Iberian Journals

Iberian Journal of Applied Sciences and Innovations

2020 vol 1, Issue 1

A novel security usability method for e-learning platforms

Golbarg Nasiri
Islamic Azad University
Tehran North Branch
Tehran ,Iran
Golbarg.nasiri@yahoo.com

Negin Hajiahmadi
University of Tehran Kish International Campus
Kish,Iran
n.hajiahmadi@gmail.com

***Abstract*—Traditionally, security and usability has acted against each other. Specially, for inexpert people, usability means ignoring security and secure systems are not usable. Researchers and developers recognized that current security problems would be solved only through addressing issues raised through usability and human factor. In fact, future of cyber security relies on deployment of security technologies which widely could be used by inexpert users. Interpretative Key Management (IKM) is a cryptographic key management system under category of master key which empowers users to generate the cryptographic keys within the end-user systems. This article proposes a novel method which specifically helps beginners to achieve both safety and usability of communications and network-based software by utilizing IKM. In this method processes of user authentication and encryption of transmitted and stored data will be fully automated and does not require the users to do any security configuration. The main targeted application of proposed method is to enhance security and usability of e-learning systems when the trainees do not have enough computer knowledge.**

Keywords— security; usability; security usability; authentication; e-learning

I. INTRODUCTION

Security usability deals with analysis of both aspects of security and usability of the designed systems [1]. To evaluate security, the confidentiality, integrity, and availability properties would be studied [2], while usability talks about how easy are processes of authentication and utilization of a system particularly for beginners [3,4].

System usability measures easiness of security protection and running the system for the targeted users [5]. It could be studied from different aspects like psychological, social, organizational, and technical [6]. Psychological acceptance of a developed system for first time introduced as a measure in 1975 [6,7]. Zurko and Simon introduced three groups of *developers*, *users*, and *administrators* as the groups which benefit usability of the developed systems [8]. recognizes the *system owners* as the group which benefits more than other two groups from high level of usability [9].

Authentication techniques like password, passphrase, pass-face, pass-point, or even different biometric technologies are devised to recognize legitimate users than illegitimate ones to be granted access to resources [10,11,12]. Authentication process has two aspects of safety of proposed method and its usability [13]. Although developers aim to make process of authentication easier, but due to the advances in software and hardware technologies it has become more and more complicated over the time [14,15]. A password with 8 characters including alphabet, special characters, and numbers only delivers an average level of security while in 1980 only a five-characters alphabetical password was completely secure [16,17,18].

In 1982 [19] introduced passphrase as a new authentication method which used a meaningful sentence instead of a word. He believed that memorizing a meaningful sentence is easier than memorizing a meaningless word. Two years after [20] invented pass-algorithm authentication method. In pass-algorithm the users should learn an algorithm and then answer the authentication questions according the given algorithm. Cognitive password proposed 21] in 1990 authenticates a user by means of the information which exclusively is known by only the legitimate user. Although this information might also be known by few close people, but usability studies showed fair performance of their scheme [22,23,24].

[25] in 2000 introduced pass-face method. In their method the user has to select the correct face shown on displayed network of faces in four consequent times. Dhamija and Perrig [26] in 2000 changed faces to objects and called it Déjà vu. Pass-point, which introduced [27,28] in 2005, is another authentication technique which that presents a photo to the users and they must click on predetermined point on it to pass authentication process.

Authentication, key management, and encryption are the most important techniques for protection of security [29,30,31]. To protect secrecy, key management techniques and commercial products like the products introduced by IBM [32], Oracle [33], HP [34], Bell [35] and encryption techniques like DES [36], 3DES [37], AES [38], Two fish [39], Serpent [40] could be utilized to protect secrecy of stored and transmitted data. As a sample of secrecy protection Pretty Good Privacy (PGP) [41] which is known as same level of quality with army encryption techniques [42] is presented both as standard and ready product to be tied into under development projects. Due to its decentralized architecture, PGP is utilized in variety of projects like GNUPG [43] and OpenPGP [44]. Instead of relying on centralized certificate authority, it relies on cooperation of members for trustworthiness evaluation of nodes [45].Today, variety of techniques and products are available for protection of secrecy and enhancement of usability, but each one of them might be proper for particular usage. In this article a method based on Interpretative Key Management (IKM) technique [46] which works under category of master key is introduced and evaluated to enhance security and usability of e-learning systems.

