Iberian Journals

*Iberian Journal of Applied Sciences and Innovations*

2021 vol 1, Issue 2

# Challenges in Integrity of E-voting Systems: Important Properties, Threats, and Solutions

Mohsen Borousan
*Asia Pacific University of Technology & Innovation*
*Kuala Lumpur, Malaysia*
*Mohsen.boroosan@gmail.com*

Mostafa Kateb
*Department of Electical Engineering, Science and research*
*Branch, Islamic Azad Univerity, Tehran ,Iran*
*mostafakateb@gmail.com*

***Abstract*— Today, developed and developing countries are moving more and more towards e-government systems to deliver integrated, fast, and cheaper services to their citizens. Electronic voting is one of the crucial domains in this area, as the results of the elections profoundly affect the future of the nation and even other countries. Confidentiality, integrity, and availability are the three sides of the CIA triangle that are the principal measurements for evaluating the security of the employed e-voting systems. Since system and data integrity are crucial factors for preserving the security of the designed and developed systems, this study explores the properties, threats, solutions, and unresolved challenges in integrity of e-voting systems, to help researchers, designers, and developers evaluate their systems in term of integrity.**

***Keywords*— voting integrity; e-voting; e-government; voting security**

## I. Introduction

In the traditional practices of paper balloting and hand counting, not only the whole process is observable for the public, but also it is simply understandable to the average voters. In the beginning, the empty ballot box is sealed by the polling staff, and after the election, the seal can be broken and the votes are counted in front of observers [1]. This simplicity and transparency make it easy for observers to identify likely errors. At the same time, candidate agents, political parties, and the media can perform a monitoring function [2].

This simplicity and transparency are lacking in the e-voting systems, as the complexity of the systems is only understandable for the field experts. E-voting systems utilize black-box technology that receives input from voters and then generates an output that is not simply verifiable by observers and even the election administrators [3,4]. This is the point where the integrity, transparency and trust problems arise. As a result, in the e-voting systems, complementary measurements are required to serve the same level of assurance as traditional practices [5]. These measurements may include the followings:

*Transparency*: is a way to satisfy the integrity problem in e-voting and vote counting technologies [4,6]. While this feature alone does not guarantee the accuracy of the results, it provides the ground to achieve this goal. Transparency in e-voting lets the electoral management bodies (EMB) and stakeholders to supervise the critical elements of the process, and avoid intentional and accidental errors [6].

*Testing and certification*: due to the lack of transparency in e-voting systems and counting process, compared to traditional paper balloting practices, it is critical that election administrators test and verify the voting machines to build trust and confidence before they are used [7]. Testing and verification are needed to guarantee that the machines meet the criteria defined by the EMB. The test results should be reviewed by observers and electoral contestants to ensure public confidence [8].

Additionally, some countries only accept certified e-voting and counting technologies. These certifications serve the same as testing procedures. However, the issuance of certifications should be independent of political parties, EMB, suppliers and government [9,10]. Ideally, the certification process must happen by a widely accepted source and through a transparent and open procedure.

*Authentication*: is the process of digitally signing the tested and verified software [11]. The signature can be verified by those which observe the election. Moreover, the validity of data in transition stages - like sending votes for the tabulation process – need to be verified as well; otherwise, the votes could be simply manipulated [11].

To prevent alteration of the votes, only the data with authentic digital signature are acceptable to be passed into the tabulation system. Transmission of the results requires safeguards that are monitored by candidate/party agents [11].

*Audit*: is verifying the operations and auditing the results of an e-voting or counting system. The most practiced way is using a voter-verified paper audit trail (VVPAT) that delivers the paper trail of the casted vote to the voter [12].

The audit trail is a critical factor for verifying the accuracy of the e-voting machines or counting process [12]. A randomly selected audit trail should be verifiable against the e-voting results to prove the consistency of the electronic and audit trails. Such a verification, if made for the public, has a great influence on the public trust [12].

## II. Literature Review

E-voting integrity deals with system trustworthiness, including both provided function and data. In other words, it is to implement safeguards to protect e-voting data and software against changes in unauthorized ways. A solution to resolve the integrity issues of stored data is to utilize cryptographic protocols and techniques like public-key, homomorphic cryptography, Secure Socket Layer (SSL), and transport layer security (TLS) [13]. E-voting schemes utilize various techniques to enhance the preservation of their integrity. Some of the prominent schemes are as follows.

