ISSN No:-2456-2165

Review of Challenges in Integrity of E-voting Systems

Behnaz Bagherian
Faculty of Computer Science University of Putra Malaysia

Khashayar Hassanifeizabadi
Business School, City University

Abstract:- Nowadays, advanced and developing countries are moving increasingly toward E-government systems to supply integrated, fast, and cheaper offerings to their residents. Electronic voting is one of the critical domain names in this vicinity because the elections profoundly affect the destiny of the nation and even different nations. Confidentiality, integrity, and availability are the three facets of the CIA three-way relationship, which are the primary measurements for comparing the safety of the employed e-voting structures. Given that system and statistics, integrity is critical for maintaining the designed and developed systems; This paper explores the type of e-voting residences, threats of e-vote casting systems to help researchers, designers, and builders evaluate their systems in time of integrity.

Keywords:- *Voting Integrity; Type of E-Voting; E-Government; Voting Security, Electronic Voting.*

I. INTRODUCTION

Electronic balloting (E-voting) contains a wide range of vote casting systems that apply electronic factors in a single or extra step of the electoral cycle[1]. This attention on is targeting structures that electronically guide one or more of the following steps in the election or referendum technique: recording, casting, and counting votes.

It may seem that automating manual balloting approaches via the usage of records technology could be a straightforward application that might enhance performance and keep away from problems that plagued the 2000 US presidential election [2]. This paper considers one-of-a-kind e-vote casting schemes, net balloting, and direct recording electronic (DRE) balloting systems. At present, there are several trials of those structures being executed internationally. Proponents of e-vote casting have argued that it will have the subsequent salutary effects: multiplied participation for disadvantaged groups, an antidote to voter apathy, more voter convenience to vote time and location, get admission to for humans with disabilities, cash saving, and more accuracy[1-3]. However, several authors have raised caution that e-vote casting poses several protection problems [4].

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 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 [5-8]. These measurements may include the following:

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 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 the 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. Observers and electoral contestants should review the test results 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 [9-11]. Ideally, the certification process must happen by a widely accepted source and through a transparent and open procedure.

Authentication: is the process of electronicly signing the tested and verified software [12]. 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 [13- 16].

Only the data with authentic electronic signatures can be passed into the tabulation system to prevent alteration of the votes. Transmission of the results requires safeguards that are monitored by candidate/party agents [17-20].

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 [21].

The audit trail is a critical factor for verifying the accuracy of the e-voting machines or counting process [22]. A randomly selected audit trail should be verifiable against the e-voting results to prove the consistency of the electronic and audit trails. If made for the public, such verification has a significant influence on public trust [23].

II. LITERATURE REVIEW

Several articles have been released during the last few years to Talk about the security and privacy problems associated with e-voting structures[24].

Paper [25] discussed the historical background of the electronic voting system, types of voting technology, and the manual experience of the balloting system in Nigeria. The Research was motivated to solve the problems of election malpractices such as impersonation, multiple voting, false counting of votes, and deliberate disenfranchisement of voters by the polling officers. The research objectives were to design and implement a secured voting system that was not prone to manipulation, rigging, and complaints from citizens and political parties. I achieved the design on a three-tier web-enabling application such as apache as a web server with extended capacity for Hypertext Preprocessor (PHP) scripting language and MySQL relational database. The Research achieved authentication and simplicity as measures of fulfilling the electronic voting requirements. The Research could not achieve confidentiality, integrity, secrecy, transparency, convenience, and suitability of e-voting functional and security requirements 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) [26-27]. 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 [28] – 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 can verify the election externally. Some of the prominent E2E-based e- voting schemes include STAR-Vote [29], Helios [30], Scantegrity [31], Prêt à Voter [32], and Neff's Markpledge [33].

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 that displays the casted ballots in encrypted form, once the voters cast their votes and received their encrypted votes [34-36] Vote receipt is an essential feature of the e-voting protocols to prove the vote in a dispute.

Several protocols like [37] and [38] are designed based on the Helios system while mitigating 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.

