Biometric Security in Internet of Things Based System against Identity Theft Attacks

Amit Kumar Tyagi[0000-0003-2657-8700]
Department of Fashion Technology, National Institute of Fashion Technology, New Delhi, Delhi India
amitkrtyagi025@gmail.com

Gadiparthy Harika Sai
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai Campus, Chennai, 600127, Tamilnadu, India.
gharikasai@gmail.com

N Sreenath
Department of Computer Science and Engineering, Puducherry Technological University, Puducherry, India
nsreenath@pec.edu

Abstract: Over the years, the Internet of Things (IoT) has been gaining popularity and is being used everywhere. The IoT has its applications extended to almost every area of technology. Though it is being used everywhere, security issues have been a major problem even in the field of IoT. One such issue is the identity theft attack. At times when companies or organizations are in a rush to get the IoT devices to market, they sometimes leave the devices unsecured and these are easily prone to security attacks. Hackers can get access to the personal information of the users and can create fake identities and hack the devices. To reduce these sorts of identity thefts, biometrics can come into play since biometrics remain unique to each person and cannot be copied by others. Biometrics comprise of fingerprints, iris, retina, face recognition, DNA, palm print etc. In this paper, an analysis of the possible biometric solutions for the problem is made and one feasible and appropriate solution is implemented. After a complete analysis, a fingerprint-based identification and authentication model is implemented in this work. This model can prevent the IoT devices from getting hacked or can make them less prone to security attacks like Identity Theft.

Keywords: Internet of Things, Security, Authentication, Biometrics, Identity Theft

I. INTRODUCTION

The Internet of Things (IoT) is a system of interconnected objects capable of collecting and transferring data over the internet. The 'things' in IoT refer to the devices connected that are attached sensors or RFID (Radio Frequency Identification) tags and internet connectivity. The services of IoT range from smart health cards to smart home control in the day-to-day lives of people. In recent years, there has been a constant increase in the number of IoT devices being connected to the internet. IoT uses IPV6 addressing over the internet instead of Ipv4 due to the limited address space of the latter [13]. IoT is being implemented successfully in many of the domains including Smart Environment, Health care, Smart Cities, Transportation and Logistics, Personal and Social, Agriculture and Pharmaceutical industry etc., [1]. Many recent studies stated that the IoT would rule the network industry by extending its applications to every sector existing in the coming decades. IoT is being used everywhere in the world with thousands of users authenticating the involved devices which also sometimes leads to security attacks in IoT. Security of a device or data has the main stand in any of the systems. While the security between IoT devices is being focused constantly by researchers and developers, the security between an IoT device and the user accessing it is being neglected in some cases. This is the main reason behind the increase in Identity Thefts in IoT over the recent years.

979-8-3503-4821-7/23/$31.00 ©2023 IEEE

Identity thefts can lead to unpredictable loss of data which mainly involves the loss of personal data, the connections concerning the device prone to attack. Not just the user or device that is being attacked but also the other devices or users connected to that particular device are also vulnerable to security attacks. Identity theft attacks have become more prevalent than even some coffee machines that are connected over the internet could be taken over by the hackers to steal the respective machine's owner personal data or some kind of important bank details which can result in a huge loss to the user.

With many increased hackers and hacking techniques in recent decades, IoT devices are subjected to attacks easily. This is where user authentication is necessary. Unauthorized access of the devices can lead to the disclosure of personal information of the user or misuse of the device etc. Password-based security has become outdated because of this. Cryptographic security can also aid in security but once a cryptographic key is cracked, then it will be easier for the hackers to take control over the system. Also, cryptographic based security is suitable for the threats that occur between the devices and data or data and data in the IoT environment but not in the device-user security. IoT operates over different layers of communication level and different types of security suit at different communication levels. Biometric security is highly endorsed in the layers where human authentication is required directly. Biometric authentication can play a key role in security because the bio-features of a person cannot be replicated and used by someone else which in turn provides a very good way of securing the IoT device. Biometric security deals with the identification of users based on their physiological and behavioural characteristics. This unique aspect of biometrics is making it usable and reliable in many larger industries, government applications like Aadhar etc. It is not that the biometric-based security system is not at all vulnerable to any kind of threat but it makes it difficult for the hackers or perpetrators to cause threats to the system having biometric security when compared to any other kind of security mechanisms since biometrics are unique to each person as stated earlier. The remaining part of the work is organized as:

- The section of Literature Survey discusses the already available work in the past on biometric security and challenges in the field of IoT. There is a lot of research going on in this particular field of security in IoT.
- The section of Problem Definition defines the problem of prevailing security attacks in IoT including the Identity Theft attacks. It discusses different forms of security threats that IoT devices and data are vulnerable to. Section 4 focuses on the existing type of biometrics and solutions for the security of IoT. The two types of

biometric features- physiological and behavioural features have a number of ways through which the IoT devices and data can be secured with.