II. MASTER KEY

Master key uses a key derivation function to convert input key and some other initial data into keying material to be used in cryptographic algorithms [47]. The initial value for key derivation function is Key Derivation Key (KDK) [48] which might be generated either through an automated key generation process [49] or by an approved random bit generator [50]. If the KDK be generated by automated key generation process, it would be considered as portion of the secret keying material.

Any portion of derived keying material with desired length can be used for cryptographic algorithms [51]. To guarantee that all of the users will have the same keys in hand, they should use the same Key Derivation function (KDF) and agree on the method of converting the keying materials into cryptographic keys [52]. For example, if length of derived keying material is 256 bits, the first 128 bits (first segment) could be used for authentication key and the second 128 bits (second segment) as encryption key. If the KDF is uses Pseudo Random Function (PRF), according to desired length for keying material, the KDF may call PRF for several times to achieve required length [53]. Following key generation modes are the main key derivation functions of master key [54]:

- Counter mode key derivation function
- Feedback mode key derivation function
- Double pipeline iteration mode key derivation function

a) Length of Key Derivation Key

For some KDFs, length of the KDK depends on PRF. For example, if Cipher-based Message Authentication Code (CMAC) is chosen as PRF, the length of the key would be defined according to the length of the respective block cipher [55]. Therefore, at the application time, consistency of PRF and KDK must be verified.

Unlike CMAC, if Keyed-hash Message Authentication code is selected as PRF, the key derivation key could have any length. To preserve consistency between outcome of PRF and length of block, if length of the key is longer than length of the hash function block, the key again should be hashed into length of the hash function output [56].

b) Converting keying materials into cryptographic keys

The length of derived keying material relies on the selected cryptographic algorithm. Application of the cryptographic key, like Message Authentication Code (MAC), will determine length of the key [57]. If no limitation is defined, every portion of derived keying material with the required length could be used as cryptographic key, only if the derived keys do not overlap on KDF output. Therefore, derived keying material length should be equal or longer than sum of the keys [58].

III. Proposed security usability model

The proposed method is founded based on restructured IKM framework for enhancement of security usability. Following paragraphs elaborate the proposed structure and the method of using IKM to implement automated authentication and preserving confidentiality.

a) Structure

Users: any designed security technology is proper for particular applications and group of users. The proposed technique will be useful if group identity of users is more important than their individual identity. For instance, if the users are group of students using an e-learning system, the group identity of these students will determine which resources should be accessible for them. In this example, group identity has more importance than individual identity as the resources would be granted to them according their program.

Bit-stream source: one of the key generation factors in IKM is the bit-stream which will be located into bit-matrix to be surveyed in process of key generation. Since in the proposed method every group of users has a label that describes the group identity, instead of downloading the bit-stream, hash value of the label generates the required number of bits to be arranged into the bit-matrix.

Grouping: one of the features provided in proposed model is possibility of grouping and establishing hierarchy among the groups. In this method, every group has a unique label which describes the type and aim of constituting it. After organizing the groups, particular tables form to let the server recognize type of user for future communications. These tables help the server to recognize the user faster and consume less resources. If individual identity of the users is important, the combination of the given identity code and key generation factors will let server to recognize individual identity of the user.

Session establishment: since the server is responsible to manage the users and groups, it should first recognize which user belongs to which group. Once the group(s) of user determined, the the user IP will be added in IP-Group table to accelerate process of recognizing user’s group and encryption key in continue of the communication, especially when the session expires due to user inactivity. When a new packet from an unknown user receives to the server, it will look into the IP-Group table to find its potential sender. If the IP was found and the corresponding cryptographic key could decrypt the received packet, the user group is identified, otherwise, the server will try to decrypt the received packet by means of keys of all groups.