This paper [39] researched a sophisticated Microcontroller based biometric authentication vote casting Gadget. The studies become influenced to solve the Trouble of counting poll paper time, decreasing the Expenditure incurred on human resources, and carrying photograph Identification cards for reputation. The objectives of the Research were to layout and expanded a relaxed e-voting Device-based totally on biometric fingerprint technique. The e-voting system became designed and carried out the usage of Fingerprint biometric and ATmega328 microcontroller to Gain authentication and visible primary programming Language to develop the utility. The election officials utilized passwords. The fingerprint ridges Patterns were formulated and used for authentication of The voters. The Research could not achieve confidentiality, integrity, secrecy, transparency, comfort, and Auditability of e- balloting purposeful and security Necessities. Also, the password of polling officers Can be detected by the fraudsters for alteration of Election consequences[40].

III. TYPE OF E-VOTING

A. Punch-card voting systems

With punch-card balloting systems, the ballot is a card (or cards), and the voters punch holes in it (with a supplied punch device) after their candidate or preference. After punching the hollow(s), the voter can also region the ballot in a ballot field. The voter may also feed the ballot into an electronic vote tabulating tool on the vote casting location[41].

Not unusual sorts of punch-card voting systems are the "Votomatic" and the "Datavote" machine. With the Votomatic card, the places to punch holes to suggest votes are each assigned number. The number of the hole is the handiest facts printed on the cardboard. They print the listing of candidates or ballot problem choices and directions for punching the corresponding holes in a separate e-book. With the Datavote card, they printed the call of the candidate or description of the choice at the poll after the place of the hollow to be punched. The re-be counted of ballots in Florida throughout the 2000 presidential election created a debate about the reliability of punch-card balloting systems. After 2000, the recognition of punch-card voting structures in the US decreased extensively[42].

B. Optical scan (voting) systems

- Those structures use an optical scanner to read and count marked ballot papers. Numerous structures may be defined as optical scan (voting) structures inclusive of Marksense structures wherein an optical mark (e.g. Made with a graphite pencil at the ballot paper) can be diagnosed by using a scanner.
- Electronic poll markers (EBM) may be used to fill out optical scan ballots. The structures look like conventional DREs, however, they document votes on paper ballots instead of internal memory. EBM can useful resource a disabled voter in marking a paper poll; it could allow for

audio interfaces Virtual.

- Digital pen: those systems use ballots on digital paper. A small digital camera within the pen can recognize how the voter marks the virtual ballot paper. The ballots are amassed within the polling station and the virtual pen has to be lower back to the elections group of workers for tabulation.

Optical test vote casting systems combine paper with electronic devices. All of the systems hold a tangible ballot paper which serves as a tangible document of the voter´s purpose. Through that, optical experiment systems allow for guide recounts of ballots. The massive benefit is that the counting system can be carried out in a central location and that the counting is a good deal quicker. The machine is without problems understandable through the voter: for him/her, it does not trade a great deal; they can mark their desire on a poll paper nonetheless. Moreover, if – for anything purpose – the scanning system fails to paintings, ballots can be counted manually[43].

C. Direct-recording electronic (DRE) voting machines

With a DRE gadget, vote casting can be achieved on Election Day or used as a developed vote casting tool in polling stations. It's far without difficulty comprehensible: the voter simply pushes a button next to his/her favorite candidate or desire. Or the DRE machines have a touch screen showing the ballot. After the election or referendum, the DRE gadget tabulates the vote casting facts stored in a removable reminiscence issue and as a revealed copy. The machine might also allow for the transmission of character ballots or vote totals to a central area. The result can then be consolidated in a single relevant place[44].

DRE vote casting machines commenced being vastly used in 1996 in Brazil. They have also been used on a big scale within the US after the Florida 2000. Imaginative and prescient- impaired citizens gain from DRE machines because they can cast their vote without assistance from any other person. DRE machines had been additionally deployed in Europe, e.G. Inside the Netherlands, wherein NEDAP provided their personal DRE machines in 1989. They were used within the Netherlands until 2006. In 2009, the German Constitutional courtroom discovered that the DRE-kind voting machines utilized in Germany's parliamentary elections were unconstitutional. They did now not allow residents to observe the determination of the result[45].

