side detection of content sniffing attacks with file encryption and file splitter technique. International Journal of Advanced Computer Research. 2012; 2(5):227-33.
[21] Dubey A, Gupta R, Chandel GS. An efficient partition technique to reduce the attack detection time with web based text and PDF files. International Journal of Advanced Computer Research. 2013; 3(9):80-6.
[22] Gupta S. Secure and automated communication in client and server environment. International Journal of Advanced Computer Research. 2013; 3(4):263-71.
[23] Saraireh S. A Secure Data Communication system using cryptography and steganography. International Journal of Computer Networks & Communications. 2013; 5(3):125-37.
[24] Park HA. Secure chip based encrypted search protocol in mobile office environments. International Journal of Advanced Computer Research. 2016; 6(24):72-80.
[25] Marwaha M, Bedi R. Applying encryption algorithm for data security and privacy in cloud computing. International Journal of Computer Science Issues. 2013; 10(1):367-70.
[26] Goshwe NY. Data encryption and decryption using RSA algorithm in a network environment. International Journal of Computer Science and Network Security. 2013; 13(7):9-13.
[27] Al-Hazaimeh OM. A new approach for complex encrypting and decrypting data. International Journal of Computer Networks & Communications. 2013; 5(2):95-103.
[28] Dubey AK, Dubey AK, Namdev M, Shrivastava SS. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. In sixth international conference on software engineering 2012 (pp. 1-8). IEEE.
[29] Torvi SD, ShivaKumar KB, Das R. An unique data security using text steganography. In international conference on computing for sustainable global development 2016 (pp. 3834-38). IEEE.
[30] Bhute S, Arjaria SK. Security of text data outsourcing in cloud computing. International Journal of Advanced Technology and Engineering Exploration. 2016; 3(20):91-7.
[31] Bhute S, Arjaria SK. An efficient AES and RC6 based cloud-user data security with attack detection mechanism. International Journal of Advanced Technology and Engineering Exploration. 2016; 3(21):110-17.
[32] Sharma R, Bollavarapu S. Data security using compression and cryptography techniques. International Journal of Computer Applications. 2015; 117(14).
[33] Bhardwaj A, Subramanyam GV, Avasthi V, Sastry H. Review of solutions for securing end user data over cloud applications. International Journal of Advanced Computer Research. 2016; 6(27):222-9.
[34] Conteh NY, Schmick PJ. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research. 2016; 6(23):31-8.