International Journal of

INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Biometric System Survey of Safety and Confidentiality Issues

Gur Sharan Kant[1], Kavi Bhushan[2], Bharat Singh Chittoriya[3], Dr. Rajneesh[4], Dr. Shikha Agarwal[5], Rakesh Kumar Pandey[6], Santosh Prasad Singh[7], Dr. Subodh Kumar[8]

Submitted: 07/10/2023 **Revised:** 24/11/2023 **Accepted:** 04/12/2023

Abstract: A biometric system is a futuristic system that uses the data about the solitary, previously kept in the record, to identify the difference. Biometric systems are increasingly accepted since they provide security and privacy to the data so that no one can misuse the data. But still, the system is not entirely secure because the pattern can be recognized by a third party with the help of the remote application, like response attacks or realistic detection over the Internet to access the biometric data. This paper presents a survey of security and privacy issues in the biometric system and discusses the various case studies, such as E-passport and, identification, followed by the dangers and problems. So, in this paper, it's mainly concluded that there need to be a few strategies or protocols that might be primarily based totally on sign processing and the cryptography mechanism that might protect the biometric data from intruders. This paper presents a survey of security and privacy issues on the biometric system and discusses the various case studies such as E-passport and Aadhaar identification, followed by the dangers and problems. So, in this paper, it's mainly concluded that there should be a few strategies or protocols that might be primarily based totally on sign processing and the cryptography mechanism that might protect the biometric data from intruders.

Keywords*: intruders, biometric, protocols, identification, cryptography*

Introduction: A biometric system is a system that is basically a pattern recognition system that is operated by collecting the biometric data from a distinct, through extracting a set of data from the collected data and comparing the extracted set of data with the saved data in the database [1]. Biometrics system is used to measure individuals' unique behavioral or somatic features to authenticate or recognize their identity [2]. There are two modes on which a biometric system can operate, depending on the application context. The modes are verification modes and identity modes. In verification modes, the biometric machine already shops the consumer template in a database; whilst validating the consumer, the machine compares the accumulated statistics with the saved statistics, and if they match, then the user is a valid user, else not. any other mode is identity mode wherein the gadget acknowledges a consumer through evaluating its information with all of the stored templates inside the database; that is, one to many Comparisons take region for organizing a person identity. Since biometric-based authentication has many benefits over conventional methods, there has been a significant rise in the use of biometric systems in recent years. It is very important that a biometric system must be intended in such a way that it can tolerate attack when used in security-critical applications, mainly in unattended distant applications like e-commerce [3]. Nowadays almost every citizen is using the Internet as a source of communication, transaction, registration, and for many more. They are sharing their dynamic data such as Aadhaar number, PAN number, bank account number, and personal photographs over the Internet, being unaware that an intruder can misuse their data. This paper is organized as follows: Section 2 of the paper discusses the literature review. A case study is defined in Sect. three of the paper accompanied through issue and destiny scope in Sect. 4

[1,2,3,4,5,6,7,8]*Assistant Professor*
gskant9319@gmail.com,
kavybhushan@gmail.com,
bharat_pme2027@sliet.ac.in,
rajneesh_ccs@rediffmail.com,
sagarwal.scriet@rediffmail.com,
rakesh18.pnd@gmail.com,
santosh.rgec@gmail.com,
Panwardrsubodh@Gmail.com
Department of Computer Science 1,2
Department of Mechanical Engineering3
Department of Applied Science 4,5,8
Electronics and Instrumentation Engineering Department 6,7
Sir Chhotu Ram Institute of Engineering & Technology 1, 2, 3, 4, 5, 6,7, 8
Chaudhary Charan Singh University, Meerut

1 Literature Review

1.1 IT Act and GDPR

General Data Protection Regulation (GDPR) is the act of European Union law on privacy and protection of statistics for all the citizens of the European economic place and European Union. This act was modified into carried out on May 25, 2018. Similarly in India, the Information Technology Act 2000 (IT Act) is the primary law that deals with electronic commerce and cybercrime. This act provides a legal structure for the recognition of digital signatures as well as records that are electronically saved. This section provides the differences and similarities between notable features of the IT Act and GDPR for data protection.

