AES-GCTR Mode-based Efficient Hybrid Encryption Scheme in Cloud-CCTV Service Environment

Yujin Jung, Won-chi Jung, Sangik Oh, Donghyeok Lee, Namje Park

Abstract: ***In the environment of Cloud-CCTV surveillance, encryption of images for the protection of privacy is essential. Yet, the existing encryption method has overhead regarding the management of mass data and streaming processing. As encrypted vectors are created and applied in a bucket unit in the proposed method, it has more efficient performance in the process of encryption and decoding compared to AES-CTR mode, and it makes an analysis attack difficult according to the randomness of a bucket size. In this paper, AES-GCTR mode that has improved the existing AES-CTR operation mode was suggested. In this process, encryption of CCTV image data is required. Yet, overhead of encryption itself exists in quality, so an efficient encryption method proper for mass data is necessary. The proposed method can make encryption and decoding performance more efficient, and is expected to be easily applied to the image surveillance system based on CCTVs that demands high capacity processing and real-time streaming.***

Keywords : CCTV, Encryption, Surveillance, CTR Mode, Advanced Encryption Standard

I. INTRODUCTION

Recently, CCTV surveillance service based on cloud is drawing attention. Image data taken by CCTVs has the feature of big volume demanding large storage space, so the CCTV surveillance environment is appropriate for cloud environment that can offer mass storage. However, cloud environment is exposed to different threats to security, for instance, hacking of communication and database by an outsider and an attack by an insider, so CCTV image data needs a strong security system[1,2,3,4,5,6].

Figure 1 displays a cloud-based CCTV surveillance system model. Images taken by a CCTV are stored in a cloud server via the Internet, and the cloud server offers real-time image data to the surveillance system. In this process, encryption of CCTV image data is required. Yet, overhead of encryption itself exists in quality, so an efficient encryption method proper for mass data is necessary[7,8,9,10,11].

Furthermore, as intelligent surveillance techniques become increasingly more popular, smart surveillance is being incorporated into cloud computing environments due to a number of reasons such as data storage and availability. In the cloud environments, personal information collected through smart surveillance (CCTV tracking feeds, sensor data, metering data, etc.)is exposed to the outside world, and clouds are considered an unreliable realm. In the context, cloud services are considered the non-reliable realm because of the potential risks existing therein such as various threats to the security of data stored in cloud and data leaks by insiders. Such risks act as direct threats to the personal information. Therefore, when storing the data in databases within cloud servers, appropriate means need to be employed to protect the data. Another issue to address is that real-world cloud computing environments where CCTV surveillance data are stored are susceptible to a wide range of security-breaching factors including insider attacks. To help prevent such attacks, previous studies such as those by D. A. Rodríguez-Silva and Hossain proposed a security policy which separates private cloud networks from their public counterparts. Private clouding applications, however, are by no means immune to attacks by insiders and can thus remain vulnerable to security threats present in the conventional cloud environments [12,13,14,15,16,17,18].

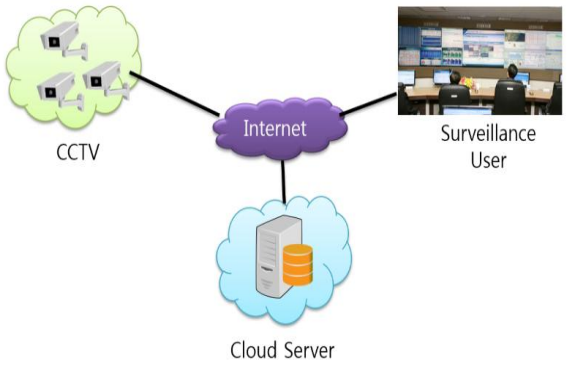

Figure 1 : Cloud-CCTV Surveillance Model

Revised Manuscript Received on July 22, 2019.

