ARTICLE IN PRESS

Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Secure privacy vault design for distributed multimedia surveillance system

Sk. Md. Mizanur Rahman [b,*], M. Anwar Hossain [a], Mohammad Mehedi Hassan [b], Atif Alamri [b], Abdullah Alghamdi [a], Mukaddim Pathan [c]

[a] College of Computer and Information Sciences (CCIS), King Saud University, Riyadh, Saudi Arabia
[b] Research Chair of Pervasive and Mobile Computing, King Saud University (KSU), Riyadh, Saudi Arabia
[c] Telstra Corporation Limited, 10/35 Collins St, Melbourne, VIC 3000, Australia

HIGHLIGHTS

- Identification of privacy leakage channels by means of privacy leakage trees.
- A secure privacy vault design for distributed surveillance system.
- Robust against different security and privacy attacks.
- Different attack models (White-box, Gray-box, or Black-box) have been considered.

ARTICLE INFO

Article history:
Received 26 December 2013
Received in revised form
17 July 2014
Accepted 9 October 2014
Available online xxxx

Keywords:
Distributed multimedia surveillance system
Video surveillance
Privacy-preserving surveillance
Data hiding
Secure privacy vault

ABSTRACT

Distributed multimedia surveillance systems utilize heterogeneous sensors such as cameras, motion sensors, sound sensors, and RFID in order to provide safety and security to people. However, due to the potential of exposing privacy by these systems, many people are reluctant to be electronically monitored and suffer from privacy loss. In order to overcome this dilemma, the current surveillance systems should adopt improved privacy preservation (i.e. hiding people's face) mechanism while they are used for typical surveillance tasks. This paper takes a holistic approach to identify the different privacy leakage channels in the distributed video surveillance context and proposes the design of a secure privacy vault to conceal privacy-sensitive data obtained from distributed visual sensors. It also shows how the proposed solution helps to mitigate the potential privacy leakage problems at different levels of the leakage channels. In order to demonstrate the viability of the proposed approach, we further provide the privacy leakage attack model as well as the security analysis of the proposed solution.

1. Introduction

Recently, we witness a significant interest in surveillance technologies due to the increased security threats around our surroundings. As a result, distributed multimedia surveillance systems are being deployed in different premises to ensure public safety and security. However, the increased presence of these systems often lead to privacy violation (i.e. exposing privacy-sensitive information) that is sensitive issue to civil liberty [1,2]. Therefore, it is important to develop improved privacy preserving technique for the surveillance systems such that these systems can be used for effective surveillance tasks while protecting people's privacy at the highest level.

Researchers have been investigating several approaches to address the privacy preservation issues. Dominant approaches are scrambling and data hiding methods [3–8], cryptographic encryption [2,9], and access control policy [10,11]. The scrambling and data hiding approaches usually first identify the regions of interest in video data that are potentially privacy-sensitive, and scramble that region to minimize the chance of privacy leakage. The cryptographic encryption approach, among other things, hides privacy information of video using watermark, while the access control strategy restricts the access of surveillance feeds to authorized users only.

Despite the above works, there is still a lack of a formal and comprehensive framework towards effective privacy preservation. At one hand, we need improved method for privacy safeguarding,

* Corresponding author. Tel.: +966 11 4676394.
E-mail addresses: mizan@scientist.com, mizan@ksu.edu.sa (Sk. Md. Mizanur Rahman).

http://dx.doi.org/10.1016/j.future.2014.10.019
0167-739X/

while on other hand we need to be aware of the different privacy leakage points. In this proposal, we updated our previous work [12] and provide a privacy leakage channel analysis for distributed surveillance system and developed a secure privacy vault to keep the secret keys of scrambled privacy sensitive regions of interest in distributed surveillance video.

This paper identifies privacy leakage channels by means of privacy leakage tree analysis and proposes the mitigation of these leakage channels by designing a secure privacy vault for distributed surveillance system. Thus, the main contribution lies in the design of a secure privacy vault, which preserves the privacy information securely. The cornerstone of this approach is that even if the privacy vault is stolen, the privacy information cannot be disclosed to the public by breaking the vault without compromising the higher level authorities of the target environments. Considering the different attack models, such as White-box, Gray-box, or Black-box, the proposed privacy vault can be implemented in different hostile environments to protect the privacy information in the surveillance video footage.

The remainder of the paper is organized as follows. Section 2 explores some related work followed by the description of background mathematics in Section 3 to clearly understand the proposed mechanism. The analysis of the privacy leakage channels is discussed in terms of privacy leakage tree (PLT) in Section 4. The overview of the proposed privacy preserving mechanism of a distributed multimedia surveillance system is given in Section 5. The privacy leakage attack model is elaborated in Section 6, while the security analysis of the proposed model is illustrated in Section 7. Finally, the conclusion is drawn in Section 8.

2. Related work

There are several related works that have a common goal of concealing privacy sensitive information to minimize privacy loss due to wide scale surveillance. These falls into the category of scrambling and data hiding, cryptographic encryption, and access control. We briefly comment on these works in the following.

Dufaux and Touradj Ebrahimi [3] proposed a code stream-domain scrambling technique that provides better scrambling result based on code-stream transformation, which pseudo randomly inverts some of the bits of AC coefficient in the target Region of Interest (ROI). Hosik Sohn et al. [13] propose a surveillance system that provides scalable video coding, ROI scrambling, and compressing. In this approach, first the images are split using Flexible Macroblock Ordering (FMO), then the FMO type 2 (rectangles over areas of ROI) are applied. The spliced sets are then forwarded to ROI scrambling and pseudo random sign inversion to AC coefficients. Shen Jie and Zheng Xiao Yu [4] describe that using the public key of the receiver the sender computes symmetric key to encrypt the seeds, the digital envelope is made by receivers public key. The receiver opens the envelope using its private key and obtains symmetric key and sends acknowledgment to sender. Sender sends scrambled seeds to the receiver and receiver uses symmetric key to decrypt the seeds and decode the scrambled coefficients.