Group change: changing group is easy process and joining a new group only requires having a label and twenty-four digits of the new group. If the server decides to change group of a user, it will send it the label and twenty-four digits of the new group to the user for using in key generation process. Thereafter, the user will be able to communicate and access the new resources.

Hierarchical order: any user who holds label and twenty-four digits of a group would be able to join the sessions and access to granted resources. Accordingly, if it holds more than one couple of key generation factors, would be able to join multiple groups. This property could be utilized for establishing hierarchy among the groups and users by giving key generation factors of users in lower levels to those who are eligible to monitor the activities.

Recognizing personal identity: individual user identity could be recognized in two ways: manual and automated. In manual method, the server recognizes the group identity of the user based on the used encryption key, and in next step, the user will be authenticated by entering its user code. Combination of given token (interpreter) and user code is the first way of recognizing a user. If the given user code be used in process of key generation, the user does not require to enter authentication code and will be authenticated through fully automated process. Automated way will impose process overhead on the server, especially if there is plenty of users. There are two ways for automatic authentication. In first method, the user identity will be send automatically to the server after the user group recognized through analysis of used encryption key. In second way, the user code will be engaged in process of key generation and therefore each user uses a different key than the rest of group members. The user code will be added to group label and, therefore, combination of hash value of the group label, user code, and 24 digits will construct preliminary materials of key generation. Since in the second way the cryptographic key of each user is unique, the server will have high processing and analysis overhead. This method is safer than the first one, as the transmitted packets are not decipherable even for the users is the same group.

To establish a session, the user system will send a constant message to server which is encrypted by its current key. To accelerate process of recognizing the user group or user identity by changing the keys, due to key refreshment intervals, current key of all groups and users will be produced. In next step, session establishment request of all nodes will be generated and stored to accelerate process of user recognition. Once a packet receives from an unknown source, it would be compared to all session establishment requests of groups to detect the group identity of source. If no match were found, it would be compared with session establishment message of inactive users which use second method of automated individual authentication.

To support the second method of individual user recognition, IP-Group-UserCode table should be established to save current session establishment message of users and keep a list of current active and inactive users.

Although automated user identification imposes process overhead on server, but it has three advantages:

- Automated processes of encryption and authentication
- Utilizing identical cryptographic key per user
- Possibility of blacklisting a single user among all group members

In group identity granting and retaking the resources would be for all of group members, while if the chosen method is individual user recognition, even a single user could be black listed to be banned from accessing resources.

b) Secrecy of stored data

Since the IKM keys are changing continuously, they are not proper to preserve secrecy of stored data as may each part of stored data be encrypted using a separate key. At decryption time, the current key also is different from the previously used keys. To prepare IKM for secrecy preservation of stored data, time and date factors should be eliminated from key generation factors and the bit-matrix would be surveyed according the embedded twenty-four digits.

IV. Security usability evaluation

To evaluate the proposed method both security and usability aspects must be studied. Security evaluation shows that how long the encrypted data would remain safe through mathematical computations. Safety of the cipher depends on the chosen encryption technique and length of the used key. Usability evaluation reveals that how much the proposed technique is efficient and acceptable for its users. The usability study is conducted through a questionnaire.

a) Security evaluation

Since the method is structured based on IKM and uses symmetric 128-bit keys, according to the article published by [34], the employed keys will guaranty secrecy of encrypted data far beyond 2050. Advances in software and hardware technology, and cost of required machines for running an attack are the main factors considered[54]. for calculating safety margin of the keys. Following table show the relation between key length and safety margin.