Namje Park*, Dept. of Convergence Information Security, Graduate School, Jeju National University, 61 Iljudong-ro, Jeju-si, 63294, South Korea. Email: namjepark@jejunu.ac.kr

Yujin Jung, Dept. of Convergence Information Security, Graduate School, Jeju National University, 61 Iljudong-ro, Jeju-si, 63294, South Korea. Email: yujinjung@jejunu.ac.kr

Won-chi Jung, , Dept. of Convergence Information Security, Graduate School, Jeju National University, 61 Iljudong-ro, Jeju-si, 63294, South Korea. Email: jwonchi@jdcenter.com

Sangik Oh, , Dept. of Convergence Information Security, Graduate School, Jeju National University, 61 Iljudong-ro, Jeju-si, 63294, South Korea. Email: raitsu58@jejunu.ac.kr

Donghyeok Lee, , Dept. of Convergence Information Security, Graduate School, Jeju National University, 61 Iljudong-ro, Jeju-si, 63294, South Korea. Email: bonfard@jejunu.ac.kr

In the environment of Cloud-CCTV surveillance, encryption of images for the protection of privacy is essential. Yet, the existing encryption method has overhead regarding the management of mass data and streaming processing. In this paper, AES-GCTR mode that has improved the existing AES-CTR operation mode was suggested. In this paper, AES-GCTR operation mode with the strength of possible parallel processing which has improved AES-CTR among AES encryption operation modes was suggested. As encrypted vectors are created and applied in a bucket unit in the proposed method, it has more efficient performance in the process of encryption and decoding compared to AES-CTR mode, and it makes an analysis attack difficult according to the randomness of a bucket size.

II. RELATED STUDIES

A. Needs for CCTV surveillance

The biggest beneficiary of clouding-based intelligent CCTV surveillance is smart cities. The purposes of smart cities are to integrate the elements of urban environment such as city infrastructure, residents, and the environment and to maximize the management and efficiency of the integration by putting information and communication technologies to good use. The concept of smart city includes the environment, energy, water resources, transportation, health, and public order and security, aiming to provide intelligent services that go beyond mere I&C infrastructure[19,20].

Smart cities are currently implemented in many countries around the world. They are expected to offer citizens a broad range of intelligent and environmentally friendly services based on leading-edge smart technologies — services that can directly benefit citizens. Providing the intelligent services required of smart cities will entail a wide range of technologies, including sensor enabled information gathering and situational detection and awareness, and also necessitate varied, systematic information-gathering regarding human activities and the operation of non-human entities. The aforementioned characteristics give importance to the role of smart surveillance systems in ensuring successful smart city implementations[1,21,22,23,24,25,26].

What must absolutely be considered for intelligent surveillance systems is the protection of users' privacy. The lack of such consideration for the individuals whose personal data are gathered could result in serious violation of personal information. For example, CCTV surveillance data will provide the viewer with enough information upon which to guess various aspects of the lifestyle of a particular individual: when that person goes out and for how long he or she stays outside home. When collected on each and every resident of a smart city, such private information will enable collective life-logging for the whole city, potentially posing an extremely serious threat to the privacy of citizens. Hence, smart cities must essentially secure privacy protection measures which they implement for CCTV surveillance environments that can guarantee secure privacy protection[2,23,24]..

B. Requirements for CCTV surveillance environments

Accessing any surveillance video data must first ensure secure access control. Accessing the surveillance server in particular must absolutely guarantee the implementation of access control measures with the highest possible degree of security[8-13]. Moreover, it is imperative that a secure authentication approach be applied for the CCTV cameras, the interoperability server, the monitoring client, and other elements of the whole surveillance system. Fail-proof authentication using biometrics such as facial recognition also bears considering. In parallel with strengthened access control, more secure management of personal information is essential when handling surveillance data gathered on the individuals recorded on video. Use of masking and/or other techniques could help protect their privacy against breaching[25,26,27,28,29,30].

C. AES CTR-Mode Encryption

AES-CTR method is to encrypt ti, the ith counter as a certain key, create EK(ctri), and finally create a cryptogam, Ci, by taking calculation of EK(ctri) and XOR with regard to the plain text, Mi. AES-CTR operation mode has the merit that it is optimal for high-speed cryptogam because parallel transaction is possible in the encryption process. However, each size of respective counter has a different encryption vector, so parallel transaction has a limit in the process of encryption and decoding. In this thesis, AES-GCTR mode with the same encryption vector inside the same bucket was proposed and this problem was improved.