1.2 Difference Between IT Act 2000 and GDPR

The goal of GDPR is to offer safety to every and each citizen at the same time as processing data. GDPR works on the following principles:

• DATA INTEGRITY: It means the consistency and accuracy of data.

• TRANSPERENCY: It means the data be clear.

• ACCOUNTABILITY: It means the discipline and the presentation of data. • FAIRNESS: It means the optimization of data.

Table 30.1 Differentiation of GDPR and IT Act

Principle	Article and section	Difference
Objective	–	• GDPR provides protection to individual rights and freedom for data processing IT Act 2000 does not express it
Processing of data	GDPR: Article 5 IT: Rule 5 of 2011	GDPR listed the following principles: Data integrity Protection from illegal processing Fairness Accountability Transparency IT Act applies only for the collection of data and its uses and does not express processing
Law of processing	GDPR: Article 6 IT: Rule 5 of 2011	• GDPR consists of five additional conditions of processing IT Act does deal with the law of processing
Delicate personal data	GDPR: Article 9 IT Act 2000: Sec. 43A IT Act 2011: Rule 3	• IT Act and GDPR of this particular category have mentioned different laws

Rights	GDPR Article (14-18) Article (20-22) Article 7(3) IT Rules, 2011 Rule 5(6) Rule 5(3) Rule 5(7)	IT Act had not used the word "RIGHT" • In GDPR, important rights are mentioned such as right to restrict processing, right to access, and many more
Security	GDPR Article 32 Article 35 Article 37 Article 30 Article 33	• GDPR consists of the security measures for data processing in detail. These include the assessment of maintaining the records of data processing by security officer
	• IT Rules 2011 – Rule4	IT Act does not mention in detail

Table 30.1, given below, highlights the key principle used for the differentiation of GDPR and IT Act.

1.3 Similarity Between GDPR and IT Act 2000

The objective of both laws is to facilitate the transfer of data for the advantage of electronic commerce. According to the GDPR rules, the collection of data should be lawful, and related data should be collected. It is also mentioned that data cannot be held for longer periods than required for data processing purposes. The same component had additionally been noted inside the IT Act. Minor exceptions are present in

the GDPR with respect to the data retention. Under IT Act and GDPR, "consent" of an information company or problem of records is an essential criterion for lawfulness. Similarly, biometric data, sexual orientation, and health records are considered sensitive data by both the Rules and the Act. Again both the Act and GDPR had made it mandatory that before collecting someone's personal data, consent should be taken. In addition, the issuer of information has the privilege of retaining the consent. Adoption of safety audits and inner regulations for defensive records are required with the aid of using each IT Act and GDPR. Protection of facts practices additionally consists of permitted certification and voluntary compliance. According to the IT Act and GDPR, data transfer to another country or body can take place only if the level of protecting data is the same for both of them. Still, the benchmark for protective facts could be very excessive in the case of GDPR; IT Act needed to revise its ACT to reap this benchmark (Table 30.2).

Table 30.2 Similarity between GDPR and IT Act

Principle	Article and section	Similarity
Objective	–	• Transferring of data for GDPR and ITAct are same in case of electronic commerce
Processing of data	• GDPR: Article 5 • IT: Rule 5 of 2011	• Laws required for are – Data should be collected lawfully – It should be specified purposely
Law of processing	• GDPR: Article 6 • IT: Rule 5 of 2011	• For both the data provider should be prerequisite for the collection of data
Delicate personal data	• GDPR: Article 9 IT Act 2000: Sec. 43A • IT Act 2011: Rule 3	• Both laws consist of – Biometric data – Sexual orientation – Health records
Rights	• GDPR – Article (14-18) – Article (20-22) – Article 7(3) • IT Rules, 2011 – Rule 5(6) – Rule 5(3) – Rule 5(7)	• Few rules under IT Act, Sec. 43A areloosely similar to the GDPR rights
Security	• GDPR – Article 32 – Article 35 – Article 37 – Article 30 – Article 33 • IT Rules 2011 – Rule4	• Some of the data security for protection are similar for both of them. They are – Security audit – Absorption of internal policies – Certification mechanism