Since the date of introducing Votegrity [14] – the first end-to-end (E2E) verifiable e-voting protocol - various e-voting protocols have been introduced. In E2E, the voters can verify if their votes are cast and counted correctly in the final tally. Additionally, public members are able to verify the election externally. Some of the prominent E2E-based e-voting schemes include STAR-Vote [15], Helios [16], Scantegrity [17], Prêt à Voter [18], and Neff's Markpledge [19].

Some types of E2E-based protocols employ the public web bulletin board (WBB) to show the total casted ballots for the public. WBB is a broadcasting channel which displays the casted ballots in encrypted form, once the voters cast their votes and received the receipt of their encrypted votes [20,21,22]. Vote receipt is an important feature of the e-voting protocols, as a way to prove the vote in case of a dispute.

Apollo [23] is a developed version of Helios protocol which resolves some of the Helios' security drawbacks. Voting assistants is an added feature that helps in verifying, locking and auditing the votes. The assistants are external devices to the voting protocol that are designed for checking the bulletin board and displaying the value of the vote in plaintext format, after casting it [23].

Mixing is another technique that shuffles the votes' data in a random sequence before transmitting it to the next destination [24]. Zeus [25] is a sample protocol designed based on mixing technology. It runs the mixing procedure to remove the links between the encrypted ballots and the voters, in multiple rounds.

Homomorphic tally is a widely applied technique that involves modifications like addition and multiplication to the ciphertext during the decryption process. E-voting schemes like STAR-Vote [26] and Helios 2.0 [27] utilize homomorphic cryptography for tallying the votes, because of its simplicity in both application and verification by the public.

A number of protocols like Apollo [28] and Zeus [25] are designed based on the Helios system while trying to mitigate some of its security drawbacks. For example, clickjacking, cross-site forgery, cross-site scripting, and clash attacks are resolved in Apollo by utilizing the voting assistants feature.

## III. Challenges in Data and Software Integrity of E-voting Systems

The integrity properties could be fallen into two categories of software and data integrity. Data integrity is protecting the integrity of audit records and election records (especially votes) [5,39]. Software integrity is to ensure that only genuine and unchanged software will be run on the electronic components [11,38].

### A. Important propertiesof data integrity

Collected data during running an electronic election is the most important asset of the system. This asset includes stored data, transmitted data, and system recovery/traceability data. The following definitions are the criteria for preserving the safety and integrity of this asset [11,29].

*Accuracy*: the results of elections are only figured based on votes of participated voters.

*Auditability*: during running the election and after it the system behavior is traceable.

*Verifiability*: auditors will be able to verify election results based on the shreds of evidence provided by the system.

*Public verifiability*: normal people independently are able to verify election results.

*Traceability*: every needed information will be recorded to let officials trace the cause of any problem.

*Recoverability*: every needed information will be stored to let recover in case of breaching integrity.

*Preventing data alteration*: any unauthorized modification, insertion, or deletion of data is prevented.

*Data alteration logging*: logging component of the e-voting system, records any data modification which may affect the results.

*Data authenticity*: the system must present enough evidence for auditors to show which record is generated by which entity.

### B. Important properties of software integrity

Since the servers store sensitive votes' information, voters, and technical data for system recovery and traceability are very important to ensure they only run authorized software, and their programs have no important security defect [30,41]. The following definitions and criteria explain the integrity features that an e-voting software must meet [31,40].

*Server software integrity*: to ensure front-end and back-end components will run only the authorized software.

*Server software authenticity*: the authenticity of the installed software must be evaluable by auditors and administrators (to prevent the installation of malware).

*Application of proper software engineering model*: the chosen software development model must be one of the best software engineering practices.

## IV. Integrity Threats and Solutions of E-voting Systems

### A. Threats of e-voting systems

E-voting systems, the same as other electronic systems, are subject to attacks or having bugs [31,37]. This may result in integrity loss and modification of election results. Particularly, if the chosen platforms are either public or private computers, it would be more vulnerable [28,29].

*Software bugs*: software bugs, the same as malicious codes, are one of the most important roots of integrity loss. Statistically, every 1000 lines of codes would have 15 to 50 errors [28,36]. Considering the fact that e-voting systems are constituted from thousands of lines, the likeliness of the existence of bugs is highly considerable.

*Server malicious codes*: the malicious codes which aim to change election results could be installed on e-voting systems, even by their IT staff or administrators, to affect the election results [28,35].

*Data and records modification*: attackers, which potentially also could be the administrators, due to integrity or vulnerability issues may modify the records to affect the results [29,34].

*Client malicious codes*: as far as normally non-expert users operate client machines, these systems are more prone to be compromised by attackers via running malicious codes, worms, Trojans, or viruses, to take control of systems, collect the important information, or even abusing it as stepping stone to penetrate other systems [30].