- The section of Existing Solutions discusses the prevailing solutions of each biometric type, their advantages and their limitations.
- The section of Proposed Model explains the proposed model of fingerprint-based authentication system for the security of IoT based systems against Identity Theft attacks. This section gives an overview of the idea, algorithm and implementation of the proposed model i.e., it discusses the dataset involved, the modules that have been worked on and the results as well. The section of simulation results includes pictures of the output of the execution of the proposed model.
- The section of Conclusion and Future Work states the future enhancements that can be done to the proposed model of biometric-based authentication system and the fields of network this model can be extended to provide security.

Hence in this work, the mai aim is to provide an IoT based system with a proper, appropriate, secure and reliable biometric security model from the available ones after analysing each biometric type. This aids in reducing the Identity Theft attacks prevailing in the corresponding field.

II. LITERATURE SURVEY

There has been a lot of research going on in this area of IoT security based on biometrics over the recent years. An efficient door locking system in home security was developed in [3]. The system was made using a fingerprint module and a raspberry pi board. This also gets the status of the gas and fire and this can be accessed remotely from any location using IoT. Biometric technology for the security of IoT can also extend its applications to the idea of smart health. The development of e-health and smart health care systems demand good security and privacy of users and data. An approach to developing such sort of security in smart healthcare using biometric technology is mentioned in [4]. Behavioural biometrics like voice can also be used to access IoT devices and protect them with security. Methods and tools involved in establishing a voice recognition system are assessed and their use in the IoT has been discussed in [7]. In this proposed voice recognition system, there are two phases. The first phase is the enrolment process where the noise is removed from the voice and then it is enrolled into the database using some feature extraction techniques. The second phase is the authentication phase where the voice is authenticated if it belongs to the database or not.

Another physiological feature that can be used in user identification is Electrocardiography (ECG) which is also a promising approach for user identification and Authentication. All the statistical, morphological and wavelet features belonging to ECG remain unique to every individual. In [9] a particular feature selection, using the fiducial points from the ECG based authentication system is proposed. The evaluation results of this model reached very high accuracy results greater than 98.2% which proved this model is good enough for user authentication. An overview and an analysis of different machine learning models and data mining methods used in authentication schemes for many IoT devices are discussed in [18]. Also, the threats and countermeasures of biometric-based authentication for IoT devices are assessed. Detailed analyses on the existing biometric-based authentication models in the area of IoT security are also analyzed. Detailed analysis on the different biometrics like fingerprint, iris, smart card, face recognition etc., that can be considered for user identification and authentication are also discussed.

A lightweight biometric-based authentication and a key agreement scheme in IoT services security has been proposed and discussed in [20]. Lightweight hash operations and XOR operations are made use of in this lightweight biometric-based authentication scheme. This analysis of security proves that this system is efficient security against many security attacks. AVISPA tool is used for performing verification in this model which confirms security against a possible intruder. The use of different biometrics for user authentication and security against Identity Theft Attacks is discussed and analysed in [21]. Also, vulnerabilities in the biometric system are discussed in the work. The limitations, adversary attacks possible in Biometrics based authentication are also mentioned. The Identity sciences involved in biometric-based identification are also discussed. The security templates and requirements are also assessed in the research. In the last, authors in [27, 28, 29, 30, 31, and 32] have listed various uses of Blockchain in preserving privacy, analytics role for improving people life or increase growth of many sectors, whereas articles [30, 31] summarize that how cyber-attacks are the essential attacks to counter/ overcome in this smart era with emerging technologies.

III. PROBLEM DEFINITION

IoT has its applications extended to almost every area of technology and communication. Though the IoT has its applications in every aspect of technology, there are security issues that are troubling users and companies in trusting the IoT services and devices.