Table 1. Security lifetime of symmetric keys [34]

Key Length (bits)	Safety border
78	2010
82	2015
86	2020
89	2025
93	2030
101	2040
109	2050

b) Usability evaluation

To evaluate user acceptance and friendliness of the designed method, 100 users were chosen randomly to work with the developed simulator and fill the given questionnaire. The only criterion for candidates was to be over than 12 years old. The attendees were grouped in three age categories of 12 to 20 (group A), 20 to 40 (group B), and over 40 (group C). Also in another classification, they were classified as beginner, intermediate, and professional based on their experiences and qualifications. If an attendee was able to install an operating system, perform security configurations, and install common software, it places in professional group. Intermediate level was for a user that is able to install OS or common software, but had no experience about security configuration. Beginners had no one of counted skills.

The developed simulator was given to all of the attendees and they were taught how to work with it. Then, they were given the equivalent instruction that teaches how to achieve to the same level of safety. After working in both ways, they were asked to fill in the questionnaire and give their recommendations. The following tables show the questionnaire and the analysis results.

Table 2. The distributed usability measurement questionnaire

<table>
<tr><th>Question</th><th colspan="2">Answer</th></tr>
<tr><td>1. What is your age?</td><td></td><td></td></tr>
<tr><td>2. Are you able to install an Operating System?</td><td>Yes</td><td>No</td></tr>
<tr><td>3. Are you able to install a piece of software?</td><td>Yes</td><td>No</td></tr>
<tr><td>4. Are you able to configure or install a firewall or any other type of security product?</td><td>Yes</td><td>No</td></tr>
<tr><td>5. How many years' experience you have in computer security?</td><td colspan="2"></td></tr>
<tr><td>6. Which one is your preferred method: combination of username/password or a token for authentication?</td><td>User/Pass</td><td>Token</td></tr>
<tr><td>7. Which one do you prefer: manual or automated security configuration?</td><td>Manual</td><td>Automatic</td></tr>
<tr><td>8. After having the experience of using IKM-based security usability, which one is your favourite option for securing your sessions: manual or the automated IKM-based method?</td><td>Manual</td><td>IKM-based automated method</td></tr>
<tr><td colspan="3">If there is any comment, explanation, or recommendation regarding the questions 6,7, and 8, you can write it here:</td></tr>
</table>

Table 3. Questionnaire results for selecting between user/pass and token-based authentication methods

	User/Pass	Token
Beginner	19.23%	80.77%
Intermediate	76.93%	23.07%

Professional	100%	0%

Table 4. Questionnaire results for selecting between manual and automated security configuration

	Manual	Automatic
Beginner	0%	100%
Intermediate	13.85%	86.15%
Professional	55.55%	44.45%

Table 5. Questionnaire results for selecting between manual and automated IKM-based security usability method

	Manual	Automatic
Beginner	7.70%	92.30%
Intermediate	18.46%	81.54%
Professional	77.78%	22.22%

Table 6. Questionnaire results for computer security experience (years)

	Group	IKM-based method	Automatic
Beginner	4.46	4.29	7
Intermediate	5.23	4.49	8.24
Professional	8.1	4.5	9.14

Table 7. Questionnaire results for experience in using user/pass and token (years)

	User/Pass	Token
Beginner	6.40	3.95
Intermediate	5.71	3.75
Professional	8.1	-

Table 8. Questionnaire results for average experience of users for choosing between IKM-based and manual security configuration

	User/Pass	Token
Beginner	-	4.46
Intermediate	8.2	4.75
Professional	9.2	6.75

Table 9. Questionnaire results for choosing between authentication method preference according to age classification

Users' age classifications	User/Pass	Token
Beginners-group A	20%	80%
Beginners-group B	16.6%	83.34%
Beginners-group C	20%	80%
Intermediate-group A	73.69%	26.31%
Intermediate-group B	87.1%	12.9%
Intermediate-group C	53.3%	46.7%
Professional-group A	100%	0%
Professional-group B	100%	0%
Professional-group C	100%	0%

Table 10. Questionnaire results for security configuration preference according to age classification