1.3 Related Work

Prabhakar et al. [4] presented the view that the biometric system was much more efficient than that of the tradition system for recognition purpose. So the security of this authentication perspective was greater concern. According to the authors, for making the authentication a secure platform, the basic requirements were:

- Universality: The characteristic should be universal that every person must have the particular characteristic.
- Distinctiveness: The characteristics of every person should be unique or differ from each other.

- Permanence: The characteristics of each person must be permanent.

By keeping all these factors in mind, there was a possibility that for allowing access in the record, the fingerprint of one person matches with the fingerprint of another person. Therefore, it was the great need to secure the system more to avoid replication or to enhance the biometric system [4].

Jain et al. [1] had proposed a scheme whose objective was to ensure that the services were used by the genuine user only. Examples of this application are ATM, laptop, access to buildings securely, computer system, and cellular phones. These systems are insecure, in the lack of strong scheme for personal recognition. Biometric recognition means the process of automatic identification of a person, based on his or her behavioral and physiological features. It is also possible to either confirm or establish a person's identity, which is centered on "who she is" than by "What she have" or "what she remembers" [1].

Juels et al. [5] had explained the security and privacy effects of the forthcoming worldwide experiment in authentication technology. They also explained security and privacy issues that can be applied to e-passports and then analyze the issues with respect to ICAO (International Civil Aviation Organization) ethics for e- passports. They had identified privacy and security threats for e-passports and then estimate developing and future of e-passport types in respect to this threat. They had primarily analyzed the standard of ICAO and the reason for being adopted by some nations. Some principles had been identified for the protection of biometric identity cards and analyzing those principles with respect to the e-passport standard of ICAO, Malaysian e-passport, and ICAO deployments. They had drawn some conclusions like:

- The privacy data needed for biometric information mean illegal

reading of e- passport information, which is a privacy risk and security risk too. If biometric authentication is done without supervision, then risk can grow.

- At least basic access and Faraday cage control must be applied in ICAO deployments for preventing remote unauthorized access of e- passports data. They had cited an example of the USA where deployment of ICAO e-passport does not deliver enough protection for its biometric information.
- Since the active authentication used by the US deployment, users data are essential to supply to the US deployment according to ICAO spec for combining the capability of optically scan e-passport, which was sufficient for elementary access control in the US deployment for ICEO e-passport, but are not convincing.

According to the author, e-passport deployment is in the first part of coming- generation identification devices. E-passport might provide important knowledge for how to build more private and secure identification platform in the coming future [5].

Faundez-Zanuy [6] described that biometric offers superior deposits of advantages than that of making "password" but it was not adopted yet. The dis advantage of the biometric system was that the data are not to be used as secret, not be able to replace or in case of elder people or manual define the identity of remote user. There are three types of authentication factors that were:

- Passwords: This is known by the client.
- Smart card: It is with the client.

workers who do not have fingerprints. There were many remote applications like anti-reply attacks or liveliness detection over the Internet to access the biometric data by third party (intruder). According to the author, there must be constant update to keep the data protected [6].

Lai et al. [7] discussed security system of biometric under the framework of privacy–security trade-off. Two different conditions had been identified, either the attacker had side information related to the biometric measurement or not, and had been considered. In the situation where the attacker/hacker does not have information, the author considered the two cases of perfect privacy and perfect security. In both cases, the region had been identified for the complete privacy– security trade-off. More precisely, that an outer bound on the privacy–security pair was achievable by any system had been derived. Furthermore, a system had been proposed to attain this upper bound. In the situation when the hacker has information about the biometric measurements, outer and inner bounds on the privacy and security portion have been derived [7].