Security Attacks in IoT

Though the IoT is gaining popularity over the recent years, IoT devices and data involved are vulnerable to many security attacks if not handled appropriately. It has been reported by SonicWALL that in 2018 there has been an increase of 215.7% (from 10.3 million in 2017to 32.7 million in 2018) in IoT malware attacks [22, 33-57]. There are numerous cyber-attacks that IoT devices are vulnerable to. A quick dive into a few possible security attacks in IoT:

- ***Encryption Attacks****:* These types of attacks occur when there is data on the IoT that is left unencrypted. This data can be accessed by hackers or perpetrators easily leading to a data loss. Also, if an encryption key is unlocked once, then the attackers can use their algorithms and take over the system control.
- ***Botnets****:* Botnet is a typical network of devices or routers connected to the IoT that are either malicious or taken over by malicious actors. These botnets lead to a plethora of security attacks concerning the IoT out of which a DDoS attack is also one. Generally, a single command-and-control (C&C) server controls these botnets which are connected to all these infected devices called the “bots”. Another

exceptional case is the use of peer-to-peer networking instead of the C&C server making it more back-breaking to turn these botnets down.

- ***Man in the Middle Attack:*** This attack occurs when there is a communication breach between two systems or networks by any hacker or perpetrator. A secret intervention is made in the communication between two parties making the recipient believe that the message received is an authorized one from the sender.
- ***DoS Attack:*** DoS attack is a situation where a resource or a network is made unavailable by the perpetrators by disrupting the service of the device connected over the internet. A DDoS attack is where a target is attacked by a large number of systems. These attacks are generally done by the botnet where a single service is demanded by many devices at the same time.
- ***Identity Theft Attack:*** A situation where an unauthorized person can access an IoT device by stealing the identity of the user like stealing the passwords or PIN etc. This can lead to loss of personal data or misuse of that particular device over the internet. If an IoT device is being accessed by an unauthorized person, then the data produced or being communicated by that device is instinctively at stake. Identity theft attacks have been a major concern and there have been a lot of problems arising because of this Identity theft and unauthorized access.

IV. EXISTING SOLUTIONS

Identity thefts have been increasing over the recent decades and are leading to the loss of the personal data of a lot of users. In the case of Identity Theft, it is not only the user who is going to be in trouble but also there is a threat to the data of other users who are connected to the respected user because the user's identity is impersonated by someone else. This can be a very huge problem in the fields of large businesses as well. This is where there is a need to authenticate users on their identity. There are a lot of techniques and models being followed for the authentication of users. Data encryption is one such technique but this only provides security to the IoT data but not the devices involved. There is still a chance for the perpetrators to get access to the device and misuse it. Another way is securing the devices with high-security passwords. Though this had been a traditional model in the past, this can no longer be followed because there are a lot of hackers who can hack these with so much ease. This is where biometrics can be brought into play.

Biometric Security against Identity Theft

The biometrics of each person remains unique and cannot be impersonated by someone else. This unique feature of biometrics makes them stand on top in securing any device or data. In the field of IoT, the security of data and security between devices are being given more importance in recent times. But the security of a device from the user is being neglected which also can lead to a huge loss of data and personal information of the users handling the data. Biometrics can improve the security of a device against Identity Thefts. There are many biometric technologies available that can be used in the security of the devices. Biometrics are typically of 2 types: Physiological features and Behavioral Features

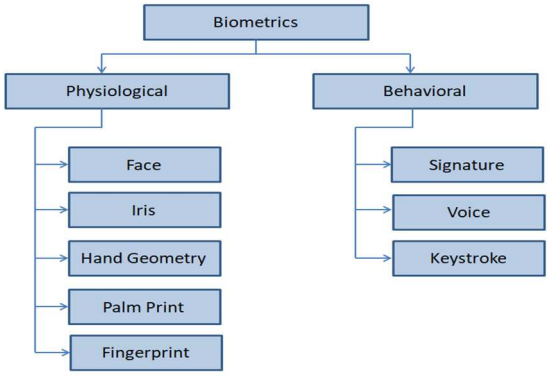

Figure 1: Types of biometrics

Physiological Features

These features refer to the direct measurements of any part of a human body like the face, iris, retina, hand geometry, etc. More types of biometrics can be found in figure 1.