Like the scrambling techniques, which aim to scramble the ROIs in surveillance videos, data hiding is another technique that aims the same. Isabel Martinez-ponte et al. in [6] proposed a face masking technique to hide faces in motion JPEG data. M.D. Swanson et al. [14] proposed a technique to hide high bit-rate supplementary data by pixels in the video format. Moncrieff et al. [8] suggest general techniques like data hiding, context awareness, data equity to embedded into surveillance systems to ensure that the privacy of the people is safeguarded against the increasing number of attacks on the surveillance systems. Authors in [15] proposed a compression independent approach to selectively encrypt regions that reveal identity using permutation-based encryption in the pixel domain. The work in [16] uses an obfuscation technique that uses a video console to determine the sensitive parts of the video and obscures that part in a way that the recognition software cannot identify that part. This approach is irreversible and hence is not suitable for actual surveillance needs. Another approach in [17] proposed to decrease the quality of ROI in JPEG2000, which ensures varying visual quality from poor to near invisibility. It works in bitstream domain and dependent on compression standard used. This approach is also irreversible and hence does not meet critical surveillance needs.

In our earlier work [2] we adopted cryptographic approach to also hide privacy sensitive ROIs in surveillance video. This technique takes inputs from the video surveillance data and compresses the RoI using the Chaos Encryption based on the logistic functions and mappings. J.M. Rodrigues et al. [9] proposed a method to partially encrypt the face in video sequence. This method is based on Advanced Encryption Standard (AES) stream ciphering using variable length coding of the Huffman's vector. Besides, Newton et al. [18] used a de-identification technique to hide face regions, which prevents traditional face recognition techniques to identify the original face. The actual hiding of face is done by blacking out the face. However, their approach conserves several facial properties such as eigenvectors of the original face and based on the similarity matrix of the faces they restore new faces that resemble the original face but not exactly the same as the original.

Video surveillance privacy and confidentiality are also addressed using sophisticated access control policy with which sensitive information embedded video segments will only be accessed by authorized personnel [10,19]. This approach is restricted in the sense that all the surveillance operators will require adequate access rights in order to continue monitoring the video footage and hence privacy concerns will be compromised. In a recent work [20], a different approach to privacy loss protection in surveillance is proposed, which emphasizes on identifying the location, time and activities in video footage in addition to people's faces. Unlike the above works, we identify the privacy leakage channels in video surveillance from video capture to video storage and access and propose a secure privacy vault that preserves the key information to hide the privacy sensitive regions in video.

3. Mathematical background

3.1. Discrete Cosine Transformation (DCT)

Discrete Cosine Transformation (DCT) [21] is used to compress MPEG-4 video [22] by applying on 8×8 pixel blocks. In a matter of fact, DCT is a linear and invertible function, defined as $f : \Re^N \longrightarrow \Re^N$. Equivalently, it is defined as an $N \times N$ invertible square matrix. Thus, let $F(x) \longrightarrow \alpha(\theta)$ and $G(x) \longrightarrow \beta(\theta)$, then $C_1F(x) + C_2G(x) \longrightarrow C_1\alpha(\theta) + C_2\beta(\theta)$.

3.2. Pseudo-Hadamard Transformation (PHT_r)

Consider the N-bit integers x, y, χ, and γ, i.e., $|x| = |y| = |\chi| = |\gamma| = N$. Let, transformation of x is denoted as $PT_r(x) = \chi$ and the transformation of y is denoted as $PT_r(y) = \gamma$. Therefore, the inverse transformation of χ, denoted as $PT_r^{-1}(\chi) = x$, and the inverse transformation of γ, denoted as $PT_r^{-1}(\gamma) = y$. Thus, the transformed x can be computed as $\chi = (x+y) \ mod \ 2^N$; and transformed y can be computed as $\gamma = (x + 2y) \ mod \ 2^N$. On the other hand x, and y can be computed from χ and γ as $x = (2\chi - \gamma) \ mod \ 2^N$ and $y = (\gamma - \chi) \ mod \ 2^N$, respectively. Detail description on Pseudo-Hadamard Transformation can be found in [18].

Please cite this article in press as: Sk. Md. Mizanur Rahman et al., Secure privacy vault design for distributed multimedia surveillance system, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.019

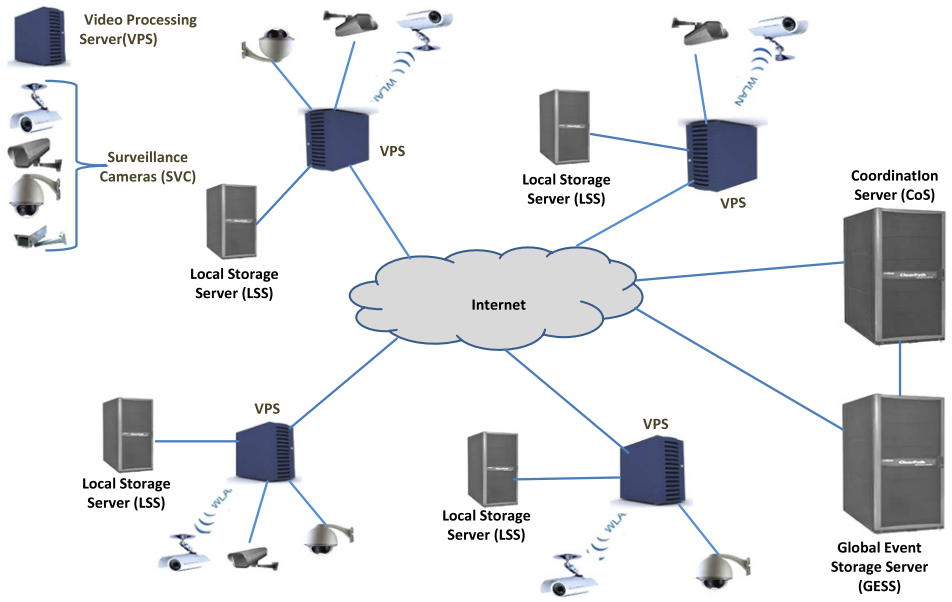

Fig. 1. Enterprise level architecture of the proposed distributed multimedia surveillance system network.

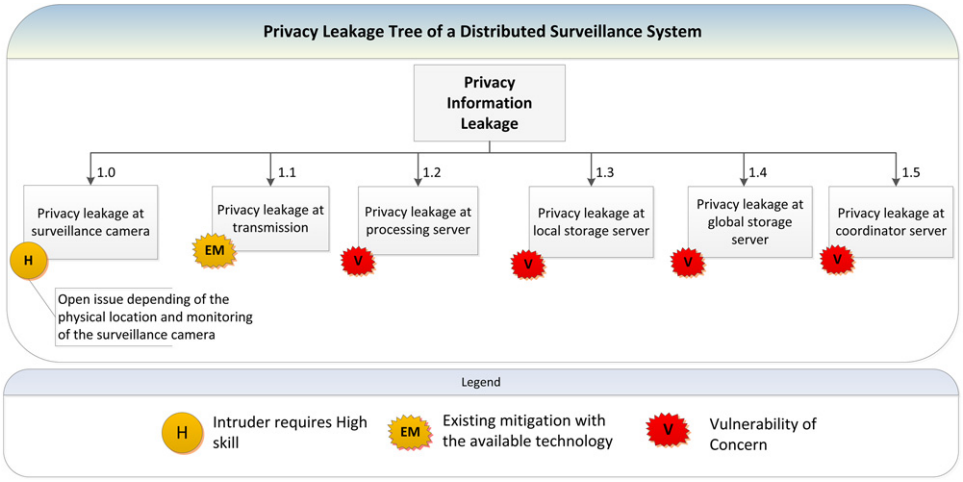

Fig. 2. Privacy leakage tree of a distributed surveillance system.