Huang et al. [8] had defined different types of resources allocated in the form of network services managed and provided by servers. The mostly used method is remote authentication, which is used to

- Biometric characteristics like iris scan, voice print, and fingerprint.

Conserving privacy and security was a thought-provoking matter in distributed network. This

research paper had shown a movement toward solving this matter by suggesting a general framework for three types of authentication factors to safe resources and services from unauthenticated usage. An authentication was created on biometrics, password, and smart card. The author's framework not only explains how to get secure three-layer authentication from two layers, but it also mentions several prominent matters of biometric authentication in a network that was distributed [8].

Meng et al. [9] had revealed the survey reports on various biometric user authentication techniques, which can be developed on the touch- enabled mobile phones. Some of the points on biometric authentication were as follows:

The taxonomy of the existing biometric authentication on the mobile phones as well as it had analyze, what would be the feasibility if they are implemented on mobile phones which are touch enabled.

- Systematic characteristics of any generic biometric authentication system had been described highlighting and their countermeasures on touch-

PPBSs, including encryption-based biometric schemes, hybrid and multimodal based schemes, con- callable biometric based schemes, and SC-based schemes. It had also explained the functional mechanism of PPBSs. The drawbacks associated with PPBSs were also discussed and summarized. The analysis can help to develop more efficient and effective PPBSs in the future [10].

Memon [11] narrated that biometric was also used to access the data from the personal devices that overcome the limitation of commonly used password-based mechanisms as biometric was easy and more convenient but there were also the chances of stolen of biometric data with the help of malicious ways. The author presented the idea that there must be some techniques or protocols that were basedon the signal processing and the cryptography mechanism that would protect the biometric data from the intruders [11].

Kumar et al. [12] proposed a privacy-preserving-based biometric authentication system in the field of healthcare. There was a huge impact of the recent technologies such as Internet of Things in the healthcare and medical sector. The patients were treated much better than that of the traditional approaches. But with the recent development, the patient's data travelled a lot from one area to another. So there might be a great need enabled mobile phones.

- A system for implementing a reliable authentication framework by establishing a multimodal user authentication of biometric in a proper way, for validating the framework experimental results had been provided. The results show that biometric with multimodal can be implemented on the touch-enabled mobile that can significantly decrease the false rate of a single biometric system.
- Lastly, various challenges were identified in these areas. It had suggested that explained dynamics could become the mainstream object for designing user authentication on the touch-enabled mobile phones [9].

Natgunanathan et al.'s [10] biometric characteristics are linked with individuals if these data are leaked, then it will violate individual privacy, and may cause serious and continuous issues, since the biometric data of individual are irreplaceable. The privacy-preserving biometric schemes (PPBSs) had been developed over the past decade for protecting the biometric data, but they too had some drawbacks. The main objective was to provide a brief summary of the existing

to provide complete authentication to the data. Biometric system was considered to be the best and low-cost system to secure the patient's parameters as well as the authentication to the patient when there was a case of sensor data [12].

Jaronde et al. [13] proposed a low-cost biometric system for newborn infants not to get swapped in the hospital. Swapping of newborns in the hospitals was a challenging issue that occurred all over the globe. The traditional DNA procedure was very expensive. To overcome the limitation, a low-cost method was implemented, which involved the scanning and matching of the infant's footprints and the mother's hand impressions using a biometric system. In case the infant got swapped in the hospital, recognize the infant with the help of data that are being stored. So by this way, a biometric identification system was considered a great and low-cost tool [13].

Osadchy and Dunkelman [14] traced that the existing authentication system discarded the center of attraction which was privacy protection. In the traits of biometrics such as fingerprint and face detection, there must be a system that is well-trained for its users. There was a need to develop a system for preserving privacy with great accuracy [14].