- ***Face:*** Face recognition algorithms have been popular in recent times. These algorithms use the relationship among different facial features like eyes, nose, lips, chin and also the overall appearance of the face. Some factors that make trouble in face recognition algorithms are the makeover, brightness, obstruction etc. Moreover, if there is a person who is a look-alike of the user, then this face recognition technique would fail in that case. Though the face recognition technology has good accuracy, it fails in the above-mentioned case. An implementation of a novel face identification framework can be seen in [25] which is capable of handling all kinds of pose variants.
- ***Iris:*** Iris is a coloured part in the eye around the pupil that has complex human eye patterns and it is proved that iris patterns remain unique to each individual i.e, no two persons have the same iris patterns and this feature makes the iris-recognition patterns more reliable. The stripes, furrows, pits in the iris of a person are considered for identification and authentication of a person and are considered to be proof of identity in many government applications like Aadhar as well. The accuracy of iris-recognition patterns has been proved to be medium. One drawback is the lack of legacy in many databases of iris patterns which makes it to be a hassle for many applications involving iris-based recognitions.
- ***Hand Geometry:*** It is also proved that a person can be identified and authenticated based on the shape of their hands. Features that come into play here are the width, height, thickness, perimeter of the palm and the area covered by the fingers. This model uses low-resolution hand pattern image samples for extracting the features mentioned above. Since the accuracy of this hand geometry-based recognition is not so high and quite limited, it is mostly restricted to 1:1 classification and not extended to 1:N classification.
- ***Palm Print:*** Another accepted biometric in the field of IoT security is the alm print-based recognition. This is similar to fingerprint-based recognition which uses the ridges and creases on the palm for identification. There is also research going on in the area of 3D palmprint

recognition systems[26]. 3D palmprint has many advantages over the normal 2D palmprint based recognition. Though there are merits, this is also restricted only to 1:1 classification but not used for 1:N classification in the identification scenario. This makes it one of the drawbacks for palmprint based recognition techniques from being used widely.

- ***Fingerprint:*** Fingerprint-based recognition models have been quite successful over recent years. This can be used in personal identification and authentication even in the field of IoT security. Fingerprint remains unique to every individual and cannot be copied by someone else. Every fingerprint has its unique pattern or texture made of ridges and valleys. The minutiae points which are used to categorize the ridges are used to match fingerprints of two different persons. Fingerprint authentication is also being used in identifying criminals worldwide. Forensic departments of many countries consider using fingerprint-based for their civil and commercial purposes as well.

Behavioural Features

- ***Signature:*** One of the behavioural biometrics which is used in everyday transactions in business and other commercial purposes as well. Many pieces of research on concrete and accurate signature-based recognition models are going on but are not successful yet. Though signature is being used in everyday life frequently, it is more vulnerable to many threats and identity thefts as well. One's signature can be forged by an expert and this can result in a huge loss of personal data. Though the security level of the signature biometric is low, it can still be used on small scale recognition models.
- ***Voice:*** Voice-based recognition systems identify persons based on their vocalized worlds. This particular behavioural biometric also involves a bit of physiological biometric features like the shape and size of the vocal tracts, cavities, lips and mouth. The duration, pitch and intensity of the voice play a major role in training the model for voice-based recognition. The voice-based recognition system is also vulnerable to threats because an expert could easily mimic the voice of a user and can access the information. Another drawback is that if the user's voice is not good due to some reasons and even if it has small variations, he or she cannot access the device or the information.
- ***Keystroke:*** An authentication system based on the typing patterns of the individuals. But there is no solid proof or evidence yet that no two persons have the same keystroke dynamics which makes it a drawback for this model.

V. PROPOSED MODEL

After analysing the different biometric techniques available with regards to different parameters, fingerprint recognition proved to be more promising in terms of identification and authentication. The following table 1 shows the comparison of different biometric technologies available [1, 24] :

Table 1: Comparison of different biometric techniques

Type of Biometric	Accuracy	Ease of Implementation	Easy to use	Cost
Voice	Medium	High	High	Low
Retina	High	Low	Low	Medium
Iris	Medium	Medium	Medium	High
Face	Low	Medium	High	Low
Hand Geometry	Medium	Medium	High	High
Signature	Medium	Low	Medium	Medium
Fingerprint	High	High	Medium	Medium

Fingerprint recognition model

The implementation is entirely done in python with a few deep learning algorithms (see figure 2) involved.

