Vol. 3 No. 4
Scientific Voyage: ISSN: 2395-5546
Government College of Engineering and Ceramic Technology, West Bengal, India

Data Security Perspective in Secure Data Communication

Sayantan Chakrabarti[1,*], **Sudipta Roy**[2], **Soumit Chowdhury**[3], and **Pranab Gharai**[4]

[1-2]*Department of Information Technology, B. P. Poddar Institute of Management and Technology, Kolkata*

[3]*Department of Computer Science, Government College of Engineering and Ceramic Technology, Kolkata*

[4]*Department of Computer Science, Brainware University, Kolkata*

[*]*92sayantan@gmail.com*

Received: Nov 09, 2023
Accepted: Dec 17, 2023

ABSTRACT

With the enrichment of use of the internet the confidentiality and security of our information becomes vulnerable now-a-days. Security in confidential information becomes one of the key challenges in context of data leakage and unauthorised access of data. Data security is one of the main concern in recent data industry to prevent alteration and illegal access of data. To ensure utmost security researches are going on rapidly on data security aspects. Various security methods and algorithms has been introduced to protect our data. Data can be secured in multiple forms like converting the actual data into non-readable data by applying cryptography concept, Data can be hidden under any cover medium by applying stenography approaches and visual cryptography. Data can be authenticated through watermarking applications. Thus sensitive information can be protected from unauthorised access. These concepts have been introduced to satisfy main data security principles for ultimate protection.

Keywords: Data Security, Cryptography, Steganography, Watermarking, Visual Cryptography

1 INTRODUCTION

Data security become one of the challenging aspects now-a-days to protect sensitive data from misuse. Data security principles has been designed and followed to ensure security. The main aspects are Confidentiality of transferred data, Integrity of the data communication, Authenticity of the data communication medium and Non-repudiation. Confidentiality states that the information shared by users are confidential among the respective users only. No data leakage will be there among the transactions. Different cryptography techniques have been used to make sensitive information confidential[1].

Integrity ensures that the information shared in any communication are not invoked by any other than the actual users. The data should not be altered or tampered and it must be original data [1]. Authenticity provides the surety that the data received by any user transferred from an authentic source. It implies that the communication is trusted and information are generated from genuine users [1]. Non-repudiation indicates that the receiving of data could not be denied by the receiver. It basically acts as log of data sharing [1]. Data security principles deals with different aspects of secure mechanism to provide utmost security in communication medium.

2 Literature Review

Different cryptographic algorithms are discussed in paper [1] to highlight the idea of cryptography in data communication. Different key based cryptographic algorithms and multiple key concepts has been discussed in paper [2]to highlight the categories of keys in cryptographic algorithms. Different cryptographic algorithms like play fair cipher in3D image medium has been discussed in paper [3] and paper [4] concentrated for colour medium. Symmetric and Asymmetric key exchange properties have been discussed in paper [5] and paper [6]. Paper [7] focuses on the application of watermarking in sensitive information like biometric data. Sensitive content can be authenticated through the application of watermarking. Application of steganography in recent days like IoT has been discussed in paper [8]. Security in IoT data transfer is also an important concern of late to protect data leakage in IoT data transfer channel. The concept of visual cryptography has been emphasized in paper [9] to focus the utility of visual cryptography in recent days. Paper [10] gives idea on different watermarking techniques and its application.

3 Data Security Techniques

Information sharing depends upon transferring data in multiple form like text, image, audio, video etc. Securing of data can be achieved in two ways i.e. Data hiding and Cryptography. Data hiding deals with concealing of sensitive information into various

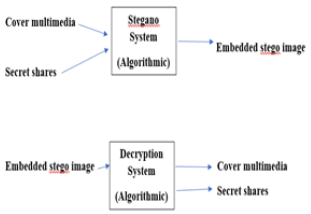

Fig. 1. Encryption and Decryption system

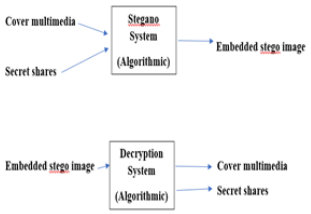

Fig. 2. Steganography system

cover medium. Cryptography deals with converting a readable text into unreadable text.

3.1 Cryptography

Cryptography is used to convert a readable plain text into unreadable cipher text by applying cryptographic encryption algorithm and keys. Cipher text is used and transferred among users so that it will not be recognised by unauthorised users [6]. Cryptographic decryption algorithm is used to make the cipher text into readable plain text at the end point to the authentic users so that data can be readable by using keys stated in Fig 1. Key is generated with the combination of numbers or alphabets or bit string. Depending upon the use of key cryptography can be differentiated into two categories. Asymmetric key cryptography uses two different key i.e. both public key and private key [5]. Symmetric key cryptography uses same key for both encryption and decryption [4]. Original confidential information can be hidden under any cover medium like image, audio, video etc. and can be transferred securely to the authentic user. Authenticity of the sender can also be verified using watermarking.