D. Internet voting

Internet voting refers to the use of the internet to forged and/or transmit the vote. Internet vote casting can take numerous forms depending on whether it's miles utilized in out of control environments (faraway net vote casting) or not (Polling web page internet balloting, Kiosk voting). With far-flung net vote casting neither the consumer machines nor the physical environment are manipulated by election officers. Voters can cast their vote at nearly any place (at domestic, on the workplace, at public internet terminals and so on.). The vote is then transmitted over the net. This technique gives the most advantages to voters, but at the same time, it suffers from top safety concerns. They include doubts about the internet as a means of transmission of confidential information, fear of hacker assaults and tension approximately the possibility of disproportionate impact being exerted on the voter throughout the voting process (e.g. 'family balloting').

The other options (polling website internet voting or kiosk balloting) talk over with structures in which electorate cast their poll from consumer machines that might be physically located in authentic polling stations or in public places that election officials manage. In each case, hardware and software program components are managed by way of election officials. The distinction is that with polling website net balloting, the authentication of the electorate might also take vicinity via traditional approach and with kiosk voting (in public places), the physical surroundings and voter authentication are not without delay underneath manipulate of election officials[46].

IV. 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 protects the integrity of audit records and election records (especially votes) [1]. Software integrity ensures that only genuine and unchanged software will be run on the electronic components [47-49].

A. Important propertiesof data integrity

Collected data while running an electronic election is the most critical 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].

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. Essential properties of software integrity

Since the servers store sensitive votes' information, voters, and technical data for system recovery and traceability, they must ensure they only run authorized software. Their programs have no critical security defect [30].

The following definitions and criteria explain the integrity features that an e-voting software must meet [50].

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

Server software authenticity: The installed software's authenticity must be evaluated 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.

V. 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]. This may result in integrity loss and modification of election results. Exceptionally, if the chosen platforms are either public or private computers, it would be more vulnerable [28,29].

Software bugs: Like malicious codes, software bugs are one of the most important roots of integrity loss. Statistically, every 1000 lines of codes would have 15 to 50 errors [28]. Because 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].

Data and records modification: attackers, which could also be administrators, may modify the records to affect the results [29].

Client malicious codes: as far as usually 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 critical information, or even abusing it as stepping stone to penetrate other systems [30].

B. 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: Many critical security threats like botnets, malware, or viruses exist that endanger the security of personal computers for casting secure votes [30,51].

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 [52,53].

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

VI. CONCLUSION

E-government is a growing field, especially in developing countries. E-voting is one of the most critical aspects of e-government as it greatly influences people's lives. 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 the details of these criteria depend on the applied system, the relevant concepts and concerns must be 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]. Lauer, T. W. (2004). The risk of e-voting. Electronic Journal of E-government, 2(3), 177-186.
[2]. 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.
[3]. Zeidanloo HR, Manaf AB, Ahmad RB, Zamani M, Chaeikar SS. A proposed framework for P2P Botnet detection. International Journal of Engineering and Technology. 2010 Apr 1;2(2):161.
[4]. Chaeikar SS, 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.
[5]. Mazdak Z, Azizah BA, Shahidan MA, Saman SC. Mazdak technique for PSNR estimation in audio steganography. InApplied Mechanics and Materials 2012 (Vol. 229, pp. 2798-2803). Trans Tech Publications Ltd.
[6]. Azarnik, A., & Shayan, J. (2012). Associated risks of cloud computing for SMEs. Open International Journal of Informatics (OIJI), 1(1), 37-45.
[7]. Chaeikar SS, Abd Razak S, Honarbakhsh S, Zeidanloo HR, Zamani M, Jaryani F. Interpretative key management (IKM), A novel framework. In2010 Second International Conference on Computer Research and Development 2010 May 7 (pp. 265-269). IEEE.
[8]. Chaeikar SS, Ahmadi A. Ensemble SW image steganalysis: A low dimension method for LSBR detection. Signal Processing: Image Communication. 2019 Feb1;70:233- 45.
[9]. Alizadeh, M., Salleh, M., Zamani, M., Shayan, J., & Karamizadeh, S. (2012). Security and performance evaluation of lightweight cryptographic algorithms in RFID. Kos Island, Greece