1.4 History of Biometric System

Year	Description
2000	The vendor test of face recognition held first time
2000	Consists of the vascular patterns used for the recognition purpose published first time
2000	Program on biometric degree was established at the University of West Virginia
2001	In Florida, face recognition process was used for the first time at Super Bowl
2001	Subcommittee of ISO/IEC on biometrics was established
2002	Technical committee of M1 on Biometrics was formed
2002	Palm Print Paper was submitted to ISC (Identification Services Committee)
2002	Formal US Government coordination of biometric activities begins
2003	ICAO adopted blueprint to merge biometrics to machine-readable documents
2003	Forum of European biometrics was established
2004	Program of US-VISIT becomes operational
2004	DOD implemented ABIS
2004	In the USA, database of first state automate palm print was deployed
2004	The grand challenge of face recognition begins
2005	Iris recognition patent filed by the USA
2008	U.S. Government begin coordinating biometric database use
2010	U.S. national security apparatus utilizes biometrics for terrorist identification
2011	Biometric identification used to identify body of Osama bin Laden
2013	Apple includes fingerprint scanners into consumer-targed smartphones

1.5 Existing Authentication Techniques

Methods	Examples	Properties
The user knows	Username Password PIN code	• Forgotte n password /PIN Many passwords Can be shared
The user has	Cards Keys	Duplicity Lost Stolen

		Can be shared
The user has and the user knows	ATM card PIN	Password (weak link) Can be shared
Unique about the user	Face Fingerprint Iris Voice	Can never be shared Can never be lost Can never be stolen

2 Case Study

2.1 Aadhaar Card

When there was a need for the authentication approach, the model that comes under consideration was "Aadhaar." Aadhaar is basically a 12- digit number for the unique identification given by a governmental agency of India called Unique Identification Authority of India, commonly known as UIDAI. It is based on the information of biometric and demographic [15]. UID, that is, Universal Identification, is the largest program of biometric identification in the world having more than 200 million people enrolled [16]. Aadhaar provides a very strong authentication in different services such as in the field of e- health care, voting mechanism, commercial, and many more. In the case of voting mechanism, finger printing for the identification plays a vital role. So, to access the finger print, the database of Aadhaar card is used [17].

In Aadhaar card authentication, UIDAI members collect the following data for the enrolment in the Aadhaar service:

- Iris scanning of both eyes
- Fingerprinting of all fingers including thumbs
- Digital photograph

This multimodal is very advantageous because various biometrics suit best for different fields. The scanning of iris provides much more than that of fingerprinting but in the same phase fingerprinting is cheaper than the iris. Aadhaar card holders use smart phones with personal identification number, that is, PIN or can use biometric to verify the identity of individual. The Aadhaar data in the centralized database can be accessed by anyone, such as bank, employers, law, and many more in real time.

Fig 1.1

(https://www.nec.com/en/global/solutions/biometrics/face/index.html)

However the security risks are always a controversial part of the Aadhaar system. There is a valid proof that the system like Aadhaar is having some security issues. One of the journalists found that the description of many of the enrollees with their Aadhaar number was posted online in the Indian governmental website [18].

2.2 E-Passport

According to the US Government, within few years, travelers from different nations would carry a new type of passport that is e-passport. It will deploy two new technologies like biometric and RFID (Radio Frequency Identification) (Figs 1.1,1.2, and 1.3).

Almost all computer-oriented biometrics, which include face recognition, finger- print, and irises, are used for deployment in e- passport.

- *Face Recognition:* It means photographic imaging of face. Essentially, it is the automated analog of the human process for face recognition.
- *Fingerprint Recognition:* It depends on an imaging. Criminal investigation used finger print, which is often based on different type of features available in fingerprint. Fingerprint scanner can be silicon sensor or optical form.

Fig. 1.2 Fingerprint recognition https://www.nec.com/en/global/solutions/biometrics/fingerprint/index.html

Fig. 3.3 Iris recognition (https://www.biometricupdate.com/202206/iris- recognition-reaches-the-mainstream-for-identification-authentication)

- *Iris Recognition:* Noninvasive scanning which is deployed with the high-precision camera is used for iris scanning in biometric systems. In a biometric system, the device that collects the user data is called sensor.