Age classes	Manual	Automated (IKM-based)
Beginners-group A	0%	100%
Beginners-group B	0%	100%
Beginners-group C	0%	100%
Intermediate-group A	15.79%	84.21%
Intermediate-group B	12.9%	87.1%
Intermediate-group C	13.3%	86.7%
Professional-group A	33.3%	66.7%
Professional-group B	75%	25%
Professional-group C	50%	50%

Table 11. Questionnaire results for security usability preference according to age classification

Users'age classifications	Manual	Automated (IKM-based)
Beginners-group A	0%	100%
Beginners-group B	0%	100%
Beginners-group C	13.3%	86.7%
Intermediate-group A	15.79%	84.21%
Intermediate-group B	22.58%	77.42%
Intermediate-group C	13.3%	86.7%
Professional-group A	66.7%	33.3%
Professional-group B	100%	0%
Professional-group C	50%	50%

V. Discussion

The results show that experience of the attendees is the main factor for their evaluation of the proposed technique. On average, attendees with less experience were more interested to the designed method. Considerable number of beginner users were willing to use IKM-based token rather than memorizing combination of username and password, while majority of the intermediate and all professionals preferred to use username/password. The main cause the beginners expressed is lack of self-confidence - due to lack of enough experience - and also trusting a tangible token.

Every single one of the beginners chose the automated security configuration instead of manual way. Majority of the intermediate users preferred to work with embedded automated security configuration and almost close to half of the professionals supported IKM-based automated security preservation method. The main reason of choosing automated system explained as lack of enough security knowledge and oddity of security protocols.

For authentication, combination of username/password was chosen by majority of the users instead of having a token in hand. For security preservation, majority of the users preferred to use automatic security configuration rather than manual way. Once they asked to choose either of the ways, considerable number of the users trusted IKM-based method for both authentication and security preservation, and only some of the professionals were in favour of manual way.

Once the attendees were classified according their chosen method, the statistics revealed that in general less experienced people were more tend to use automated model and experienced ones preferred traditional way.

Analysis of the results show that the proposed technique enhances security and usability, if the targeted users are not experienced and do not have adequate computer knowledge. For this group of the users, employing IKM-based security usability enhancement method increases satisfaction of both system owners and users.

VI. Conclusion

Security usability tries to simplify security configurations and enhance usability especially for untrained users. In this article a new method which uses IKM cryptographic key management model is used to eliminate processes of authentication and encryption configurations for its users. Technical details of the key derivation functions are explained, and then the proposed method is evaluated in terms of security and usability. Security of designed method is examined by mathematical computations and usability is measured based on the user answers in the questionnaires. Security evaluation shows that secrecy of the encrypted data is guaranteed far beyond 2050, and usability evaluation reveals that less experienced users are more interested in the designed method. Employing the proposed technique is extremely offered to online learning systems when their users do not have enough computer security knowledge.

REFERENCES

[1] Zamani M, Manaf AA, Ahmad R, Jaryani F, Taherdoost H, Shojae Chaeikar S, Zeidanloo HR. A novel approach for genetic audio watermarking. Journal of Information Assurance and Security. 2010;5:102-11.

[2] Karamizadeh, S., Abdullah, S. M., Manaf, A. A., Zamani, M., & Hooman, A. (2013). An overview of principal component analysis. Journal of Signal and Information Processing, 4(3B), 173.

[3] Manaf AB, Zamani M, Ahmad RB, Jaryani F, Taherdoost H, Shojae Chaeikar S, Zeidanloo HR. Genetic Audio Steganography. International J. of Recent Trends in Engineering and Technology. 2010 May;3(2).

[4] Karamizadeh, S., Abdullah, S. M., Halimi, M., Shayan, J., & javad Rajabi, M. (2014, September). Advantage and drawback of support vector machine functionality. In 2014 International conference on computer, communications, and control technology (I4CT) (pp. 63-65). IEEE.

[5] Shojae Chaeikar S, Jafari M, Taherdoost H, Kar NS. Definitions and criteria of CIA security triangle in electronic voting system. International Journal of Advanced Computer Science and Information Technology. 2012 Oct;1(1):14-24.