4. Privacy leakage channels identification

Privacy leakage can occur at different levels of an enterprise level distributed multimedia surveillance systems. Fig. 1 shows the architecture of such a system. A surveillance system at a site consists of (1) surveillance cameras (SVC), (2) video processing server (VPS), (3) local storage server (LSS), (4) global event storage server (GESS), and (5) coordination server (CoS). SVCs (IP cameras) are connected to VPS through wireless or wired medium. The VPSs are connected to the LSS. Finally, GESS is connected to the CoS and they are accessible through the internet by the other servers.

A secure channel is established between the SVC and VPS whenever they want to communicate, based on the availability of the IP camera technologies. Each session of the communication between VPS and the LSS is performed using secure cryptographic communication protocol over the internet, namely, Secure Sockets Layer (SSL). Similarly, the security of communication between VPS and GESS as well as between VPS and CoS will be enforced.

The privacy leakage channels of the enterprise level architecture is identified with the help of several privacy leakage trees and are analyzed in the following subsections. The leaf nodes in the privacy leakage tree represents the mitigation techniques. The proposed mitigation techniques to counter the privacy leakage channels is described in Section 5.

4.1. Privacy leakage channels of a distributed surveillance system

The highest level privacy leakage tree of a distributed surveillance system is illustrated in Fig. 2. The vulnerability of the concerned channels are also pointed out in this figure.

A summary of the leakage likelihood and impact severity in the privacy leakage tree of a distributed surveillance system is illustrated in Table 1. The privacy threat at node 1.0 and 1.1 are tampering with the surveillance cameras and on the communication path. The mitigation is provided by the existing robust solution. The impact severity of these nodes are high, as the assets of the target system are directly related to the privacy information. On the other hand likelihood is low, as the attacker needs very high skill to get the privacy information. Nodes 1.2–1.5 are the concern of existing vulnerabilities and the mitigation is provided by the proposed technique and it is discussed in detail in Section 7.

Please cite this article in press as: Sk. Md. Mizanur Rahman et al., Secure privacy vault design for distributed multimedia surveillance system, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.019

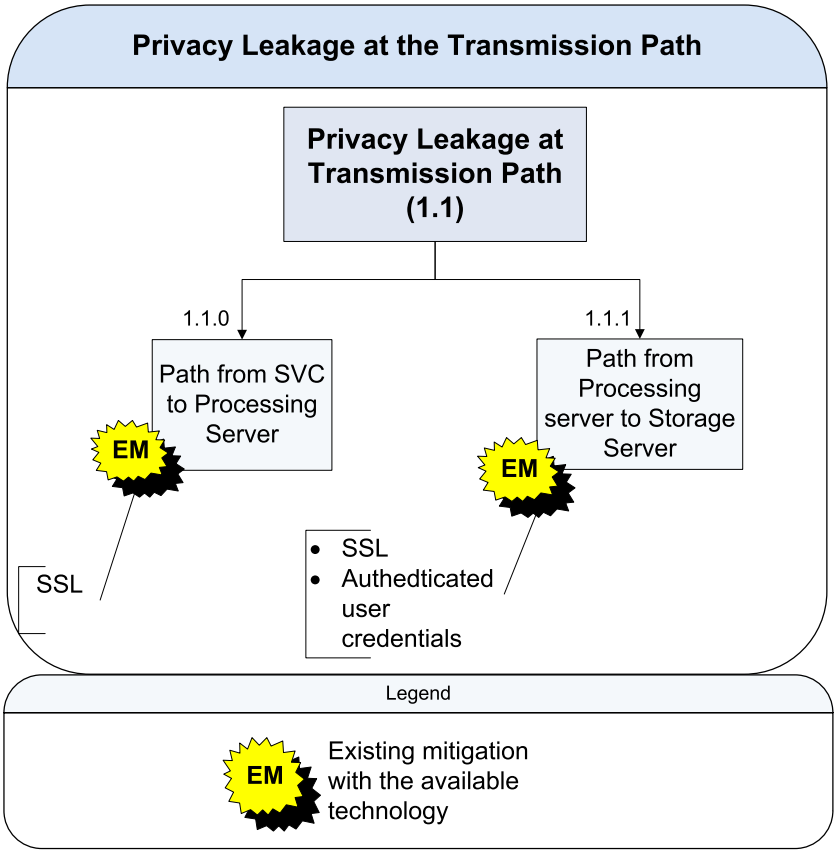

Fig. 3. Privacy leakage tree for the transmission path.

Table 1
Summary of the highest level leakage tree of a distributed surveillance system.

Node	Privacy threat	Likelihood	Impact severity
1.0	Tampering	Low (High skill)	High
1.1	Tampering	Low (High skill)	High
1.2	Information disclosure, tampering	Low	High
1.3	Information disclosure, tampering	Low	High
1.4	Information disclosure, tampering	Low	High
1.5	Information disclosure, tampering	Low	High

4.2. Privacy leakage during transmission

The privacy leakage tree for the transmission path is illustrated in Fig. 3. The vulnerability and the corresponding mitigation of the target channels are depicted into the tree.

A summary of the leakage tree during transmission in terms of leakage likelihood and impact severity is illustrated in Table 2. The privacy threat at node 1.1.0 and 1.1.1 are the shimming at and the snipping on the channels. The robust existing solutions provide mitigation for these kinds of passive and active attacks. Similar to the previous Table 1, the impact severity and the likelihood of these nodes (1.1.0 and 1.1.1) are high and low respectively, and the reasons are already discussed in the previous section.

Table 2
Summary of the leakage tree during transmission.

Node	Privacy threat	Likelihood	Impact severity
1.1.0	Tampering	Low (High skill)	High
1.1.1	Tampering	Low (High skill)	High

4.3. Privacy leakage at the processing server

The privacy leakage tree for the video processing server is shown in Fig. 4. The mitigation for the vulnerable of concerned channels are given as well.

