Journal of Autonomous Intelligence (2024) Volume 7 Issue 4
doi: 10.32629/jai.v7i4.863

ORIGINAL RESEARCH ARTICLE

Fingerprint based authentication framework for IoT environment

Vijender Singh*, Chander Kant

Department of Computer Science and Applications, Kurukshetra University, Haryana 136119, Kurukshetra, India
*** Corresponding author:** Vijender Singh, vijender14ranga@kuk.ac.in

ABSTRACT

Internet of Things (IoT) approach makes the humans life easy and safe and due to its acceptability and portability. Humans are surrounded by multitude of heterogeneous devices which assist them in their daily routine. The integration of Blockchain technology with IoT played an important role in medical science and online transaction. At same point of time, the IoT network and devices are vulnerable that can be exploit to affect the network and devices security and accessibility. Therefore, robust authentication techniques should be implementing to secure the IoT network as well as devices accessibility. Due to high heterogeneity of applications, providing authentication for these devices is always challengeable. In this work, a novel fingerprint-based authentication framework in implemented in which Gaussian filter is used for image smoothness, Robert filter for edge detection and achieve 94% accuracy while authentication.

Keywords: smart things; IoT; blockchain; biometric authentication; CASIA

ARTICLE INFO

Received: 30 June 2023
Accepted: 19 September 2023
Available online: 2 February 2024

1. Introduction

Minimal involvement in human life and make their life better are the desired goals of IoT devices. Internet of things is the network of smart things which are able to interact with each other through some communication medium like Wi-Fi, NFC(Near Field Communication), Bluetooth, etc. The term “smart thing” is used for the object that can sense, monitor and react to the environment, process the collected data securely, protect from intrusions and threats i.e., smart watch and other wearable devices[1]. During COVID-19, the use of IoT devices increased at huge rate and collects more sensitive data from the user or its environment. Due to the increasing rate of IoT device, the security issues are also increased related to the network and device accessibility. Therefore, some robust protection mechanism should be implemented to protect the device from the threats or intruders. Blockchain technology plays an important role in IoT domain for online transaction and data sharing or access controls. This paper is focused on the authentication framework to protect the network or device access (remote access). Fingerprint based authentication is the most acceptable and secure that is unique to every user. Various enterprise use fingerprint sensor technology to authenticate the user. In this work, fingerprint-based authentication framework is proposed for device identity in IoT environment. The demands for IoT enable devices in healthcare sector increased at a high rate to monitor the patient in emergency around the world. Numbers of IoT enabled devices are used worldwide to control, monitor, and to

prevent the outbreak of COVID-19. Currently, IoT is also used for tracking the things based on GPS, RFID and On-Board Diagnostics[2]. The use of biometrics instead of PIN and password or other traditional authentication protocols becomes instructing and popular[3]. Due to the heterogeneity and large numbers of IoT device, security and privacy issues are raised and the device are also vulnerable. Therefore, to protect the devices from unauthorized access some robust authentication protocols should be there for remote control system, financial transactions etc. The benefits of such a system include the ease of setting up, lower costs and low maintenance[3,4].

The contribution of the work as follow:

- The proposed framework is more efficient as it reduces the size of the template size, low computational overhead and fast matching, which make it more suitable in IoT environment.
- The proposed framework reduces the issues of template comprising, no one can revoke the original template data from the system.
- The paper provides the higher accuracy and the sensitive data can be accessed by the genuine users only.

The rest of work is organized as: Section 2 presents the related work; section 3 presents the proposed work and different dataset that are used in the work. Section 4 gives an overview of the results and discussion of the proposed work and conclusion is presented by section 5.