[6] Azarnik, A., & Shayan, J. (2012). Associated risks of cloud computing for SMEs. Open International Journal of Informatics (OIJI), 1(1), 37-45.

[7] Zamani M, Abdul Manaf AB, Zeidanloo HR, Shojae Chaeikar S. Genetic substitution-based audio steganography for high capacity applications. International Journal of Internet Technology and Secured Transactions. 2011 Jan 1;3(1):97-110.

[8] Alizadeh, M., Salleh, M., Zamani, M., Shayan, J., & Karamizadeh, S. (2012). Security and performance evaluation of lightweight cryptographic algorithms in RFID. Kos Island, Greece.

[9] Shojae Chaeikar S, Zamani M, Manaf AB, Zeki AM. PSW statistical LSB image steganalysis. Multimedia Tools and Applications. 2018:77(1):805-835.

[10] Shayan, J., Azarnik, A., Chuprat, S., Karamizadeh, S., & Alizadeh, M. (2014). Identifying Benefits and risks associated with utilizing cloud computing. arXiv preprint arXiv:1401.5155.

[11] Zeidanloo HR, Manaf AB, Ahmad RB, Zamani M, Shojae Chaeikar S. A proposed framework for P2P Botnet detection. International Journal of Engineering and Technology. 2010 Apr 1;2(2):161.

[12] Hooman, A., Marthandan, G., Yusoff, W. F. W., Omid, M., & Karamizadeh, S. (2016). Statistical and data mining methods in credit scoring. The Journal of Developing Areas, 50(5), 371-381.

[13] Taherdoost H, Sahibuddin S, Namayandeh M, Jalaliyoon N, Kalantari A, Shojae Chaeikar S. Smart card adoption model: Social and ethical perspectives. Science. 2012 Aug;3(4).

[14] Mollaie, F., Alizadeh, M., Dadsetan, S., & Rashno, A. (2013). Implementation and evaluation of lightweight encryption algorithms suitable for RFID. Journal of Next Generation Information Technology, 4, 65-77.

[15] Yazdanpanah S, Shojae Chaeikar S. IKM-based Security Usability Enhancement Model. IRACST-International Journal of Computer Science and Information Technology & Security (IJCSITS). 2012 Aug(4).

[16] Dehzangi, A., & Karamizadeh, S. (2011). Solving protein fold prediction problem using fusion of heterogeneous classifiers. INFORMATION, An International Interdisciplinary Journal, 14(11), 3611-3622.

[17] Mazdak Z, Azizah BA, Shahidan MA, Shojae Chaeikar S. Mazdak technique for PSNR estimation in audio steganography. Applied Mechanics and Materials. 2012:1(229): 2798-2803.

[18] Fard, M. A. K., Karamizadeh, S., & Aflaki, M. (2011). Enhancing congestion control to address link failure loss over mobile ad-hoc network. arXiv preprint arXiv:1110.2289.

[19] Shojae Chaeikar S, Zamani M, Chukwuekezie CS, Alizadeh M. Electronic Voting Systems for European Union Countries. Journal of Next Generation Information Technology. 2013 Jul 1;4(5):16.

[20] Karamizadeh, S., Abdullah, S. M., Zamani, M., & Kherikhah, A. (2015). Pattern recognition techniques: studies on appropriate classifications. In Advanced Computer and Communication Engineering Technology (pp. 791-799). Springer, Cham.

[21] Alizadeh M, Hassan WH, Zamani M, Khodadadi T, Shojae Chaeikar S. A prospective study of mobile cloud computing. International Journal of Advancements in Computing Technology. 2013;5(11):198-210.

[22] Alizadeh, M., Hassan, W. H., Behboodian, N., & Karamizadeh, S. (2013). A brief review of mobile cloud computing opportunities. Research Notes in Information Science, 12, 155-160.

[23] Yazdanpanah S, Shojae Chaeikar S. Secure SMS Method Based on Social Networks. International Journal of Scientific Research in Science, Engineering and Technology. 2016: 2(6): 368-376.