[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]. 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.
[12]. 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.
[13]. Chaeikar SS, Manaf AB, Zamani M. Comparative analysis of Master-key and Interpretative Key Management (IKM) frameworks. Cryptography and security in computing. 2012 Mar 7:203.
[14]. Dehzangi, A., & Karamizadeh, S. (2011). Solving protein fold prediction problem using fusion of heterogeneous classifiers. INFORMATION, An International Interdisciplinary Journal, 14(11), 3611-3622
[15]. 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.
[16]. 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.
[17]. Chaeikar SS, Manaf AA, Alarood AA, Zamani M. PFW: Polygonal Fuzzy Weighted—An SVM Kernel for the Classification of Overlapping Data Groups. Electronics. 2020 Apr;9(4):615.
[18]. Yazdanpanah S, Chaeikar SS. IKM-based Security Usability Enhancement Model. IRACST-International Journal of Computer Science and Information Technology & Security (IJCSITS). 2012 Aug(4).
[19]. 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
[20]. 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.
[21]. 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.
[22]. Zamani M, Manaf AA, Ahmad R, Jaryani F, Taherdoost H, Chaeikar SS, Zeidanloo HR. Genetic audio steganography. International Journal on Recent Trends in Engineering & Technology [IJRTET]. 2010;3(2):89-91.
[23]. Karamizadeh, S., Abdullah, S. M., & Zamani, M. (2013). An overview of holistic face recognition. IJRCCT, 2(9), 738-741.
[24]. Karamizadeh, F. (2015). Face Recognition by Implying Illumination Techniques–A Review Paper. Journal of Science and Engineering, 6(01), 001-007.
[25]. 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.
[26]. 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).
[27]. Chaeikar SS, Ahmadi A. SW: A blind LSBR image steganalysis technique. InProceedings of the 10th International Conference on Computer Modeling and Simulation 2018 Jan 8 (pp. 14-18).
[28]. 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
[29]. 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.
[30]. 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.
[31]. Chaeikar SS. Pixel Similarity Weight for Statistical Image Steganalysis (Doctoral dissertation, Universiti Teknologi Malaysia).
[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]. 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.
[34]. Taherdoost H, Sahibuddin S, Namayandeh M, Jalaliyoon N, Kalantari A, Chaeikar SS. Smart card adoption model: Social and ethical perspectives. Science. 2012 Aug;3(4).
[35]. 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.
[36]. Chaeikar SS, Yazdanpanah S, Chaeikar NS. Secure SMS transmission based on social network messages. International Journal of Internet Technology and Secured Transactions. 2021;11(2):176-92.
[37]. 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.

[38]. 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.
[39]. Chaeikar SS, Zamani M, Manaf AB, Zeki AM. PSW statistical LSB image steganalysis. Multimedia Tools and Applications. 2018 Jan;77(1):805-35.
[40]. Karamizadeh, S., Shayan, J., Alizadeh, M., & Kheirkhah, (2013). Information Security Awareness Behavior: A Conceptual Model for Cloud. International Journal Of Computers & Technology, 10(1), 1186-1191.
[41]. Chaeikar SS, Moghaddam HS, Zeidanloo HR. Node Based Interpretative Key Management Framework. InSecurity and Management 2010 (pp. 204-210).
[42]. 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
[43]. 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
[44]. 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.
[45]. Azarnik, A., SHAYAN, J., ZADEH, S. K., & PASHANG, (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).
[46]. 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).
[47]. 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
[48]. 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.
[49]. Karamizadeh, S., & Arabsorkhi, A. (2018). Skin Classification for Adult Image Recognition Based on Combination of Gaussian and WeightKNN. International Journal of Information and Communication Technology Research, 10(2), 56-62.
[50]. 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.
[51]. arabsorkhi A, karamizadeh S. Method to improve the illumination normalization in adult images based on fuzzy neural network. اطلاعات فناوری(41. 2020; 11فصلنامه and 42) :1-12
[52]. 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.
[53]. Taş, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of challenges and opportunities of blockchain for E-voting. Symmetry, 12(8), 1328.