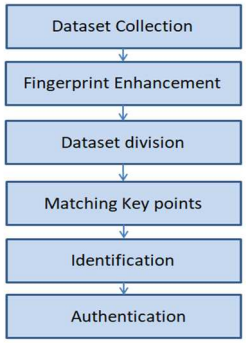

Figure 2: Flowchart of the proposed model

- ***Dataset:*** For the fingerprint samples, the dataset has been made use of from FVC2002: the second International Competition for different Fingerprint Verification Algorithms. This particular dataset has 4 different fingerprint databases out of which the second database DB2 has been used here for training. And for the testing purpose, samples from the same DB2 dataset and also samples from the DB1 dataset have been used. The DB2 dataset has a total of 80 fingerprint images belonging to 10 different individuals, 8 samples per person.
- ***Fingerprint Enhancement:*** All the fingerprints are then processed, enhanced and converted to greyscale using an enhancement library that makes use of Oriented Gabor Filter which is a linear filter used for texture analysis in image processing [23]. The ridges of the images are oriented properly so that they would be accurate for further processing and identification. Then the dataset is divided into training and test sets. Also, the DB1 images are processed the same way and used as test images.
- ***Keypoints Matching:*** Oriented FAST and Rotated BRIEF (ORB) descriptor is used in finding the matching key points of the fingerprints. For matching this, we match features and the count of these matching features using a threshold value determines the number of key points matched

- ***Identification and Authentication:*** For the identification purpose a 1:N classification algorithm is used where the input fingerprint sample is taken and then is searched among the database if it is present. Then for the Authentication scenario, A 1:1 classification is used where the fingerprint sample is matched against every sample image that is in the database. If there are any matches and the probability of accuracy is greater than 83.3%, the user is authenticated and if less than that, the person is not authenticated.
- ***Testing the model*:** As mentioned, for testing the model samples from two different datasets are used. A test sample image from the dataset DB2 which is also used for training gives the result as an authenticated user. Any sample from the other dataset results in an unauthorized user.

VI. SIMULATION RESULTS

A few snippets of the simulation of the proposed model are shown below. Figure 3 displays a few pictures from the dataset that has been used. Figure 4 shows a sample fingerprint image that has been enhanced over the ridges making it easier for recognition and making the model accurate.

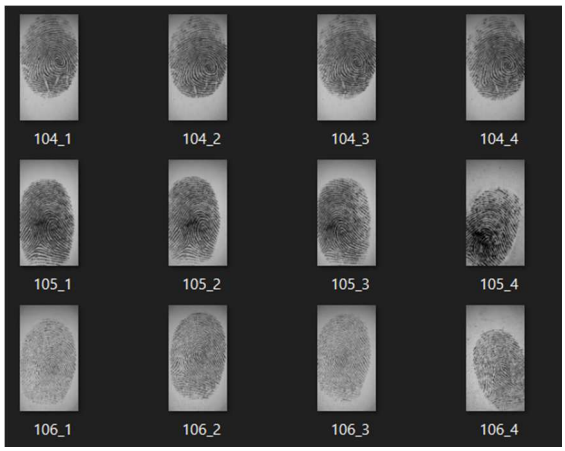

Figure 3: An overview of the dataset

```
plt.subplot(1, 2, 1)
plt.title('Before enhancement')
img_fpr = cv2.imread(image_files[0])
plt.imshow(img_fpr, cmap='gray')
plt.subplot(1, 2, 2)
plt.title('After enhancement')
img = cv2.imread(image_files[0])
gray_img = grayscale_image(img)
img = enhance_image(gray_img)
plt.imshow(img, cmap='gray')
plt.show()
```

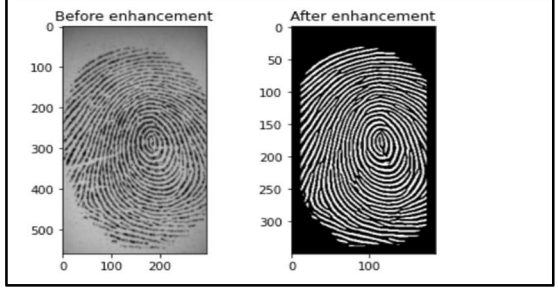

Figure 4: Sample of an enhanced fingerprint image

Figure 5 shows the result where a person is correctly authenticated i.e, the sample used for testing, in this case, is a sample from the trained dataset. Figure 6 shows the result where a person is not authenticated i.e., the sample used for testing, in this case, is an image from another different dataset.

```
# Example
test_image_id = list(test_set)[13]
authentication_db = {}
ratio = {}
authentication_db[0]=authentication_databases['101']
authentication_db[1]=authentication_databases['102']
authentication_db[2]=authentication_databases['103']
authentication_db[3]=authentication_databases['104']
authentication_db[4]=authentication_databases['105']
authentication_db[5]=authentication_databases['106']
authentication_db[6]=authentication_databases['107']
authentication_db[7]=authentication_databases['108']
authentication_db[8]=authentication_databases['109']
authentication_db[9]=authentication_databases['110']
for i in range(0,10,1):
    best_matches_dict = get_best_matches(test_set[test_image_id], authentication_db[i] , 73)
    count_same = count_same_fprs(best_matches_dict, 12)
    ratio[i] = count_same/len(authentication_db[i].keys())
print('--- For query image: {} ---'.format(test_image_id))
max=0
for i in range(1,10,1):
    if(ratio[i]>max):
        max=ratio[i]
        j=i
fpr=format(round(max,4))
if(float(fpr)>=0.83):
    print('Person Authenticated')
else:
    print('Person not Authenticated')
```

```
--- For query image: 107_6.tif ---
Person Authenticated
```