[24] Karamizadeh, S., Abdullah, S. M., & Zamani, M. (2013). An overview of holistic face recognition. IJRCCT, 2(9), 738-741.

[25] Shojae Chaeikar S, Ahmadi A. Ensemble SW image steganalysis: a low dimension method for LSBR detection. Signal Processing: Image Communication. 2019:70: 233-245.

[26] Karamizadeh, F. (2015). Face Recognition by Implying Illumination Techniques–A Review Paper. Journal of Science and Engineering, 6(01), 001-007.

[27] Shojae Chaeikar S, Manaf AA, Alarood AA, Zamani M. PFW: polygonal fuzzy weighted - an SVM kernel for the classification of overlapping data groups. Electronics. 2020: 9, 615.

[28] Karamizadeh, S., & Arabsorkhi, A. (2018, January). Methods of pornography detection. In Proceedings of the 10th International Conference on Computer Modeling and Simulation (pp. 33-38).

[29] Shojae Chaeikar S, Manaf AB, Zamani M. Comparative analysis of Master-key and Interpretative Key Management (IKM) frameworks. In Cryptography and Security in Computing 2012. InTech.

[30] Karamizadeh, S., Abdullah, S. M., Zamani, M., Shayan, J., & Nooralishahi, P. (2017). Face recognition via taxonomy of illumination normalization. In Multimedia Forensics and Security (pp. 139-160). Springer, Cham.

[31] Shojae Chaeikar S, Moghaddam HS, Zeidanloo HR. Node Based Interpretative Key Management Framework. In Security and Management 2010 (pp. 204-210).

[32] Karamizadeha, S., Mabdullahb, S., Randjbaranc, E., & Rajabid, M. J. (2015). A review on techniques of illumination in face recognition. Technology, 3(02), 79-83.

[33] Shojae Chaeikar S, Razak SA, Honarbakhsh S, Zeidanloo HR, Zamani M, Jaryani F. Interpretative key management (IKM), a novel framework. In 2010 Second International Conference on Computer Research and Development, 2010 May 7 (pp. 265-269). IEEE.

[34] Karamizadeh, S., Cheraghi, S. M., & MazdakZamani, M. (2015). Filtering based illumination normalization techniques for face recognition. Indonesian Journal of Electrical Engineering and Computer Science, 13(2), 314-320.

[35] Zamani M, Manaf AB, Ahmad RB, Jaryani F, Shojae Chaeikar S, Zeidanloo HR. Genetic audio watermarking. In International Conference on Business Administration and Information Processing, 2010 Mar 26 (pp. 514-517). Springer, Berlin, Heidelberg.

[36] Fard, M. A. K., Karamizadeh, S., & Aflaki, M. (2011). Enhancing congestion control to address link failure loss over mobile ad-hoc network. arXiv preprint arXiv:1110.2289.

[37] Yazdanpanah S, Shojae Chaeikar S, Zamani M, Kourdi R. Security features comparison of master key and IKM cryptographic key management for researchers and developers. In International Conference on Software Technology and Engineering, 3rd(ICSTE 2011) 2011. ASME Press.

[38] Shayan, J., Abdullah, S. M., & Karamizadeh, S. (2015, August). An overview of objectionable image detection. In 2015 International Symposium on Technology Management and Emerging Technologies (ISTMET) (pp. 396-400). IEEE.

[39] Sen J, editor. Cryptography and Security in Computing. BoD–Books on Demand; 2012 Mar 7.

[40] Fard, M. A. K., Karamizadeh, S., & Aflaki, M. (2011, May). Packet loss differentiation of TCP over mobile ad hoc network using queue usage estimation. In 2011 IEEE 3rd International Conference on Communication Software and Networks (pp. 81-85). IEEE.

[41] Honarbakhsh S, Masrom M, Zamani M, Chaeikar SS, Honarbakhsh R. A Trust Based Clustering Model for Dynamic Monitoring in Ad hoc Network. InInternational Conference on Computer and Computational Intelligence (ICCCI 2010) 2010 Dec 25.