2. Literature review

The reliability of session-based CA systems is determined by the capacity of that system to recognize whether the user that is being assessed has changed during the session or it is still. These systems must have a low FRR (False Reject Rate) and here, offered by these systems should be close to zero[5,6]. Soft biometrics includes the biometric data only be valid for a short span of time, i.e., raise, and skin color. The possible applications of a CA system can be determined by these two aspects. However, the thing required is to know having a passive is regarded as a feasibility constraint for any CA approach. They could apply to other different things like authenticating devices in IoT based smart grid[7]. He and Wang[8] proposed biometrics authentication but their work costs very high communication cost and great computational problem. Zhao et al.[9] analyzed the different key organization Methods. The storage and communication cost are comparatively significant in this approach but there is more possibility of attacks in this work. Hu et al.[10] proposed a scheme to verify the correspondence between the end-users. The verification of communication is done between user at WBAN and user at external side. Here, attribute-based encryption (ABE) is recommended. ABE is not highly secured approach and work also undergo from great communication and storage costs. Dhillon and Kalra[11] suggested a protocol for authentication of the user by biometrics for IoT environment. To implement the work, perception hashing operation is used. Alotaibi[12] suggested a user authentication based on biometrics for WSNs (wireless sensor networks) but cannot protect user's anonymity and user intractability. Kang et al.[13] suggested another method for authenticating the user in IoT environment. This method is biometric based method. They worked on the point that the authentication scheme of Kaul and Awasthi[14] was vulnerable in the case of "user impersonation attack", "time synchronization problem", "user anonymity", and "offline password guessing attack". However, the scheme proposed by Kang[14] is prone to "ESL attack under privileged insider attack". Li[15] suggested a "three factor user authentication protocol" for Wireless Sensor Networks and discovered that the scheme fails to defend DoS attack. Artur proposed a protocol based on digital fingerprint system for device authentication and categorized the work for WSN, V2V and wearable devices[16]. Lin You implemented a novel approach for device authentication with zero knowledge. Captured fingerprint image are encrypted and encryption password forwarded by the user are used to calculate the result. Here, an identity proof is required while requesting for services[17]. Dalkilic and Ozcanhan[18] proposed strong identity protocol by transferring the data from the IoT gateway by Pin and mutual authentication. The work is best against man in middle attack,

malicious code injection, reply and DoS attack. Based upon randomized non-negative least square method, Kho et al.[19] proposed cancelable biometrics template. Recently, multifiltering cancelable fingerprint biometrics template scheme was developed and achieved the desired goal.

3. Proposed work

Multiple biometric traits are available for authentication purpose but our framework is based on the fingerprint biometric. The whole process is divided into two phases: enrollment and authentication. Here, a novel fingerprint-based authentication protocol is proposed as shown in Figure 1 that allows the IoT devices to access either data from other devices or the IoT network. Administrator can check list of requests which were made by devices which are not registered through any communication medium, data is uploaded on the server makes it better for monitoring the smart environment. The proposed work is implemented on Raspberry Pi kit. At very first, users are enrolled on the server stored on the server with various details of the devices by the administrator. After the enrolment of the fingerprints, whenever the user or any devices wants to access the IoT environment or gain access remotely for data/smart devices must be go through the authentication protocol. We assumed that every device has fingerprint sensor.

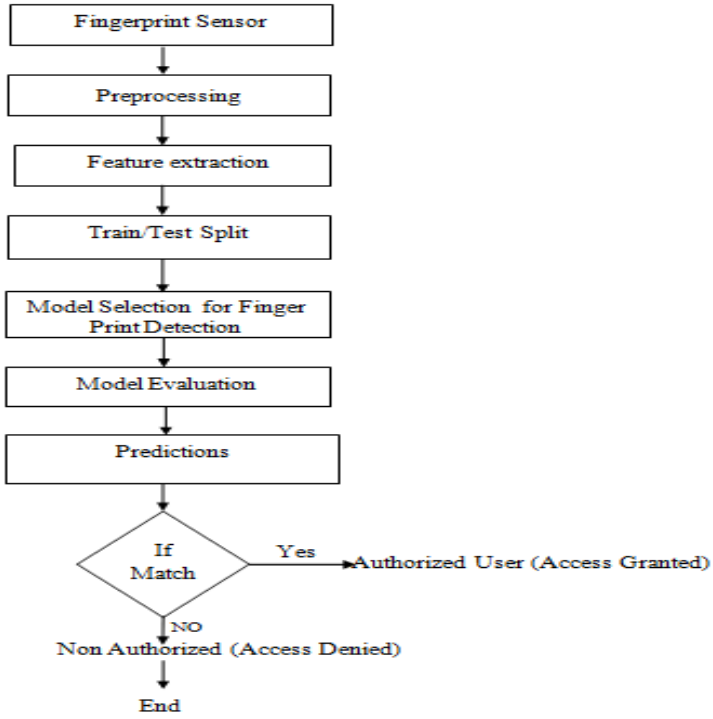

Figure 1. Flow diagram of the proposed framework.