Privacy information leakage from secure bucket will be a severe threat and will have serious impact on the system. As the header of the secure bucket is encrypted with AES and the key is generated from the private parameters produced by the high level authorities of the system, it is assumed to be secure. Because, there is no practical feasible attack available on AES encryption algorithm. If the system runs in a hostile environment where intruder has the accessibility on the system, then the suggested AES implementation is AES white-box implementation to protect the content of the secure bucket. The only way to find the privacy information is by compromising the high level authorities of the system, which is assumed to be infeasible. The proposed mitigation approach is to be applied at the nodes 1.2.0, 1.2.1 and 1.2.2.

The summary of the privacy leakage tree for the processing server with regard to leakage likelihood and impact severity are mentioned in Table 3. The impact severity is high, because the assets of the proposed system is the privacy related information or data which is the main target of an attacker. On the other hand the likelihood is low as the attackers need very high skill, if it

Please cite this article in press as: Sk. Md. Mizanur Rahman et al., Secure privacy vault design for distributed multimedia surveillance system, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.019

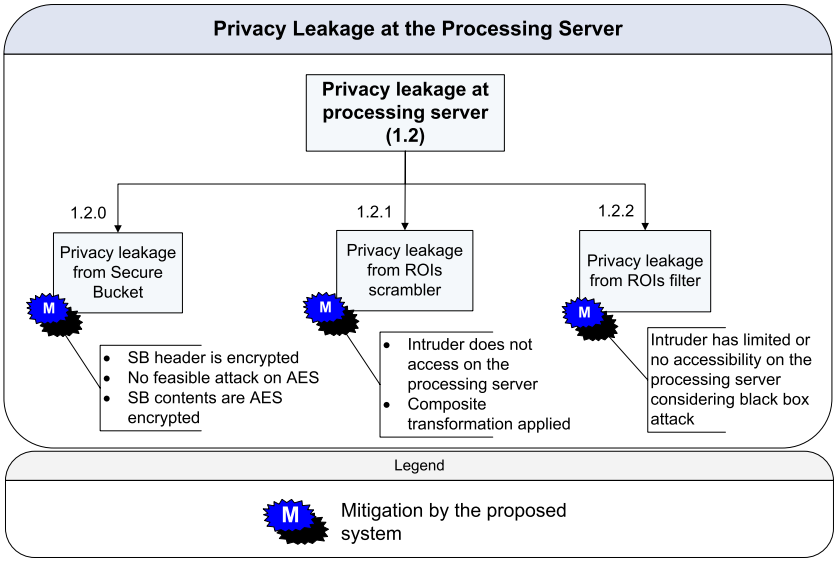

Fig. 4. The privacy leakage tree for the processing server.

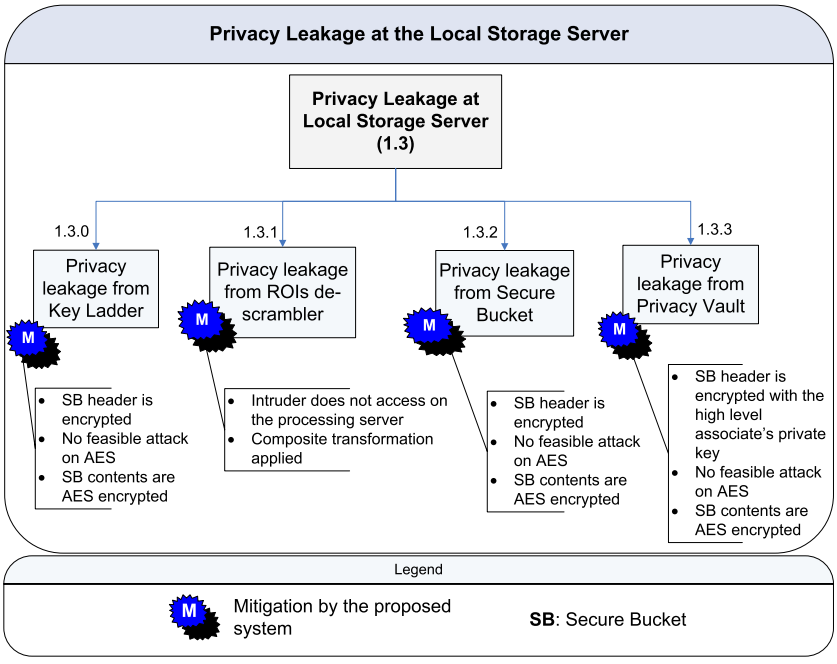

Fig. 5. Privacy leakage tree for the local and global storage server.

Table 3
Summary of the processing server privacy leakage tree.

Node	Privacy threat	Likelihood	Impact severity
1.2.0	Information disclosure, tampering	Low (High skill, infeasible)	High
1.2.1	Information disclosure, tampering	Low (High skill, infeasible)	High
1.2.2	Information disclosure, tampering	Low (High skill, infeasible)	High

considered as a white-box attack scenario or infeasible, in the case of black-box attack scenario.

4.4. Privacy leakage at local and global storage servers

The privacy leakage tree for the global and local storage servers is shown in Fig. 5. The mitigation for vulnerable of concerns are also illustrated in this figure.

The proposed mitigation technique is to be applied at the nodes 1.3.0, 1.3.1, 1.3.2 and 1.3.3. Similar to the case of processing server, privacy leakage from the secure bucket for the storage server is assumed to be infeasible.

The summary of the leakage tree for the local and global storage server is given in Table 4. The impact severity is high, due to the assets of the target system are directly related to the privacy related data and information those are the main concern for the

Please cite this article in press as: Sk. Md. Mizanur Rahman et al., Secure privacy vault design for distributed multimedia surveillance system, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.019