III. PROPOSED GCTR-AES ENCRYPTION

A. Abbreviation

Table 1 explains the suggested GCTR-AES encryption operation mode.

Table 1 : Abbreviation

Abbreviation	*Content*
ds	the size of the whole encryption data
sid	the initial value of a bucket I.D.
s	the seed value of pseudorandom numbers
$P(data)_n$	the occurrence value of the nth pseudorandom numbers with Data as the initial value
H(data)	the outcome value of the hash of data

B. Method to extract a bucket ID

Figure 2 shows the size of each bucket and how to create an ID. Prior to this, the sizes of the bucket groups need to be determined. In Figure 2, the size of the bucket group unit was decided as 100. In other words, plural bucket IDs are assigned to one bucket group unit, and each bucket ID has a different bucket size. Here, the bucket size is determined based on pseudorandom numbers with sid as an initial value. Figure 2 below shows five buckets included in one bucket group.

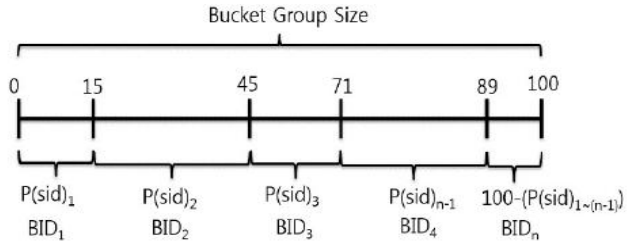

Figure 2 : Bucket Group

The side necessary for pseudorandom numbers can be created as below with the initial seed and the XOR value of the whole encryption data size.

$$sid = H(s) \oplus H(ds) \qquad (1)$$

Figure 3 shows the process of how to encrypt into AES-GCTR operation mode. N buckets belong to one bucket group, and each bucket has the same encryption vector value. Therefore, when partial images are extracted in the unit of a particular bucket, they come to have the same encryption vector value, so can display more efficient encryption performance than AES-CTR mode. In other words, for encryption and decoding, AES-CTR operation mode needs the creation of different encryption vectors for each counter, but the proposed method is efficient because only one time of vector calculation is carried out within the same bucket

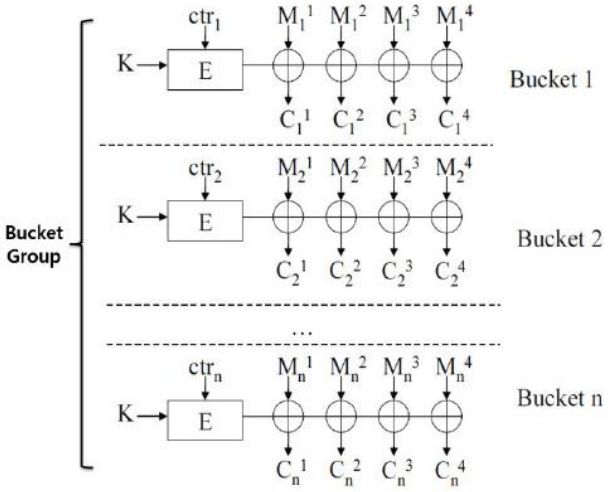

Figure 3 : AES-GCTR Mode

IV. CONCLUSION

In intelligent surveillance environments lie massive threats to security. In the past, the threats took the form of, for instance, insider hackers who attempt to obtain personal information by illegal means. The present-day environments, however, witness not only hackers from within (i.e., a by-product of the information and technology advancements) but also more varied types of threats that are presented from the outside world connected via the Internet, such as systematic technology stealing and illegal information/data collection by hackers. In other words, nowadays the very fact that intelligent surveillance environments are connected wholly to the Internet exposes various information access paths to the threats and could give rise to many unprecedented forms of security threats. Hence, the need for a standardized framework that can safeguard against hacking and insider security breaches that constantly reside in intelligent CCTV surveillance environments.

ACKNOWLEDGMENT

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) [2019-0-00203, The Development of Predictive Visual Security Technology for Preemptive Threat Response]. And, This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2019R1I1A3A01062789). Corresponding Author is Namje Park.