When a request is made by the devices the fingerprint data is also sent to the hardware kit. In next steps the, some preprocessing in done on the scanned image and histogram are prepared for scanned images. After this, features are extracted from the fingerprints. Robert and Sobel Filter are used for edge detection from the fingerprints and then minutiae points are extracted. Deep CNN and Alex Net 2 methods are used to calculate the training and validation results with their accuracy and loss graph. The prediction to either the device is authenticated or not is decided at the end. All the working steps are shown below with supporting figures and results respectively.

If all details like device details and fingerprint will matched with the stored data than it will be able to gain access, otherwise not able to access. Permissions are pre-assigned by the administrator to all the devices. All requested are stored on the server; therefore, the administrator will be able to detect the unwanted access request.

3.1. Methodology of the research

This section describes the dataset and methods that are used in the proposed work in tabulated form as shown below. Here, the minutiae points' extraction process is explained and the results of various steps are given in images. Dataset for the proposed work is given below in Table 1.

Table 1. Dataset description.

S.N.	Category	Name of dataset	Link for the dataset	Description
1	Fingerprint	CASIA fingerprint dataset	http://biometrics.idealtest.org/dbDetailForUser.do?id=7#/datasetDetail/7	CASIA fingerprint image database version 5.0 (or CASIA- Fingerprint V5) contains 20,000 fingerprint images of 500 subjects. The fingerprint images of CASIA- Fingerprint V5 were captured using URU4000 fingerprint sensor in one session given on left column.
2	Fingerprint	Sokoto Coventry fingerprint dataset	https://www.kaggle.com/ruizgara/socofing	Fingerprint dataset designed special for the research objective with 6000 fingerprints form the African subjects.

3.2. Libraries used

To implement the proposed framework, different types of library which were used are usImutils, OS, Keras, Tensorflow, Matplotlib, Seaborn, Pandas, Numpy, Sklearn and CV2.

3.3. Preprocessing

Input images are prepared for the next step of the authentication protocol to produce better quality of the output images as shown in **Figure 2**.

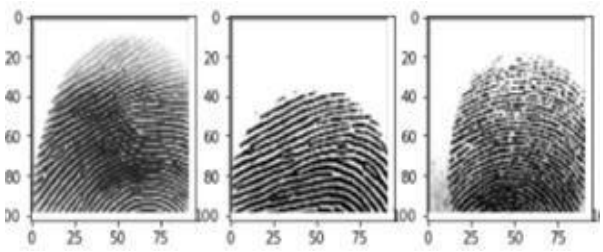

Figure 2. Image Preprocessing

Below **Figure 3** shows the Smooth images original image, Gaussian and Median (CV2. Gaussianblur(), CV2. Medianblur() is used).

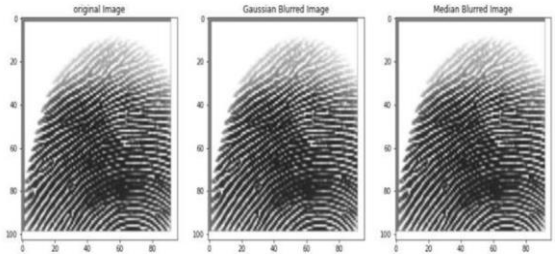

Figure 3. Image smoothing.

Otsu's Thresholding for input images are shown in **Figure 4** given below.

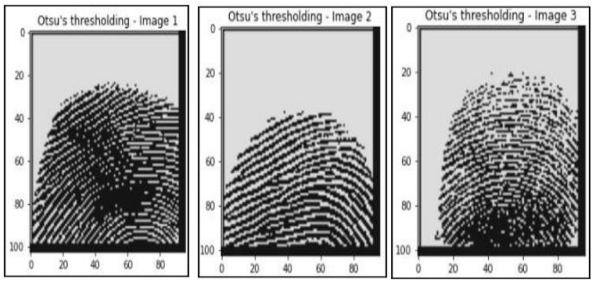

Figure 4. Otsu image of input fingerprint.

(CV2. threshold (image, location, CV2. THRESH BINARY+CV2. THRESH OTSU)) is used.

Table 2 shows the methods that are used for edge detection of the fingerprint.

Table 2. Edge detection methods Robert and Sobel filter.