Figure 5: Example of an authenticated sample

```
# Example
test_image_id = list(test_set1)[13]
authentication_db = {}
ratio = {}
authentication_db[0]=authentication_databases['101']
authentication_db[1]=authentication_databases['102']
authentication_db[2]=authentication_databases['103']
authentication_db[3]=authentication_databases['104']
authentication_db[4]=authentication_databases['105']
authentication_db[5]=authentication_databases['106']
authentication_db[6]=authentication_databases['107']
authentication_db[7]=authentication_databases['108']
authentication_db[8]=authentication_databases['109']
authentication_db[9]=authentication_databases['110']
for i in range(0,10,1):
    best_matches_dict = get_best_matches(test_set1[test_image_id], authentication_db[i] , 73)
    count_same = count_same_fprs(best_matches_dict, 12)
    ratio[i] = count_same/len(authentication_db[i].keys())
print('--- For query image: {} ---'.format(test_image_id))
max=0
for i in range(1,10,1):
    if(ratio[i]>max):
        max=ratio[i]
        j=i
fpr=format(round(max,4))
if(float(fpr)>=0.83):
    print('Person Authenticated')
else:
    print('Person not Authenticated')
```

```
--- For query image: DB1_B\102_6.tif ---
Person not Authenticated
```

Figure 6: Example of an unauthenticated sample

VII. CONCLUSION AND FUTURE WORK

The proposed fingerprint recognition is implemented entirely in python using a few deep learning techniques, ORB detector for matching key points. After an analysis of all the different biometric techniques available, fingerprint-based recognition was found to be more feasible, accurate and easy to implement and maintain further. This model uses a simple dataset for training and testing with a total of 80 images. One additional feature of the model is that this also involves enhancement of the fingerprint samples which makes it easier and more accurate while matching the key points, identification and authentication scenarios. The work can be extended to a large dataset for testing purposes. This model has an accuracy of approximately 90 per cent which can be increased further with the use of some algorithms. This model can extend its use to healthcare in the identification and authentication of patients and doctors. This proposed model can also be used in banks

where the devices store highly confidential information and transaction details of the users. The use of biometric-based security systems in banks is gaining popularity in recent times and the proposed model could also contribute to the same.

REFERENCES

[1] Mohammad S. Obaidat, Soumya Prakash Rana, Tanmoy Maitra, Debasis Giri, and Subrata Dutta, "Biometric security and internet of things (IoT)." *Biometric-Based Physical and Cybersecurity Systems*. Springer, Cham, 2019. 477-509.

[2] Z. Guo, N. Karimian, M. M. Tehranipoor and D. Forte, "Hardware security meets biometrics for the age of IoT," 2016 IEEE International Symposium on Circuits and Systems (ISCAS), 2016, pp. 1318-1321, doi: 10.1109/ISCAS.2016.7527491.

[3] Prakash, Narayanam Sri, and N. Venkatram. "Establishing efficient security scheme in home IoT devices through biometric fingerprint technique." *Indian Journal of Science and Technology* 9.17 (2016): 1-8.

[4] Hamidi, Hodjat. "An approach to develop the smart health using Internet of Things and authentication based on biometric technology." *Future generation computer systems* 91 (2019): 434-449.

[5] Habib, Kashif, Arild Torjusen, and Wolfgang Leister. "A novel authentication framework based on biometric and radio fingerprinting for the IoT in eHealth." *SMART 2014: The Third International Conference on Smart Systems, Devices, and Technologies*. 2014.

[6] Oday A. Hassen, Ansam A. Abdulhussein, Saad M. Darwish, Zulaiha Ali Othman, Sabrina Tiun and Yasmin A. Lotfy, "Towards a Secure Signature Scheme Based on Multimodal Biometric Technology: Application for IoT Blockchain Network." *Symmetry* 12.10 (2020): 1699.