REFERENCES

1. H. Hacigümüş, B. R. Iyer, C. Li, and S. Mehrotra, “Executing SQL over encrypted data in the databaseservice-provider model”, In Proc. ACM SIGMOD Conf. June 2002. DOI : 10.1145/564691.564717
2. Youjin Song, Donghyeok Lee, and et al. "Design of Fast Encryption/Decryption Mechanism for Query in DAS(Database As a Service) Model", Proceedings of the 28th Korea Information Processing Society Fall Conference, 14(2),
3. S. Aramvith, S. Pumrin, T. Chalidabhongse, and S.Siddhichai, "Video Processing and Analysis for Surveillance Applications", in Proc. Int. Symp.Intelligent Signal Processing and Communication Systems pp.607-610, 2009. DOI : 10.1109/ISPACS.2009.5383765
4. Environment", LNCS, Advanced Web and Network Technologies and Applications, 2016, Vol.3842, pp.741-748. https://doi.org/10.1007/11610496_100
5. H. M. Moon and S. B. Pan, "A New Human Identification Method for Intelligent Video Surveillance System", in Proc. IEEE Int. Conf. Computer Communications and Networks, Switzerland, Aug. 2010. DOI : 10.1109/ICCCN.2010.5560021
6. Park, J., Shin, S., Kang, N., “Mutual Authentication and Key Agreement Scheme between Lightweight Devices in Internet of Things”, J. Korea Inf. Commun. Soc., 2013, 38, pp.707–714. DOI : 10.7840/kics.2013.38B.9.707
7. Hae-Min Moon, Sung-Bum Pan, "The Analysis of De-identification for Privacy Protection in Intelligent Video Surveillance System", Journal of Korean Institute of Information Technology 9(7), pp.189-200, 2011.7.
8. Park N, Bang H-C, “Mobile middleware platform for secure vessel traffic system in IoT service environment”, Security Communication Network, 2016, 9(6), pp.500–512. https://doi.org/10.1002/sec.1108
9. H. M. Moon, C. H. Seo, Y. W. Chung, and S. B.Pan, "Privacy Protection Technology in Video Surveillance System", in Proc. Int. Conf. Embedded and Multimedia Computing, pp. 160-165, Dec. 2009. DOI : 10.1109/EM-COM.2009.5402973
10. Lee D, Park N, “Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance”, J Supercomput, 2016, 73(3), pp.1103–1118. https://doi.org/10.1007/s11227-016-1841-5
11. Park N, Hu H, Jin Q, “Security and privacy mechanisms for sensor middleware and application in internet of things (IoT)”, Int J Distrib Sens Netw, 2016. https://doi.org/10.1155/2016/2965438
12. Do-Kim Gwon Woo, Han Jong Wook, “Proceedings of Symposium of the Korean Institute of communications and Information Sciences”, pp. 1623-1624, 2009.
13. Park N, Kang N, “Mutual authentication scheme in secure internet of things technology for comfortable lifestyle”, Sensors, 2016, 16(1), pp.1–16. https://doi.org/10.3390/s16010020
14. Yeonghae Ko, Namje Park, “A Study of IT Centered Smart Grid's STEAM Curriculum and Class for 3rd and 4th Graders in Elementary School”, Journal of the korean association of information education, 2013, Vol.17 No.2 pp.167-175.
15. Jaewan Shin, Shin Dong Kyoo, Shin Dong Il, "Design of Brain-Computer Interface System for User Intention Recognition", Proceedings of Symposium of the Korean Institute of communications and Information Sciences, 2013.6, pp. 790-791
16. Park N, Kim M, “Implementation of load management application system using smart grid privacy policy in energy management service environment”, Clust Comput, 2014, 17(3), pp.653–664.