1.1 Biometric Authentication Process

The biometric authentication process is nearly similar to other systems. An authenticated user can register initially by presenting a good-quality image to the sensor. The system can store the data in the data structure known as a template. The template is used as a reference for user authentication. Matching is the process where currently presented biometric data will be compared to the saved data contained in the templates for the authorized user.

It seems to be simple, but in reality, the process of biometric authentication is surrounded with security and privacy complications

2.3 The Biometric Threat of E-Passport

If the biometric data are leaked, than an e-passport will have the following risk:

- Security for e-passport deployment will be compromised.
- Compromised security for external biometric system also.

Biometric data play a very important role in the e-passport system. A digitized facial image is allocated as the "global interchange feature," which means that it will serve as international standard for biometric authentication.

Optional fields are fingerprint and iris information, which might be used at the issuing country's discretion. In biometric system, data secrecy is a subtle issue.

Two trends badly affecting security by the mean of public disclosure of biometric information:

1. Automatic
2. Spillover

- *Automation:* As biometric authentication is an automation process, so it normally leads to relaxation of oversight. This is the case with e-passport.

At the Malaysian airport, whenever an individual places an e-passport in front of the gate, it will automatically be opened and the individual with the help of a fingerprint scanner can authenticate himself, without any intervention from another human being. If the fingerprint data match with the e-passport data, then he or she can board the flight. Australia is also planning to implement "Smart Gate" technology in its airports with face recognition.

It will minimize human oversight for user authentication but will increase the chance of spoofing of biometric systems.

- *Spillover:* Biometric data stored in one system are used to authenticate user in multiple areas but can threaten the integrity with others or unrelated ones.

Many systems used for fingerprint recognition can be fooled when gelatin "fingers" are presented in them with ridges copied from the image of fingerprints. Biometric data are very important for individuals, so secrecy should be maintained so that unauthorized access of data can be prohibited.

1.1 Smart Card

In a system like client-server, smart card with the authentication scheme based on password is mostly used for validating a user residing at the remote location. Simple password can easily be hacked, to solve this type of problem secret keys of cryptographic and password is used for authentication purpose of the user located at the remote area [19]. This also had problem like long cryptographic keys are hard to remind and it leads confusion to identify the actual user.

Some merits of biometrics are as follows:

- Keys of biometrics are unforgettable.
- These types of keys are difficult to share or copy.
- It is very difficult to share or copy biometric keys.
- Difficult to guess easily.
- It is not easy to break someone's biometric information.

Thus authentication of remotely located user by biometric system is highly secured and reliable than the traditional authentication scheme [20].

2 Limitation and Future Scope

The biometric framework was significantly more efficient than traditional frame- work for recognition patterns. But still there are several issues that are mentioned below:

- The data are not to be used as secret.
- The data are not able to replace, or in case of elder people or manual workers, they do not have fingerprints.
- If the database of the biometric data anyhow gets corrupted, then the whole system fails.
- The secrecy requirements for biometric data imply that unauthorized reading of e-passport data is a security risk as well as a privacy risk. The risk will only grow with the push towards unsupervised use of biometric authentication.

To overcome these limitations, the future work for these problems will be:

- It is the great need to secure the biometric system more to avoid replication done by different hacking algorithms like antireply attack or to enhance the biometric system.
- There must be some techniques or protocols that were based on the signal processing and the cryptography mechanism that would protect the biometric data from the intruders.
- The future work is to identify all the practical threats on authentication and develop more secure authentication protocols with better results.

There must be constant update to keep the data protected

References

[1] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, *14*(1), 4–20. https://doi.org/10.1109/TCSVT.2003.818349.

[2] Liu, S., & Silverman, M. (2001). Practical guide to biometric security technology. *IT Professional*, *3*(1), 27–32. https://doi.org/10.1109/6294.899930.

[3] Bolle, R. M. (2001). Enhancing security. *IBM Systems*, *40*(3), 614–634. https://doi.org/10.1147/sj.403.0614.