3.2 Steganography

Steganography states that the sensitive information will be embedded into cover medium and the cover medium will be sent to the receiver [8]. The data will be extracted from the cover medium in the receiver end. Thus ensures the security that embedded information will not be disclosed to anyone except appropriate receiver stated in Fig. 2. Based on the cover medium Stenography can be subdivided into some segments [8]. Text Steganography: Text file has been used as cover medium to embed the secret data into it. Image Steganography: Image file has been used as cover medium to embed the secret data into it. Audio Steganography: Audio file has been used as cover medium to embed the secret data into it. Video Steganography: Video file has been used as cover medium to embed the secret data into it.

3.3 Watermarking

Watermarking concept is introduced to provide authenticity on data to protect from alteration and tampering. Secret logos are used visibly or invisibly to protect data and provide copyright of the authorised users. Logos are used to authenticate the appropriate user. Based on the visibility of the logo watermarking can be categorised into two segments [7]. Visible Watermarking: Watermarked logo is visible to the user after embedding it onto data medium [10]. Invisible Watermarking: Watermarked logo is not visible to the user after embedding it onto data medium [10]. The efficiency of watermarking is measured by factors like Robustness, Imperceptibility, Transparency and Data payload [7].

3.4 Visual Cryptography

Visual cryptography is introduced in recent days after gradual development of conventional cryptographic concepts. In visual cryptography visual data like image, audio, video has been encrypted using respective algorithms. Multimedia data is segmented into different parts to generate shares. These share are transferred to receivers thorough different medium. Decode of the actual data from these shares takes place in receiver end [9].

4 Recent applications of Data Security

Data security principles has huge impact on digital medium where mostly sensitive data is used in recent day scenario. Medical image authentication, Digital document authentication could be done properly through data security approaches. Data security also plays a vital role in sensitive data transfer in defence organization, economic transfer, data protection.

5 Conclusion

This paper mainly focuses on the utility of data security in recent digital data communication. Different data security aspects have been discussed in this paper to focus the prime features of data security in electronic medium to protect the sensitive and confidential data from unauthorised access.

6 Future Scope

Data security can be implement in different sensitive aspects like protection of epic information, protection of adhar information using biometric identification, evaluation sheet protection etc.

Declaration: The authors declare no conflicts of interest.

REFERENCES

[1] Abhishek, Dr. Vandana;(April-2022), A STUDY ON MODIFIED RSA ALGORITHM IN NETWORK SECURITY; International Research Journal of Modernization in Engineering Technology and Science; ISSN: 2582-5208; Volume:04/Issue:04.

[2] Mohammed N. Alenezi, Haneen Alabdulrazzaq, and Nada Q. Mohammad;(August 2020), Symmetric Encryption Algorithms: Review and Evaluation study; International Journal of Communication Networks and Information Security (IJCNIS) ; Vol. 12, No. 2.

[3] Santoso K A;Sukmawati R A; Pradjaningsih A;(2022), "Image security development using 3D playfair cipher combination and bit shift", Volume 2391, Issue 1 , INTERNATIONAL CONFERENCE ON SCIENCE AND APPLIED SCIENCE (ICSAS), AIP Conference Proceedings 2391, 020013.

[4] Subramaniyam.c.s,Sukanya sargunar.v;(2016), Implementation of playfair cipher by using 7 by 9 matrix and colour substitution; International Journal of Engineering Associates, ISSN: 2320-0804; / Volume 5 Issue 8.

[5] Wimpenny G,Šafář J, Grant A, Bransby M;(March 2022), Securing the Automatic Identification System (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility, The Journal of Navigation , Volume 75 , Issue 2 , pp. 333 – 345.

[6] Goyal A, Kaur D;(2021), Picpass Algorithm for Solution of Key Exchange Problem in Symmetric and Asymmetric Key Cryptography; International Journal of Scientific Research in Computer Science Engineering and Information Technology; ISSN : 2456-3307; Volume 7, Issue 6; pp-305-308.

[7] Deepika R , Shambhavi M , Impana R , Shishira AP , Lavanya Krishna;Zero-Bit Watermarking Technique for Generation of Unique ID Using Biometric Images; 2022 International Conference on Intelligent Technologies (CONIT) — 978-1-6654-8407-7/22/ ©2022 IEEE — DOI: 10.1109/CONIT55038.2022.9848041.

[8] Khari M, Garg A K,Gandomi A H,Gupta R,Patan R, Balusamy B;(JANUARY 2020), Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques; IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, VOL. 50, NO. 1.

[9] Ortega A M and Hernandez M C; (2022) Ownership Authentication and Tamper Detection in Digital Images via Zero-Watermarking; 45th International Conference on Telecommunications and Signal Processing (TSP) — 978-1-6654-6948-7/22/ ©2022 IEEE — DOI: 10.1109/TSP55681.2022.9851253.

[10] Begum M, Shorif Uddin M; (2020), Digital Image Watermarking Techniques: A Review; Information, 11, 110; doi:10.3390/info11020110.