### B. Solutions of integrity threats

In this part, the important techniques for solving or mitigating integrity threats of e-voting systems are counted and described.

*Integrity preservation through cryptography techniques*: some cryptographic techniques are designed for protection of the integrity of transmitted data over insecure networks like Transport Layer Security (TLS) or Secure Socket Layer (SSL). In addition, data alteration examination techniques like Message Authentication Codes (MAC) or digital signature also can verify the integrity of the stored data [32,42].

*Modern cryptographic techniques*: end-to-end cryptographic voting techniques are the algorithms which are able to detect attacks if the final result is not aggregated on casted votes. Moreover, these protocols let people verify whether their votes are correctly counted [43,44].

*Using voter side trusted hardware components*: if the chosen platform is public or personal computers, the voting platforms are not trustable. Therefore, to overcome the insecure platform issues, trusted hardware could be designed and distributed among voters. Even though the implementation of this method is not economic, but it could be used as a multipurpose platform for e-voting, e-commerce, and other similar applications [45,46].

*Malware detection and prevention systems*: by heuristic methods or based on the signature of malicious codes, anti-malware programs are able to detect the presence of malicious codes. Though these programs are useful, they are able to detect only known signatures and even in some cases, they fail to remove the recognized malware. Using an up-to-date anti-malware distribution is a useful idea, but only for the mitigation of threats of malicious codes and not to solve this problem [26,33].

*Remote software verification*: end-point scanning software helps in scanning the computers in virtual private networks for security protection. These programs can scan the computers remotely for ensuring that they will only run authorized software [24,58].

*Formal software verification*: is a mathematical technique to prove the correctness of the written codes. In this type of verification, the codes must be accurately described as an algorithm. Performing this type of verification is very expensive and hard, and only for particular applications like military software or avionic programs is reasonable [49,50].

*Bootable DVDs or CDs*: bootable DVDs or CDs that contain needed software and applications for secure vote casting over public or private computers could be distributed among all of the voters, to help them boot up and use their computers in a safe manner. Running this process is expensive, hard, and insecure as the users may not recognize genuine DVDs or CDs from the fake ones. They may not run on all computers, and also the voters' mailing addresses may not be up to date. Accordingly, many of the voters may not receive DVDs or CDs [26,27].

*Virtual machines*: virtual machines could be used to provide a secure environment as a solution to bypass some difficulties and problems of distribution of bootable DVDs or CDs. These types of virtual machines do not require any configuration or any driver and use resources of the host computer. The main defects of this idea are the danger of distribution of fraudulent images infected by malicious codes and logistical difficulties of distribution of virtual machines for the images [47,48].

*Second channel*: as the computers might be infected by malicious codes or viruses, for verification of casted votes the voters can use a secondary channel like SMS or telephone to ensure that their votes are cast precisely. This e-voting model has outstanding usability problems [51,52].

*Unintelligible contents for malware*: easy and helpful techniques like CAPTCHA could be employed to prevent the modification of votes by malware. Since still no malware kit is designed which can support passing the CAPTCHAs, this technique could be utilized to prevent malware to vote on behalf of the people [53,54].

### C. *Major unresolved integrity issues of e-voting systems*

Despite all developments of security techniques, still, there are some unsolved serious defects. The most current major integrity issues are:

*Security of personal computers*: still many important security threats like botnets, malware, or viruses exist that endanger the security of personal computers for casting secure votes [55,56].

*Software security problem*: despite many techniques are developed for discovering software security bugs, still, there is no guaranty that all of the bugs get discovered. After deployment, the attackers can exploit software bugs to modify election results [30,57].

*Problems of advanced cryptographic techniques*: despite the advanced cryptographic techniques that can dramatically enhance security, but only certain types of attacks can be detected and still there is no way to recover the original votes [30,31].

## V. Conclusion

E-government is a growing field, especially in developing countries. E-voting is one of the most important aspects of e-government as it has a great influence on people's life. Every developed system, especially those involved in the government area, must be secured against attackers to ban abuse of the system. CIA triangle defines the principal criteria which a secure system must meet. Since these criteria' details depend on the applied system, the relevant concepts and concerns must be clearly distinguished. This study reviews the concepts, threats, and solutions involved in the integrity of e-voting systems. In the last section, the remained and unresolved challenges are discussed.

## 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. فصلنامه 11 ;2020 .اطلاعات فناوری (41 and 42) :1-12 URL: http://jor.iranaict.ir/article-1-1503 en.html