[7] Duraibi, Salahaldeen. "Voice Biometric Identity Authentication Model for IoT Devices." *International Journal of Security, Privacy and Trust Management (IJSPTM) Vol* 9 (2020).

[8] M. S. Hossain, G. Muhammad, S. M. M. Rahman, W. Abdul, A. Alelaiwi and A. Alamri, "Toward end-to-end biometrics-based security for IoT infrastructure," in IEEE Wireless Communications, vol. 23, no. 5, pp. 44-51, October 2016, doi: 10.1109/MWC.2016.7721741.

[9] Barros, D. Rosário, P. Resque and E. Cerqueira, "Heart of IoT: ECG as biometric sign for authentication and identification," 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), 2019, pp. 307-312, doi: 10.1109/IWCMC.2019.8766495.

[10] Yang, Wencheng, et al. "A privacy-preserving lightweight biometric system for internet of things security." *IEEE Communications Magazine* 57.3 (2019): 84-89.

[11] Dhillon, Parwinder Kaur, and Sheetal Kalra. "Secure multi-factor remote user authentication scheme for Internet of Things environments." *International Journal of Communication Systems* 30.16 (2017): e3323.

[12] Taheri, Shayan, and Jiann-Shiun Yuan. "A cross-layer biometric recognition system for mobile IoT devices." *Electronics* 7.2 (2018): 26.

[13] Meena, Gaurav, and Sarika Choudhary. "Biometric authentication in the internet of things: A conceptual view." *Journal of Statistics and Management Systems* 22.4 (2019): 643-652.

[14] Maček, Nemanja, et al. "Multimodal biometric authentication in IoT: Single camera case study." In Int. Conf. BISEC 2016, October, 2016, 33-38. Available at: http://eprints.ugd.edu.mk/16526/1/1.pdf

[15] Vidalis, Stilianos, and Olga Angelopoulou. "Assessing identity theft in the Internet of Things." *Journal of IT Convergence Practice* (2014).

[16] S. Rizvi, A. Kurtz, J. Pfeffer and M. Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 163-168, doi: 10.1109/TrustCom/BigDataSE.2018.00034.

[17] Labong, Ronel C. "Identity Theft Protection Strategies: A Literature Review." *Journal of Academic Research* 4.2 (2019): 1-12.

[18] Ferrag, Mohamed Amine, Leandros Maglaras, and Abdelouahid Derhab. "Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends." *Security and Communication Networks* 2019 (2019).

[19] M. Golec, S. S. Gill, R. Bahsoon and O. Rana, "BioSec: A Biometric Authentication Framework for Secure and Private Communication among Edge Devices in IoT and Industry 4.0," in IEEE Consumer Electronics Magazine, doi: 10.1109/MCE.2020.3038040.

[20] Dhillon, Parwinder Kaur, and Sheetal Kalra. "A lightweight biometrics-based remote user authentication scheme for IoT services." *Journal of Information Security and Applications* 34 (2017): 255-270.

[21] Jain, Anil K., and Karthik Nandakumar. "Biometric authentication: System security and user privacy." *Computer* 45.11 (2012): 87-92.

[22] https://www.onetech.ai/en/blog/10-types-of-cyber-security-attacks-in-the-iot

[23] https://github.com/Utkarsh-Deshmukh/Fingerprint-Enhancement-Python

[24] De Luis-García, R., Alberola-López, C., Aghzout, O., & Ruiz-Alzola, J. (2003). *Biometric identification systems. Signal Processing, 83(12), 2539–2557.* doi:10.1016/j.sigpro.2003.08.001

[25] C. Ding, C. Xu and D. Tao, "Multi-Task Pose-Invariant Face Recognition," in IEEE Transactions on Image Processing, vol. 24, no. 3, pp. 980-993, March 2015, doi: 10.1109/TIP.2015.2390959.

[26] L. Zhang, Y. Shen, H. Li and J. Lu, "3D Palmprint Identification Using Block-Wise Features and Collaborative Representation," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 37, no. 8, pp. 1730-1736, 1 Aug. 2015, doi: 10.1109/TPAMI.2014.2372764.

[27] Tyagi A.K., Kumari S., Fernandez T.F., Aravindan C. (2020) P3 Block: Privacy Preserved, Trusted Smart Parking Allotment for Future Vehicles of Tomorrow. In: Gervasi O. et al. (eds) Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science, vol 12254. Springer, Cham. https://doi.org/10.1007/978-3-030-58817-5_56.