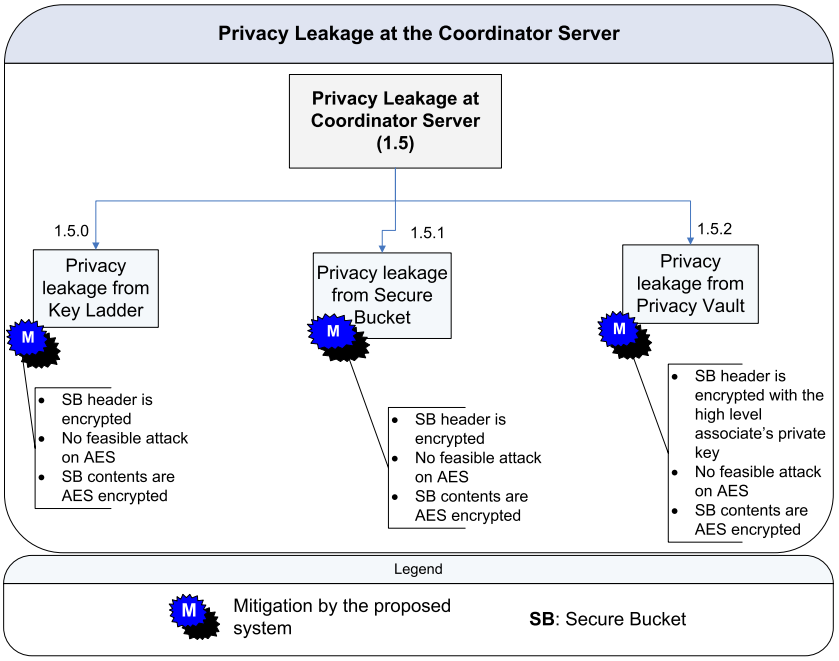

Fig. 6. Privacy leakage tree for the coordinator (CoS) server.

Table 4
Summary of the leakage tree for the local and global storage servers.

Node	Privacy threat	Likelihood	Impact severity
1.3.0	Tampering	Low (High skill, infeasible)	High
1.3.1	Information disclosure, tampering	Low (High skill, infeasible)	High
1.3.2	Information disclosure, tampering	Low (High skill, infeasible)	High
1.3.3	Information disclosure, tampering	Low (High skill, infeasible)	High

Table 5
Summary of the leakage tree for coordinator server.

Node	Privacy threat	Likelihood	Impact severity
1.5.0	Tampering	Low (High skill, infeasible)	High
1.5.1	Information disclosure, tampering	Low (High skill, infeasible)	High
1.5.2	Information disclosure, tampering	Low (High skill, infeasible)	High
1.5.3	Information disclosure, tampering	Low (High skill, infeasible)	High

intruder. On the other hand the likelihood is low and/or infeasible based on the consideration of the attack scenarios.

It should be noted that the privacy mitigation technique for global event storage server (GESS), follows the same approach as that of local and global storage servers.

4.5. Privacy leakage at the coordinator server

The privacy leakage tree for the coordinator server is shown in Fig. 6. The vulnerability of concerns and the corresponding mitigation are illustrated in this figure.

The proposed mitigation technique is to be applied at the nodes 1.5.0, 1.5.1, and 1.5.2. Similar to the case of processing server, privacy leakage from the secure bucket for the storage server is assumed to be infeasible.

The summary of the leakage tree for the local storage server is given in Table 5. So far, the main target of an attacker is on the assets of the system, i.e., the privacy related data or information of the surveillance system, that is the reason the for high impact severity. On the other hand the likelihood is low and/or infeasible based on the scenarios (black-box, white-box) that the attacker might consider.

5. The proposed privacy leakage mitigation approach

Here, we discuss the proposed technique in terms of high-level and component-level design methodology applicable to counter privacy leakage at different leakage channels.

5.1. High-level design methodology

The high-level design methodology shows the different processes and components used as part of the proposed privacy preserving solution. This includes the Privacy Information Processing and Preservation Filter (PIPPF), situated at VPS and consists of (1) ROI processing filter, (2) ROI scrambler, and (3) Secure bucket, and illustrated in Fig. 7. Clear video stream (e.g., MPEG-4) comes from SVC through an encrypted channel to the VPS.

ROI processing filter takes clear video stream as input and computes the parameters of the region of interest which describe the RIOs based on the target of the system, e.g., face, gait detection

Please cite this article in press as: Sk. Md. Mizanur Rahman et al., Secure privacy vault design for distributed multimedia surveillance system, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.019

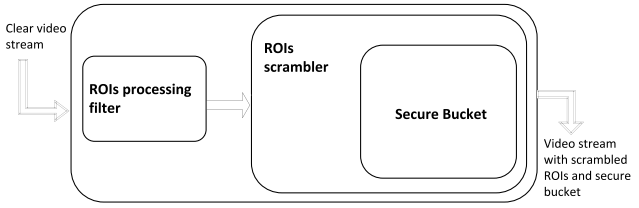

Fig. 7. Privacy information processing and preservation filter.

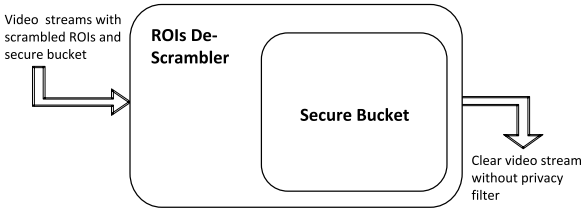

Fig. 8. Reverse processing of scrambled ROIs.

etc. To detect these ROIs (e.g., face, gait, etc.) there are existing algorithms available in the market [23].

ROI scrambler, takes the ROIs parameters together with the video stream, scrambles the RIOs by applying scrambler transformation (S_{TR}) on the RIOs, and keeps the ROIs parameters and the S_{TR}'s parameter into a secure bucket. Finally, the scrambled RIOs video stream and the secure bucket are sent to the LSS over SSL. In fact, the Secure Bucket might be sent to the LSS within a system defined time interval, T_1.

Reverse processing of scrambled ROIs (RPSR) is designed in LSS and consists of (1) region of interest de-scrambler and (2) secure bucket which is illustrated in Fig. 8.

The ROI-scrambled video stream comes from VPS to LSS over SSL connection. ROI de-scrambler takes ROI-scrambled video stream from the LSS together with the Secure Bucket, extracts ROIs parameters and S_{TR}'s parameter from the Secure Bucket and applies the inverse transformation of S_{TR}, S_{TR}^{-1} on the ROIs and descrambles the RIOs to produce the clear video stream.

The detail design methodologies of the components, e.g., scrambler transformation (S_{TR}), inverse transformation of S_{TR}, secure bucket, key ladder, privacy vault, which are used in internal architecture are discussed in detail in the next section.

5.2. Component level design methodologies

This section includes the discussion on internal components of the high-level design.