Gradient based edge detection with multiple filters	**Description**
Robert filter	This filter used to detect the edge. The vertical and horizontal filters in sequence are applied to final the final result for example, if a 2 × 2 window is used as such 1. Vertical Robert filter specs: [1 0] [0 −1]] 2. Horizontal Robert filter specs: [0 1] [−1 0]]
Sobel filter	A discrete differentiation operator used to detect the edge of the image and computes gradient approximation. Two 3 × 3 kernels are used to calculate the horizontal and vertical derivative approximations respectively: $M_1=\begin{bmatrix}-1 & 0 & 1\\ -2 & 0 & 2\\ -1 & 0 & 1\end{bmatrix}$, $M_2=\begin{bmatrix}-1 & -2 & -1\\ 0 & 0 & 0\\ 1 & 2 & 1\end{bmatrix}$

Results image of the Robert filter and Sobel filter are shown in **Figure 5**.

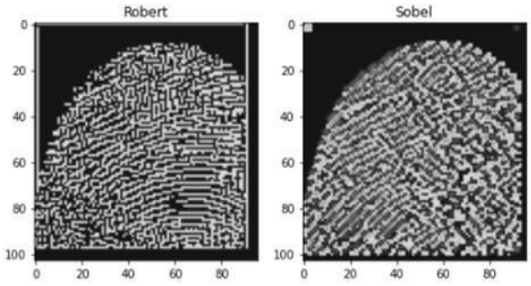

Figure 5. Robert vs Sobel filter images.

The **Figure 6** show the minutiae extraction from filtered image.

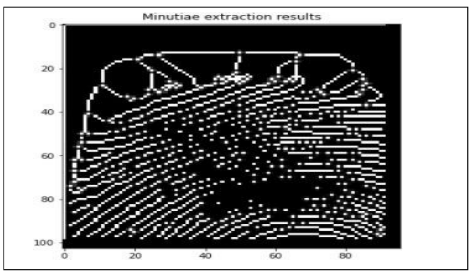

Figure 6. Minutiae points extraction.

In the proposed work, 75% of the complete data is trained data and 25% data is used as test data.

4. Results and discussion

The standard Deep CNN and AlexNet 2 methods are used in the proposed work and achieved the following results that are given in **Table 3**. The accuracy and loss graphs of the work are given in **Figure 7**. The achieved precision, recall and F1 score for Deep CNN and AlexNet 2 are given in **Table 4**.

Table 3. Table of training and validation results.

Algorithms	Training results			Validation results		
	Accuracy	Loss	RMSE	Accuracy	Loss	RMSE
Deep CNN	97.8	0.08	0.28	94.2	0.23	0.47
AlexNet 2	75.59	0.50	0.70	89.54	0.10	0.32