[42] Karamizadeh, S., Shayan, J., Alizadeh, M., & Kheirkhah, A. (2013). Information Security Awareness Behavior: A Conceptual Model for Cloud. International Journal Of Computers & Technology, 10(1), 1186-1191.

[43] Shojae Chaeikar S. Pixel Similarity Weight for Statistical Image Steganalysis [dissertation]. Universiti Teknologi Malaysia; 2016.

[44] Karamizadeh, S., & Abdullah, S. M. (2018). Race classification using gaussian-based weight K-nn algorithm for face recognition. Journal of Engineering Research, 6(2), 103-121.

[45] Zamani M, Manaf AB, Abdullah SM, Shojae Chaeikar S. Correlation between PSNR and bit per sample rate in audio steganography. In11thInternational Conference on Signal Processing 2012 Apr 2 (pp. 163-8).

[46] Karamizadeh, S., Abdullah, S. M., Shayan, J., Nooralishahi, P., & Bagherian, B. (2017). Threshold Based Skin Color Classification. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 9(2-3), 131-134.

[47] Shojae Chaeikar S, Ahmadi A. SW: a blind LSBR image steganalysis technique. In the 10thInternational Conference on Computer Modeling and Simulation2018 Jan 8 (pp. 14-18). ACM.

[48] Fard, M. A. K., Bakar, K. A., Karamizadeh, S., & Foladizadeh, R. H. (2011, May). Improve TCP performance over mobile ad hoc network by retransmission timeout adjustment. In 2011 IEEE 3rd International Conference on Communication Software and Networks (pp. 437-441). IEEE.

[49] Shojae Chaeikar S. Interpretative Key Management Framework (IKM) [dissertation]. Universiti Teknologi Malaysia; 2010.

[50] Karamizadeh, S., Abdullah, S. M., Shayan, J., Zamani, M., & Nooralishahi, P. (2017). Taxonomy of Filtering Based Illumination Normalization for Face Recognition. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 9(1-5), 135-139.

[51] Azarnik, A., SHAYAN, J., ZADEH, S. K., & PASHANG, A. (2013, February). Lightweight authentication for user access to Wireless Sensor networks. In Proceedings of the 12th WSEAS Int. Conf. on Electronics, Hardware, Wireless and Optical Communications (EHAC'13), Cambridge, UK (pp. 35-39).

[52] Duan, W., Nasiri, R., & Karamizadeh, S. (2019, December). Smart City Concepts and Dimensions. In Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City (pp. 488-492).

[53] Karamizadeh, S., & Arabsorkhi, A. (2017). Enhancement of Illumination scheme for Adult Image Recognition. International Journal of Information and Communication Technology Research, 9(4), 50-56.

[54] Dehzangi, A., Foladizadeh, R. H., Aflaki, M., & Karamizadeh, S. (2011, April). The application of fusion of heterogeneous meta classifiers to enhance protein fold prediction accuracy. In Asian Conference on Intelligent Information and Database Systems (pp. 538-547). Springer, Berlin, Heidelberg.

[55] Karamizadeh, S., & Arabsorkhi, A. (2018). Skin Classification for Adult Image Recognition Based on Combination of Gaussian and Weight-KNN. International Journal of Information and Communication Technology Research, 10(2), 56-62.

[56] Zadeh, S. K. (2012). Information Security Behaviours in Enhancing Awareness (Doctoral dissertation, Universiti Teknologi Malaysia).

[57] Fard, M. A. K., Karamizadeh, S., & Aflaki, M. (2011). Enhancing congestion control to address link failure loss over mobile ad-hoc network. arXiv preprint arXiv:1110.2289.

[58] arabsorkhi A, karamizadeh S. Method to improve the illumination normalization in adult images based on fuzzy neural network. 11 ;2020 .فصلنامه فناوری اطلاعات (41 and 42) :1-12 URL: http://jor.iranaict.ir/article-1-1503-en.html