5.2.1. Scrambler transformation (S_{TR}) and de-scrambler transformation (S_{TR}^{-1})

Changing coefficient of the discrete cosine transformation (DCT), changes can be done on all the 8×8 pixel block of a MPEG-4 video frame. Let us change DCT coefficient i by j and defined this changed 8×8 matrix as $M_i^j(x)$. Thus, changing each DCT coefficient by $\lambda(j)$, change after inverse DCT can be represented as $M(x) = \lambda(0)M_i^0(x) + \lambda(1)M_i^1(x) + \lambda(2)M_i^2(x) + \cdots + \lambda(63)M_i^{63}(x)$. On the other hand by subtracting $M(x)$ from the inverse DCT operation changes on each 8×8 pixel matrix can be eliminated.

The partial scrambler transformation, denoted as PS_{TR}, is computed by changing the DCT coefficient of 8×8 pixel block of a MPEG-4 video frame. The opposite procedure, i.e., subtracting the changing matrix from the inverse DCT is the partial inverse transformation, denoted as PS_{TR}^{-1}.

Finally, scrambler transformation, S_{TR} can be computed as the composition of PS_{TR} and PT_r, where PT_r is defined in Section 3.2; hence, $S_{TR} = PS_{TR} \circ PT_r$.

On the other hand de-scrambler transformation S_{TR}^{-1} can be computed as the composition of PT_r^{-1} of Section 3.2 and PS_{TR}^{-1}; hence $S_{TR}^{-1} = PT_r^{-1} \circ PS_{TR}^{-1}$.

5.2.2. ROI scrambler and ROI de-scrambler

Receiving ROIs parameter from PIPPF, region of interest scrambler determines the region of interest and its corresponding macroblock and blocks. ROI Scrambler applies Scrambler Transformation (S_{TR}) on the intra-frame blocks of the I-frames of clear MPEG-4 video stream. Region of Interest Scrambler keeps the transformation parameters and the ROIs parameter into a secure bucket. The transformation parameters are changed dynamically based on the system defined time frame T_1.

Receiving ROIs parameter from corresponding secure bucket, ROI De-scrambler applies S_{TR}^{-1} on the ROIs of the scrambled video stream.

5.2.3. Secure bucket

Secure Bucket is consists of (1) a secure header, (2) a secure table of contents (TOC) and (3) secure blocks.

The header of the Secure Bucket is encrypted with AES encryption and the encryption key is a dynamic secret key (H_{SK}) generated from system and super users' parameters. It has a unique identity of multiple bytes of length with a sub identity to distinguish form each other. The sub identity is generated on the basis of system defined time interval, T_1. It contains the encryption key (TB_{SK}) to encrypt and decrypt the table of contents (TOC) and the secure blocks.

Each TOC entity is multiple bytes of length and carries specific information to be stored in the secure blocks, in other words TOC entities are the headers of the secure blocks. It is encrypted with the TB_{SK}.

Secure blocks are the actual data of each of the TOC entity. Each of the blocks is a variable length of bytes with specific identifiers at the beginning and at the end and padded with an error checking bytes after the ending identifier. To generate the identifiers, secure hash algorithm (SHA) is a good candidate. It is also encrypted with the TB_{SK}.

5.2.4. Key Ladder (KL)

The Key Ladder is designed to keep the dynamic keys in the storage server. It is a secure bucket where the dynamic keys are kept permanently for a specified time period.

5.2.5. Privacy vault

It is the secure bucket where the header encryption key of secure bucket is kept. The header encryption key is derived from the private parameters, defined by the top level associates of a system. It contains all the secure buckets and the key ladders.

6. Privacy leakage attack models

In this section we discuss implementation techniques of our proposed methodology based on the access rights of the users in the system and different attack models. We provided two alternatives of white-box attack model with the rationale that if an organization requires moderate security measures, it might choose the gray box or black box model without consider the much heavier approach such as white-box.

6.1. Black box attack model

Black Box attack model is a traditional model which assumes that the attacker has no physical access to the key or any internal working principle of an encryption or decryption algorithm or

a scrambler or descrambler techniques. In this model an attacker can only observe external information and behavior, i.e., external input and output. This information consists of either the plain image (input) or the cipher image (output) of the system while assuming zero visibility on code execution and dynamic scrambling operations [24].

Considering this attack model our proposed method can be implemented using the existing available AES implementation combining the implementation of our proposed techniques using any suitable high level language.

6.2. Gray box attack model

The Gray box attack scenario assumes that the attacker has partial physical access to the Key or that it is leaking so called side channel information. Side Channel Analysis attacks (SCA) exploit information leaked from the physical implementation of a cryptographic system. The leakage is passively observed via timing information, power consumption, electromagnetic radiations, etc. Protection against Side Channel Attacks is important because the attacks can be implemented quickly and at a low cost. Publicly available side channel information allows hackers to effectively reveal parts of the Key and as a result dramatically reduce its efficacy and demote the overall protection [24].

Gray box cryptography is in fact a by-product of the traditional Black box implementation. It has been shown that even smart cards, perceived as being able to provide strong security, performing internal cryptography are in reality leaking information to the outside world. It is clear then that scenarios assumed to be a Black box are in reality only a shade of gray.

Considering this attack model our proposed method can be implemented using the existing available AES implementation combining the implementation of our proposed techniques using any suitable high level language.

6.3. White box attack model

The white box attack scenario, in contrast with previously described scenarios, handles far more severe threats while assuming internal hackers (legitimate users of the system) have full visibility and control over the whole operation. Hackers can freely observe dynamic code execution (with instantiated cryptographic keys) and internal algorithm details are completely visible and alterable at will. Despite of this fully transparent methodology, White box cryptography integrates the cipher in a way that does not reveal the key.

It is therefore clear that algorithms built for both Black and Gray box models are impractical in the face of operating on non-trusted hosts. Understandably, hackers will not try to break the cipher by only using the means available in Black and Gray box scenarios, instead they will observe the execution when the unprotected key is used directly stealing it. Traditional cryptography algorithms, as exposed in the White box scenario, assume the presence of the key as part of the implementation. The White box cryptography algorithm is protected in the White box scenario, as the key is not present in memory and cannot be extracted not even dynamically. Choosing the most appropriate, most secure cryptographic model is therefore the sole line of defense against malicious threats precisely what White box cryptography attempts to achieve [24].

Considering this attack model our proposed method can be implemented using the existing available AES implementation combining the implementation of our proposed techniques using any suitable high level language.