[4] Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy Magazine*, *1*(2), 33–42. https://doi.org/10.1109/MSECP.2003.1193209.

[5] Juels, A., Molnar, D., & Wagner, D. (2005). Security and privacy issues in E-passports. Security and privacy for emerging areas in communications networks, 2005. In *SecureComm 2005. First International Conference on* (pp. 74–88). https://doi.org/10.1109/securecomm.2005.59

[6] Faundez-Zanuy, M. (2006). Biometric security technology. *IEEE Aerospace and Electronic Systems Magazine*, *21*(6), 15–26. https://doi.org/10.1109/MAES.2006.1662038.

[7] Lai, L., Ho, S. W., & Poor, H. V. (2011). Privacy–Security trade-offs in biometric security systems—Part I: Single use case. *IEEE Transactions on Information Forensics and Security*, *6*(1), 122–139. https://doi.org/10.1109/TIFS.2010.2098872.

[8] Huang, X., Xiang, Y., Chonka, A., Zhou, J., & Deng, R. H. (2011). A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. *IEEE Transactions on Parallel and Distributed Systems*, *22*(8), 1390–1397. https://doi.org/10.1109/TPDS.2010.206.

[9] Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2015). Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys and Tutorials*, *17*(3), 1268–1293. https://doi.org/10.1109/COMST.2014.2386915.

[10] Natgunanathan, I., Mehmood, A., Xiang, Y., Beliakov, G., & Yearwood, J. (2016). Protection of privacy in biometric data. *IEEE Access*, *4*, 880–892. https://doi.org/10.1109/ACCESS.2016.2535120

[11] Memon, N. (2017). How biometric authentication poses new challenges to our secu- rity and privacy [in the spotlight]. *IEEE Signal Processing Magazine*, *34*(4), 194–196. https://doi.org/10.1109/MSP.2017.2697179.

[12] Kumar, T., Braeken, A., Liyanage, M., & Ylianttila, M. (2017). Identity privacy preserving biometric based authentication scheme for Naked healthcare environment. *IEEE International Conference on Communications*. https://doi.org/10.1109/ICC.2017.7996966.

[13] Jaronde, P. W., Muratkar, N. A., Bhoyar, P. P., Gaikwad, S. J., & Nagrale, R. B. (2018). Review on biometric security system for newborn baby. *International Journal of Scientific Research in Science and Technology*, *4*(2), 907–909.

[14] Osadchy, M., & Dunkelman, O. (2018). It is all in the system's parameters: Privacy and security issues in transforming biometric raw data into binary strings. *IEEE Transactions Depend-able and SecureComputing*,*5971*(c),1–10. https://doi.org/10.1109/TDSC.2018.2804949.

[15] Srivastava, S., Agarwal, N., & Agarwal, R. (2013). Authenticating Indian E-health system through "Aadhaar" A unique identification. *International Journal of Scientific & Engineering Research*, *4*(6), 2412–2416.

[16] Kataria, A. N., Sharma, A. K., & Zaveri, T. H. (2013). *A survey of automated biometric authentication techniques* (pp. 1–6).

[17] Hemalatha, T., Krishna, D., Krishna, K. B., & Subhramanyam, V. B. (2014). Aadhar based electronic voting system and providing authentication. *International Journal of Engineering and Advanced Technology*, *4*(2), 237–240.

[18] Dixon, P. (2017). A failure to "Do No Harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S. *Health and Technology*, *7*(4), 539–567. https://doi.org/10.1007/s12553-017-0202-6.

[19] Wen, F., Susilo, W., & Yang, G. (2015). Analysis and improvement on a biometric-based remote user authentication scheme using smart cards. *Wireless Personal Communications*, *80*(4), 1747–1760. https://doi.org/10.1007/s11277-014-2111-6.

[20] Li, C. T., & Hwang, M. S. (2010). An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications*, *33*(1), 1–5. https://doi.org/10.1016/j.jnca.2009.08.001