https://doi.org/10.1007/s10586-014-0367-y
17. Chang Gi Kim, Jeong Min Seo, "An Design and Implementation of Navigation System for Visually Impaired Persons Based on Smart Mobile Devices", JOURNAL OF THE KOREA CONTENTS ASSOCIATION, 2015, 15(1), pp.24-30. DOI : 10.5392/JKCA.2015.15.01.024
18. Park N, “Implementation of inter-VTS data exchange format protocol based on mobile platform for next-generation vessel traffic service system”, Int Inf Inst (Tokyo) Inf, 2014, 17(10A), pp.4847–4856.
19. Dong-Eun Kim, Kwee-Bo Sim, "A Study on the Relation between EEG and Strength for Artificial Hand Control", Proceedings of Symposium of the Korean Institute of Intelligent Systems, 2013.10, pp.121-122.
20. Park N, Park J, Kim H, “Inter-authentication and session key sharing procedure for secure M2M/IoT environment”, Int Inf Inst (Tokyo) Inf, 2015, 18(1), pp.261–266.
21. Dong-Eun Kim, Je-Hun Yu, Kwee-Bo Sim, "EEG Feature Classification for Precise Motion Control of Artificial Hand", Journal of Korean Institute of Intelligent Systems 25(1), pp.29-34, 2015.02. DOI : 10.5391/JKIIS.2015.25.1.029
22. Park N, “Implementation of inter-VTS data exchange format protocol based on mobile platform for next-generation vessel traffic service system”, Int Inf Inst (Tokyo) Inf, 2014, 17(10A), pp.4847–4856.
23. Luo, Ying, Shuiming Ye, and S. Cheung Sen-ching, "Anonymous subject identification in privacy-aware video surveillance", Multimedia and Expo (ICME), 2010 IEEE International Conference on. IEEE, 2010. DOI : 10.1109/ICME.2010.5583561
24. Park N, “Implementation of terminal middleware platform for mobile RFID computing”, Int J Ad Hoc Ubiquitous Comput, 8(4), pp.205–219, 2011, DOI : 10.1504/IJAHUC.2011.043583.
25. Lee Hyun Ju, Shin Dong Il, Shin Dong Kyoo, "A Study on the system design for analysis of EEG signals", Proceedings of Symposium of the Korean Institute of communications and Information Sciences, 2014, pp.610-611
26. Park N, “Performance analysis for VTS-based data exchange protocol in e-navigation environment.”, Int J Multimed Ubiquitous Eng, 11(1), pp.337–344 2016. DOI : 10.14257/ijmue.2016.11.1.32
27. Yong-Hee Lee, Chun-Ho Choi, "Pattern classification of the synchronized EEG records by an auditory stimulus for human-computer interface", Journal of the Korea Institute of Information and Communication Engineering, 12(12), pp. 2349-2356, 2008.
28. Joongheon Kim, Yeong Jong Mo, Woojoo Lee, DaeHun Nyang, "Dynamic Security-Level Maximization for Stabilized Parallel Deep Learning Architectures in Surveillance Applications", Privacy-Aware Computing (PAC), 2017 IEEE Symposium on. IEEE, 2017. DOI :10.1109/PAC.2017.22
29. Namje Park, Donghyeok Lee, “Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment”, Personal and Ubiquitous Computing, pp.1-8, Mar. 2017. DOI : 101007/s00779-017-1017-1
30. Jinsu Kim, Namje Park, Geonwoo Kim, Seunghun Jin, "CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia", Electronics,8(4), pp.412-427, 2019. doi:10.3390/e

AUTHORS PROFILE

Yujin Jung
Dept.of Convergence Information Security, Graduate School, Jeju National University Senior researcher of Creative Education Center Cybersecurity Human Resource Institute yujinjung@jejunu.ac.kr

Won-chi Jung
Jeju Free International City-Development Center Dept. of Convergence Information Security, Graduate School, Jeju National University jwonchi@jdcenter.com

Sangik Oh
Seogwipo City, Dept. of Convergence Information Security, Graduate School, Jeju National University
wnanraitsu58@jejunu.ac.kr

Donghyeok Lee, Ph.D.
Study professor of Cybersecurity Human Resource Institute Dept. of Convergence Information Security, Graduate School, Jeju National University

Professor Namje Park Ph.D.
Professor of Dept. of Computer Education, Teachers College, Dean of Dept. of Convergence Information Security, Graduate School, Jeju National University Director of Cybersecurity Human Resource Institute Director of Creative Education Center.