7. Security analysis

Considering the privacy leakage tree of a distributed surveillance system, illustrated in Fig. 2, the proposed technique mitigates the vulnerability of concerns of the nodes 1.2, 1.3, 1.4 and 1.5. Node 1.2 further discussed in detail in Section 4.3. To protect the privacy information of the assets of the system, i.e., the privacy related data and information, a secure bucket is designed in the proposed method. A secure bucket consist of the combination of some secure components, such as, secure header; secure table of contents; and secure blocks. Secure header of the secure bucket is encrypted with Advanced Encryption Standard (AES) [25] and the key for the AES engine is generated from the system specific private parameters, and maintained by the high level authorities of the system; it is assumed to be secure, considering both black box and white box attack scenario. Because, there is no practical feasible attack available on AES encryption algorithm that can break the AES engine and reveal the header of the secure bucket. In the case of Black box attack scenario, the corresponding AES implementation's specification available in [25], which is enough to protect the attack. In the case of white box attack scenario, i.e., if the system runs on an open environment where an attacker has the complete accessibility into the system, then the suggested white box AES implementation is available in the literature [26] that would be enough to protect the secure bucket. The only way to find the privacy information is by compromising the high level authorities of the system, which is, in fact an open problem. Similar approach is effective for other nodes as well.

8. Conclusion

This paper proposes a privacy preserving technique to safeguard privacy-sensitive information that might be exposed through different leakage channels in a distributed video surveillance system. A privacy vault is designed based on Hadamard and Discrete Cosine Transformation in order to counter such privacy leakage. The proposed privacy vault design ensures that privacy information will not be disclosed even when the vault is stolen. However, it can only be disclosed by compromising the top level authorities of the system, which is infeasible. Detail security analysis and the implementation guidelines for hostile environment are also described in this paper. The future work will concentrate on implementing the proposed technique in real-world multimedia surveillance environment.

Acknowledgment

This work was supported by NSTIP strategic technologies program number (11-INF1830-02) in the Kingdom of Saudi Arabia.

References

[1] Q.M. Rajpoot, C.D. Jensen, Security and privacy in video surveillance: requirements and challenges, in: ICT Systems Security and Privacy Protection, Springer, 2014, pp. 169–184.
[2] S.M.M. Rahman, M.A. Hossain, H. Mouftah, A. El Saddik, E. Okamoto, Chaos-cryptography based privacy preservation technique for video surveillance, Multimedia Syst. 18 (2) (2012) 145–155.
[3] F. Dufaux, T. Ebrahimi, Scrambling for privacy protection in video surveillance systems, IEEE Trans. Circuits Syst. Video Technol. 18 (8) (2008) 1168–1174.
[4] S. Jie, Z. XiaoYu, Security for video surveillance with privacy, in: IEEE International Conference on Internet Technology and Applications, 2010, pp. 1–4.
[5] F. Dufaux, T. Ebrahimi, A framework for the validation of privacy protection solutions in video surveillance, in: IEEE International Conference on Multimedia and Expo, ICME, 2010, pp. 66–71.
[6] I. Martínez-Ponte, X. Desurmont, J. Meessen, J. Delaigle, Robust human face hiding ensuring privacy, in: International Workshop on Image Analysis for Multimedia Interactive Services, WIAMIS, 2005, pp. 46–53.
[7] W. Zhang, S. Cheung, M. Chen, Hiding privacy information in video surveillance system, in: Proceedings of the 12th IEEE International Conference on Image Processing, 2005, pp. 868–871.
[8] S. Moncrieff, S. Venkatesh, G.A. West, Dynamic privacy in public surveillance, Computer 42 (9) (2009) 22–28.
[9] J.M. Rodrigues, W. Puech, P. Meuel, J. Bajard, M. Chaumont, Face protection by fast selective encryption in a video, in: The Institution of Engineering and Technology Conference on Crime and Security, 2006, pp. 420–425.
[10] B. Thuraisingham, G. Lavee, E. Bertino, J. Fan, L. Khan, Access control, confidentiality and privacy for video surveillance databases, in: Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies, ACM, 2006, pp. 1–10.

[11] S. Moncrieff, S. Venkatesh, G. West, Dynamic privacy assessment in a smart house environment using multimodal sensing, ACM Trans. Multimedia Comput. Commun. Appl. (TOMCCAP) 5 (2) (2008) 10.
[12] M. Hossain, S.M.M. Rahman, Towards privacy preserving multimedia surveillance system: a secure privacy vault design, in: 2013 International Symposium on Biometrics and Security Technologies (ISBAST), IEEE, 2013, pp. 280–285.
[13] H. Sohn, E. AnzaKu, W. De Neve, Y.M. Ro, K. Plataniotis, Privacy protection in video surveillance systems using scalable video coding, in: Sixth IEEE International Conference on Advanced Video and Signal Based Surveillance, AVSS, 2009, pp. 424–429.
[14] M. Swanson, B. Zhu, A. Tewfik, Data hiding for video-in-video, in: Proceedings of the IEEE International Conference on Image Processing, vol. 2, 1997, pp. 676–679.
[15] C. Paula, K. Hari, M. Spyros, Compression independent reversible encryption for privacy in video surveillance, EURASIP J. Inf. Secur. (2009).
[16] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Y. Tian, A. Ekin, Blinkering surveillance: enabling video privacy through computer vision, IBM Technical Paper, RC22886 (W0308-109).
[17] D. Chen, Y. Chang, R. Yan, J. Yang, Tools for protecting the privacy of specific individuals in video, EURASIP J. Adv. Signal Process. (2007).
[18] T. St Denis, Fast pseudo-hadamard transforms, Tech. rep., Cryptology ePrint Archive, Report 2004-010, 2004.
[19] P. Birnstill, A. Pretschner, Enforcing privacy through usage-controlled video surveillance, in: 10th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), IEEE, 2013, pp. 318–323.
[20] M. Saini, P.K. Atrey, S. Mehrotra, M. Kankanhalli, W3-privacy: understanding what, when, and where inference channels in multi-camera surveillance video, Multimedia Tools Appl. 68 (1) (2014) 135–158.
[21] N. Ahmed, T. Natarajan, K.R. Rao, Discrete cosine transform, IEEE Trans. Comput. C-32 (1974) 90–93.
[22] H. Chen, Thesis paper: Transcoding of MPEG-4 compressed video, 2003.
[23] R. Lienhart, J. Maydt, An extended set of haar-like features for rapid object detection, in: Proceedings IEEE International Conference on Image Processing, vol. 1, 2002, pp. 1–900.
[24] anonymous, Understanding white box cryptography whitepaper, Safenet-WhitePaper WP (EN)- (03.29.12), 2012, pp. 1–6.
[25] anonymous, Advanced encryption standard (AES) (FIPS PUB 197), Department of Commerce, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL) FIPS PUB (197), 2001, pp. 1–51.
[26] J.A. Muir, A tutorial on white-box AES, 2013. URL: http://eprint.iacr.org/2013/104.

