Providing Safety Measures for Cyber Security by Implementing Cryptographic Encoding using Big Data Analytics

[1]Subhasish Swain, [2]Jayachandran Balakannan, [3]Abanikanta Pattanayak

[1]Assistant Professor in Dept. of Computer Science, GIET Gangapatna, Bhubaneswar
[2]Professor in Dept. of Computer Science, GIET Gangapatna, Bhubaneswar
[3]Assistant Professor in Dept. of Computer Science, GIET Gangapatna, Bhubaneswar

Abstract: Knowledge is acquired through exposure to information. Extracting knowledge from vast amounts of data, known as Big Data, has been a significant challenge. Big Data Analytics (BDA) is a concept developed by academics to describe how large volumes of data are processed, collected, and preserved for further analysis. One of the goals is to secure big data from cyber threats using cybersecurity measures. This article explores recent cybersecurity research related to big data, with a focus on security and data preservation. Access control management is typically more robust and easier to enforce, but it also exposes data to threats. Big data encryption can be a key defense against data breaches, as data privacy is a major concern. Keywords: Big data, Cyber threats, Cybersecurity, Encryption, Access control, Research.

1. Introduction:

Surveillance is not only used in public locations like airport, busses, trains, but also in privateareas. A sincere consumer may recognize any items for which he wants to monitor or examine. Big data has certain specific characteristics to manipulate for different purposes. This is worth noting. s Encrypt a whole camera [1],[2]and an region of interest (ROI) that has details regarding sensitivity [3],[4],[5]. The use of big data in detecting risks or attacks is one of these. Hacking was originally close to the general norm. For fun and for notoriety, hackershacked. However, but attacks are more planned and inspired these days. We are utilizing information protection to deter intrusion. As a method to combat various attacks like intrusion, ransom ware, human mistakes, sophisticated persistent threading, social threats Big Data Analytics (BDA). The standard solutions for Big Data protection is encryption and access management. However, researchers have found certain forms that any form of encryption may or may not require. The existence of big data makes it impossible to encrypt anything. Any scholars have sought to decide the relevant aspects of big data and cover certain pieces only. They tried to protect big data properties that are important, since it is a challenging job to safeguard anything. To secure these prized characteristics, they use data masking. They use a rating algorithm that gives preference to attributes for big data protection to decide which attributes are of interest. Specific cryptographic and ROI extraction methods are introduced to mask data security from vulnerable areas. In order to encrypt ROIs in [6][7], Chaos' cryptography technique is implemented. Transform-domain and stream-code techniques are suggested in [8], [9] and [10]. A random key is generated that guarantees that different encryption results are presented in the same ROI blocks in different video frames, so that the algorithm can withstand so-called plaintext attacks.

2. Related Work

In this segment, we overview the corresponding encrypted ROIs, rather than encrypting the entire surveillance cycle.

2.1 *Our Approach:*

Our method is hierarchical protection of privacy for surveillance which can only be used to enable the non-authenticated user to see real-time surveillance while the authenticated user can assess the full surveillance on demand.

2.2 *Security and performance analysis:*

It is to implement large number of data. For the access control and privacy of big data, the work in presented a hybrid approach-based framework that composes and enforces privacy policies to capture privacy requirements in an access control system, a cloud security control mechanism based on big data. Cloud computing was observed to have increased the amount of data in the network. Due to this, big data leaks and losses occurred. Therefore, there was the need to provide the necessary level of protection. To that end, they conducted an analysis on big data, analyzed the current big data situation. Data for business advantages can be affected by CSP. In order to tackle the problem of safe data exchange, Cipher text policy- based encryption of attributes (CP-ABE) has proved to be an essential technology [11].

2.3 *System Architecture:*

Architecture diagram is a graphical representation it conceptual model that defines structure behavior a set of components that a part of including of their elements. In the architecture description is to formal description.

Fig.1 The plain text to be encrypted by our approach after the data to be stored under the database and that the unique key value to be generated automatically, if any user or hackers can be entering wrong password in 3rd times suddenly the security key should be changed automatically. if the key value is correct the data should be decrypted.

2.4 *Admin*

If a person legally visited in the administrated through the database connection of a user to protect the security in a surveillance of the cyber security.

2.5 *Database*

The database architecture includes database of a design is involved. That database is to protect key generator of a through between the database and cloud.

2.6 *Cloud*

If the cloud access refers to the internet of servers accessed over the internet.

2.7 *USER*

In a cloud we take some information if the person takes means automatically key generator that a right taken that that information will go directly authenticated.

3. Unauthenticated User

If a wrong person takes some kind of information means one or two times it will generatorand the third will send blocked chain.

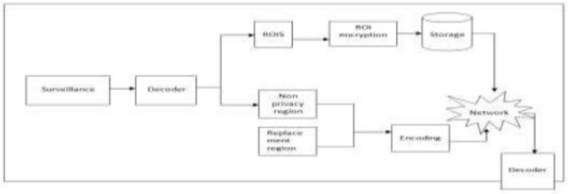


Fig.1 System Architecture

4. Proposed Framework

In my project, Fig. 2 Attributes characteristics should be easily noted, then they could secure by security masking and encrypted and access should be given by that cloud authority. I am creating a forex application to overcome a disadvantage occurs in the existing method by implementing encryption and access control (AC) to protect data.