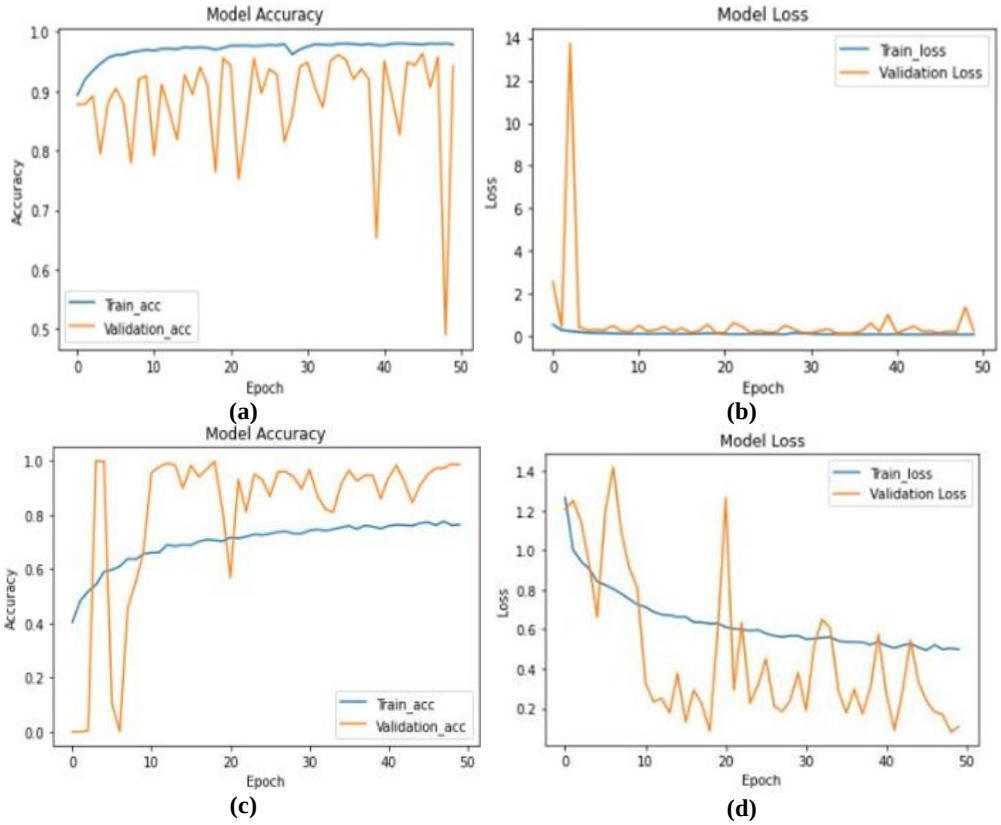

Figure 7. Accuracy and Loss graph of Deep CNN and AlexNet2.

Precision, Recall and F1 score values for Deep CNN and AlexNet 2 algorithms are below in **Table 4**.

Table 4. Precision, recall and F1 score.

Algorithms	Categories	Precision	Recall	F1 Score
Deep CNN	Altered Easy	0.99	0.94	0.97
	Altered Medium	0.98	0.96	0.97
	Altered Hard	0.78	0.81	0.76
	Real	0.98	0.94	0.89
AlexNet 2	Altered Easy	0.98	0.78	0.87
	Altered Medium	0.59	0.76	0.66
	Altered Hard	0.62	0.68	0.65
	Real	0.89	0.95	0.93

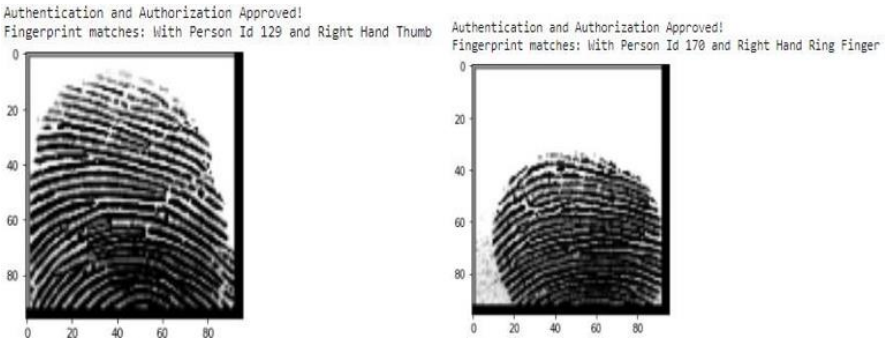

Figure 8. Predictions decision making.

It is cleared form the **Table 3** that proposed work with the Deep CNN algorithm provides the higher authentication accuracy (94%) than the AlexNet 2 algorithm. **Figure 8** shows the results of precision, recall and F1 score of the proposed work for the different methods. The works contributes improve the security at Network Layer and resolved the issue of false acceptance by improving the quality of the input fingerprint image during minutiae points extraction. **Figure 9** shows the device model of the proposed work.

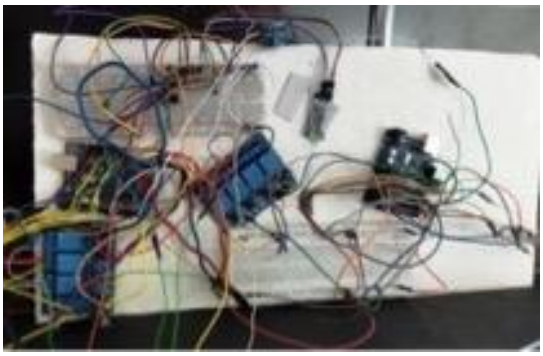

Figure 9. Device model of the proposed authentication system.

Whenever a template is created, no one can revoke it or exchange the templates with altered one and due to the small template size and low computation, faster authentication will be done as compared to other highly computation-based approaches. Therefore, only the authorized/genuine users can access the IoT devices that may have critical or sensitive data of the users.

5. Conclusion

Authentication protocols should be implemented to protect the IoT devices and the network. Therefore, different mechanism can be used to do these i.e., biometric based or other traditional methods. This work provides a fingerprint-based authentication protocol and provides the best results above 94% accuracy as compare to AlexNet 2. Proposed work is suitable for the remote access, cardless transaction etc. Further improvement can be done in this by using different methods, algorithms and different biometric to achieve the better accuracy and prediction. Integration of Blockchain technology with proposed work may provide highly secure system for IoT domain.