Sk. Md. Mizanur Rahman is an Assistant Professor in Information System Department in the College of Computer and Information Sciences at King Saud University, KSA. Prior to his current appointment, he worked for several years in cryptography and security engineering in the high-tech industry in Ottawa, Canada. He also worked as a postdoctoral researcher for several years in University of Ottawa, University of Ontario Institute of Technology (UOIT), and University of Guelph, Canada. He completed a Ph.D. in Risk Engineering (Major: Cyber Security Engineering) in the Laboratory of Cryptography and Information Security, Department of Risk Engineering, University of Tsukuba, Japan, on March 2007. Information Processing Society Japan (IPSJ) awarded Dr. Rahman with "IPSJ Digital Courier Funai Young Researcher Encouragement Award" for his excellent contribution in IT security research. He completed an M.Sc. and a B.Sc. (Hons) in Computer Science, securing first class first with distinction marks in both the programs and awarded with "Gold Medal" for the result of excellence. Primary research interest of Dr. Rahman is on Cryptography, Software Security, Information Security, Privacy Enhancing Technology and Network Security. He has applied for a patent on white-box cryptography and published over 50 peer-reviewed journal and international conference research papers and book chapters.

M. Anwar Hossain is an Assistant Professor in the Software Engineering Department, College of Computer and Information Sciences (CCIS) at King Saud University, Saudi Arabia. He received the B.Sc. Engg. degree in Computer Science and Engineering from Khulna University, Bangladesh. He obtained his master degree in Computer Science from the University of Ottawa, Canada, in 2005 and Ph.D. degree in Electrical and Computer Engineering from the same University in 2010. At this university, he was associated with the Multimedia Communications Research Laboratory (MCRLab), School of Information Technology and Engineering. He is currently leading several research projects as principal and co-investigator. Dr. Hossain received IBM faculty award in 2011. His research interests include multi-sensor systems, multimodal surveillance, multimedia cloud computing, ambient intelligence and human–computer interaction. He has authored and co-authored more than 50 publications including refereed journals, conference papers, and book chapters.

Mohammad Mehedi Hassan is an Assistant Professor of Information Systems Department in the College of Computer and Information Sciences, King Saud University, Riyadh, Kingdom of Saudi Arabia. He received his Ph.D. degree in Computer Engineering from Kyung Hee University, South Korea in February 2011. He received B.Sc. degree in Computer Science and Information Technology from Islamic University of Technology (IUT), an organization of OIC, Bangladesh in 2003. He was a Research Professor at Computer Engineering department, Kyung Hee University, South Korea from March, 2011 to October, 2011. He has authored and co-authored more than 43 publications including refereed IEEE/ACM/Springer journals, conference papers, books, and book chapters. He has served as chair, and Technical Program Committee member in numerous international conferences/workshops like IEEE HPCC, IEEE ICME, ACM Multimedia, ICA3PP, IEEE ICC, TPMC, IDCS, etc. He is currently serving as the Associate Editor of International journal of Internet and Distributed Systems (IJIDS) journal. His research interests include Cloud collaboration, multimedia Cloud, sensor-Cloud, mobile Cloud, Thin-Client, Grid computing, IPTV, virtual network, sensor network, and publish/subscribe system.

Atif Alamri is the chairman of Information Systems Department in the College of Computer and Information Sciences, King Saud University, Riyadh, Kingdom of Saudi Arabia. He received his Ph.D. degree in Computer Science from University of Ottawa, Canada in 2010. He received M.Sc. degree in Information System from King Saud University in 2004. He is the founding director of the Research Chair of Pervasive and Mobile Computing (CPMC). His research interests include Multimedia-assisted Health Systems, Ambient Intelligence, Rehabilitation, Multimedia Cloud, Sensor-Cloud, Wireless Sensor Network, Social Network, Privacy and Security. He was the Guest Associate Editor of the IEEE Transactions on Instrumentation and Measurement in 2011, a Co-Chair of the first IEEE International Workshop on Multimedia Services and Technologies for E-health, a Technical Program Co-Chair of the 10th IEEE International Symposium on Haptic Audio Visual Environments and Games, and serves as a Program Committee Member of many conferences in multimedia, virtual environments, and medical applications.

Abdullah Alghamdi is a full time professor, SWE Department, College of Computer and Information Sciences, KSU, Riyadh, KSA. He holds a Ph.D. in Software Engineering from the Department of Computer Science, Sheffield University, UK, 1997. He got a Post-Doc certificate from University of Ottawa, Canada, where he conducted a joint research at the MCRLab during academic year 2004–2005. Prof. Abdullah worked as a full and part time consultant with governmental and private organizations in the field of IS strategic planning and defense systems and headed a number of committees inside and outside KSU. He recently published a number of papers in the field C4I and Enterprise Architecture Frameworks. Currently Abdullah is the chairman of Software Engineering Department, KSU Vice Rector Assistant for Technology Transfer and Director of the national C4I Center for Advanced Systems (C4ICAS).

Mukaddim Pathan is a research fellow at the Commonwealth Scientific and Industrial Research Organization (CSIRO), the national government body of scientific research in Australia. He also holds the position of an adjunct lecturer at the Australian National University. Previously, he was a researcher at the Cloud Computing and Distributed Systems (CLOUDS) Lab of the University of Melbourne, Australia. He holds a Ph.D. in Computer Science and Software Engineering from the University of Melbourne. His research interests include data management, resource allocation, load balancing, and coordination policies in wide-area distributed systems such as Content Delivery Networks, Cloud computing, and Sensor networks. He is one of the developers of MetaCDN that leverages the capabilities of existing storage Clouds for high performance content delivery. He is the editor of the book Content Delivery Networks, Lecture Notes in Electrical Engineering, Vol. 9, Springer-Verlag, Germany. He has authored and co-authored a number of research papers in internationally recognized journals and conferences. He is involved in the organization of the UPGRADE-CN and IDCS workshops and is a PC member of several international conferences. He has edited a few research issues in reputed international journals and also serves as the reviewer of a few renowned journals such as IEEE Transactions on Circuits and Systems for Video Technology (TCSVT), International Journal of Management Science (OMEGA), Journal of Network and Computer Applications (JNCA), Computer Communications, Computer Networks, Journal of Systems and Software, and IEEE Software. He is a member of IEEE, IEEE computer society, and ACM.

Please cite this article in press as: Sk. Md. Mizanur Rahman et al., Secure privacy vault design for distributed multimedia surveillance system, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.019