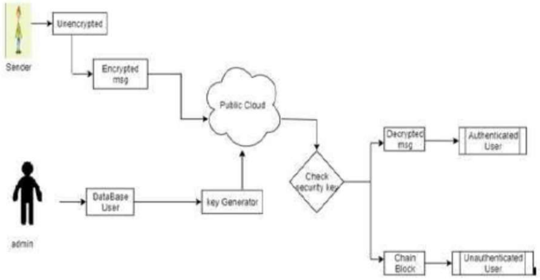


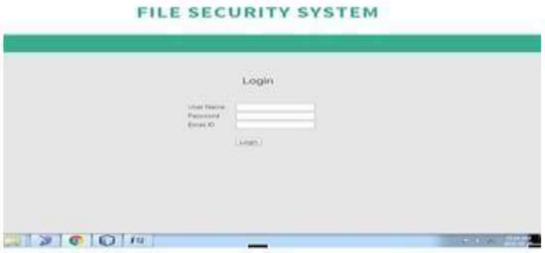
Fig.2 AC framework

5. ROI Encryption Algorithm

The binary sequences of a ROI block for the initial 8-layered protocol are used for the ROI encryption algorithm. The key component may only be viewed as a compression of the random chosen database sequence by encrypting the output of ROI.

5.1 *Implementation*

In figure 3 admin login page is displayed.


FILE SECURITY SYSTEM

Login

User Name
Password
Email ID

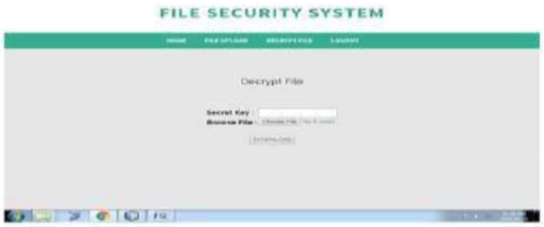
Fig.3 Admin loginIn figure 4 enter into admin home page

FILE SECURITY SYSTEM

Admin Home

Fig.4 Admin Home Page

In Fig.5 the decrypt page is created for the user to upload the files.


FILE SECURITY SYSTEM

Decrypt File

Secret Key :
Browse File : Choose File No file chosen

Fig.5 Decrypt page

Fig.6 Uploading File

6. Conclusion

In this paper, we delve into recent research in cybersecurity concerning big data, focusing on the protection and storage of such data. We anticipate future challenges where malware may target big data, requiring implementation techniques for access control and encryption to address potential vulnerabilities and errors

References

[1] A.unterweger, K.V.Ryckegem. ``Privacy-preserving H.264 video encryption scheme," *ETRI J.*, vol. 33, no. 6, pp. 935_944, 2011.

[2] M. I. Khan, V. Jeoti, and M. A. Khan, ``Perceptual encryption of jpeg compressed images using dct coef_cients and splitting of dc coef_cients into bitplanes," in *Proc. Int. Conf. Intell. Adv. Syst.*, 2010, pp. 1_6.

[3] S. Auer, A. Bliem, D. Engel, A. Uhl, and A. Unterweger, Bitstream-based jpeg encryption in real-time," *Int. J. Digit. Crime Forensics*, vol. 5, no. 3, pp. 1_14, 2013.

[4] P. Carrillo, H. Kalva, and S. Magliveras, ``Compression independent reversible encryption for privacy in video surveillance," *Eurasip J. Inf. Secur.*, vol. 2009, no. 1, pp. 1_13, 2010.

[5] A. Unterweger, K. V. Ryckegem, D. Engel, and A. Uhl,``Building a post- compression region-of-interest encryption framework for existing video surveillance systems: Challenges, obstacles and practical concerns," *Multi-media Syst.*, vol. 22, no.5, pp. 617_639, 2016.

[6] S. M. M. Rahman, M. A. Hossain, H. Mouftah, A. E. Saddik, and E. Okamoto, ``A real-time privacy-sensitive data hiding approach based on chaos cryptography," in *Proc. IEEE Int. Conf. Multimedia Expo*, Jul. 2010, pp. 72_77.

[7] S. M. M. Rahman, M. A. Hossain, H. Mouftah, A. El Saddik, and E. Okamoto,``Chaos-cryptography based privacy preservation technique for video surveillance,"*Multimedia Syst.*, vol. 18, no. 2, pp. 145_155, 2012.

[8] X. Ma,W. K. Zeng, L. T. Yang, D. Zou, and H. Jin, ``Lossless ROI privacy protection of H.264/AVC compressed surveillance videos," *IEEE Trans. Emerg. Topics Comput.*, vol. 4, no. 3, pp. 349_362, Jul./Sep. 2016.

[9] Y. Zhao, L. Zhuo, N. Mao, J. Zhang, and X. Li, ``An object-based unequal encryptionmethod for H. 264 compressed surveillance videos," in *Proc. IEEE Int. Conf. Signal Process., Commun. Comput.*, Aug. 2012, pp. 419_424.

[10] F. Dufaux and T. Ebrahimi, ``Scrambling for privacy protection in video surveillance systems," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 8, pp. 1168_1174, Aug. 2008.

[11] Subha, K. and Reddy, K., 2017. Data Sharing in Cloud Computing Based On Attribute Based Encryption System. International Journal of MC Square Scientific Research, 9(2), pp.55-63.

[12] Sharma, Ashish, and Dhara Upadhyay. "VDBSCAN Clustering with Map-Reduce Technique." Recent Findings in Intelligent Computing Techniques. Springer, Singapore, 2018. 305-314.

[13] Kumar, Manoj, and Ashish Sharma. "Mining of data stream using “DDenStream” clustering algorithm." 2013 IEEE International Conference in MOOC, Innovation and Technology in Education (MITE). IEEE, 2013.

[14] Sharma, Ashish, Ashish Sharma, and Anand Singh Jalal. "Distance-based facility location problem for fuzzy demand with simultaneous opening of two facilities." International Journal of Computing Science and Mathematics 9.6 (2018): 590-601.

[15] Shekhar, Shashi, and Nirbhow Jap Guide Singh. Design of an fir low pass filter using bare bones particle swarm optimization. Diss. 2015.