Author contributions

Conceptualization, CK; methodology, VS; validation, VS; formal analysis, VS and CK; investigation, VS and CK; data curation, VS and CK; writing—original draft preparation, VS; writing—review and editing, VS; visualization, CK; supervision, VS and CK. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Khader R, Eleyan D. Survey of DoS/DDoS attacks in IoT. Sustainable Engineering and Innovation 2021; 3(1): 23–28. doi: 10.37868/sei.v3i1.124
2. Kumar A, Sharma S, Goyal N, et al. Secure and energy-efficient smart building architecture with emerging technology IoT. Computer Communications, Computer Communications 2021; 176: 207–217. doi: 10.1016/j.comcom.2021.06.003
3. Yan B, Xu A, Cao Y, et al. Hardware-fingerprint Based Authentication for NFC Devices in Power Grids. In: Proceedings of the IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC 2019); 20–22 December 2019; Chengdu, China. pp. 1147–1154.
4. Lilhore UK, Imoize AL, Li CT, et al. Design and implementation of an ML and IoT based adaptive traffic-management system for smart cities. Sensors 2022; 22(8): 2908. doi: 10.3390/s22082908
5. Armstrong R, Hall BJ, Doyle J, Waters E. Scoping the scope' of a Cochrane review. Journal of Public Health 2011; 33(1): 147–150. doi: 10.1093/pubmed/fdr015
6. BioCatch .From Login to Logout: Continuous Authentication with Behavioral Biometrics | Cyentia Cybersecurity Research Library. 2019.
7. Bekara C. Security issues and challenges for the IoT-based smart grid. Procedia Computer Science 2014; 34: 532–537. doi: 10.1016/j.procs.2014.07.064
8. He D, Wang D. Robust biometrics-based authentication scheme for multiserver environment. IEEE Systems Journal 2015; 9(3): 816–823. doi: 10.1109/jsyst.2014.2301517
9. Zhao K, Sun D, Ren G, Zhang Y. Public auditing scheme with identity privacy preserving based on certificateless ring signature for Wireless Body Area Networks. IEEE Access 2020; 8: 41975–41984. doi: 10.1109/access.2020.2977048
10. Hu C, Li H, Huo Y, et al. Secure and efficient data communication protocol for wireless body area networks. IEEE Transactions on Multi-Scale Computing Systems 2016; 2(2): 94–107. doi: 10.1109/tmscs.2016.2525997
11. Dhillon PK, Kalra S. A lightweight biometrics based remote user authentication scheme for IoT services. Journal of Information Security and Applications 2017; 34: 255–270. doi: 10.1016/j.jisa.2017.01.003
12. Alotaibi M. An enhanced symmetric cryptosystem and biometric-based anonymous user authentication and session key establishment scheme for WSN. IEEE Access 2018; 6: 70072–70087. doi: 10.1109/access.2018.2880225
13. Kang D, Jung J, Kim H, et al. Efficient and secure biometric-based user authenticated key agreement scheme with anonymity. Security and Communication Networks 2018; 2018: 1–14. doi: 10.1155/2018/9046064
14. S.D. Kaul, A.K. Awasthi, Security enhancement of an improved remote user au- thentication scheme with key agreement, Wirel. Pers. Commun. 89 (2) (2016) 621–637.
15. Li X, Peng J, Obaidat MS, et al. A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. IEEE Systems Journal 2020; 14(1): 39–50. doi: 10.1109/jsyst.2019.2899580
16. Wu F, Xu L, Kumari S, Li X. An improved and provably secure three-factor user authentication scheme for wireless sensor networks. Peer-to-Peer Networking and Applications 2018; 11(1): 1–20. doi: 10.1007/s12083-016-0485-9
17. Guo C, You L, Hu G. A Novel Biometric Identification Scheme Based on Zero-Knowledge Succinct Noninteractive Argument of Knowledge. Security and Communication Network, Hindawi. 2022. doi: 10.1155/2022/2791058.
18. Dalkilic H, Ozcanhan MH. Strong authentication protocol for identity verification in internet of things (IoT). In: Proceedings of the 6th International Conference on Computer Science and Engineering (UBMK 2021); 15–17 September 2021; Ankara, Turkey. pp. 199–203.
19. Kho JB, Kim J, Kim IJ, et al. Cancelable fingerprint template design withrandomized non-negative least squares. Pattern Recognition 2019; 91: 245–260.