[28] M. M. Nair, A. K. Tyagi and N. Sreenath, "The Future with Industry 4.0 at the Core of Society 5.0: Open Issues, Future Opportunities and Challenges," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-7, doi: 10.1109/ICCCI50826.2021.9402498.

[29] Tyagi A.K., Fernandez T.F., Mishra S., Kumari S. (2021) Intelligent Automation Systems at the Core of Industry 4.0. In: Abraham A., Piuri V., Gandhi N., Siarry P., Kaklauskas A., Madureira A. (eds) Intelligent Systems Design and Applications. ISDA 2020. Advances in Intelligent Systems and Computing, vol 1351. Springer, Cham. https://doi.org/10.1007/978-3-030-71187-0_1

[30] Amit Kumar Tyagi. Article: Cyber Physical Systems (CPSs) – Opportunities and Challenges for Improving Cyber Security. International Journal of Computer Applications 137(14):19-27, March 2016. Published by Foundation of Computer Science (FCS), NY, USA.

[31] G. Rekha, S. Malik, A.K. Tyagi, M.M. Nair "Intrusion Detection in Cyber Security: Role of Machine Learning and Data Mining in Cyber Security", Advances in Science, Technology and Engineering Systems Journal, vol. 5, no. 3, pp. 72-81 (2020).

[32] Mishra S., Tyagi A.K. (2022) The Role of Machine Learning Techniques in Internet of Things-Based Cloud Applications. In: Pal S., De D., Buyya R. (eds) Artificial Intelligence-based Internet of Things Systems. Internet of Things (Technology, Communications and Computing). Springer, Cham. https://doi.org/10.1007/978-3-030-87059-1_4

[33] Amit Kumar Tyagi (2022), Handbook of Research on Technical, Privacy, and Security Challenges in a Modern World. IGI Global. DOI: 10.4018/978-1-6684-5250-9

[34] Khushboo Tripathi, Manjusha Pandey, and Shekhar Verma. 2011. Comparison of reactive and proactive routing protocols for different mobility conditions in WSN. In Proceedings of the 2011 International Conference on Communication, Computing & Security (ICCCS '11). Association for Computing Machinery, New York, NY, USA, 156–161. https://doi.org/10.1145/1947940.1947974

[35] Jajula, S.K., Tripathi, K., Bajaj, S.B. (2023). Review of Detection of Packets Inspection and Attacks in Network Security. In: Dutta, P., Chakrabarti, S., Bhattacharya, A., Dutta, S., Piuri, V. (eds) Emerging Technologies in Data Mining and Information Security. Lecture Notes in Networks and Systems, vol 491. Springer, Singapore. https://doi.org/10.1007/978-981-19-4193-1_58

[36] Ranchhodbhai P.N, Tripathi K., "Identifying and Improving the Malicious Behavior of Rushing and Blackhole Attacks using Proposed IDSAODV Protocol", International Journal of Recent Technology and Engineering, vlo. 8(3), pp.6554-6562, 2019

[37] Midha S, Tripathi K, Sharma MK. Practical Implications of Using Dockers on Virtualized SDN. Webology. 2021 Apr; 18,pp.312-30.

[38] D. Agarwal and K. Tripathi, "A Framework for Structural Damage detection system in automobiles for flexible Insurance claim using IOT and Machine Learning," 2022 International Mobile and Embedded Technology Conference (MECON), 2022, pp. 5-8, doi: 10.1109/MECON53876.2022.9751889.

[39] S. Midha, G. Kaur and K. Tripathi, "Cloud deep down — SWOT analysis," *2017 2nd International Conference on Telecommunication and Networks (TEL-NET)*, 2017, pp. 1-5, doi: 10.1109/TEL-NET.2017.8343560.

[40] Sai, G.H., Tripathi, K., Tyagi, A.K. (2023). Internet of Things-Based e-Health Care: Key Challenges and Recommended Solutions for Future. In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P.C., Ganzha, M. (eds) Proceedings of Third International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems, vol 421. Springer, Singapore. https://doi.org/10.1007/978-981-19-1142-2_37

[41] S. Subasree, N.K. Sakthivel, Khushboo Tripathi, Deepshikha Agarwal, Amit Kumar Tyagi, Combining the advantages of radiomic features based feature extraction and hyper parameters tuned RERNN using LOA for breast cancer classification, Biomedical Signal Processing and Control, Volume 72, Part A, 2022, 103354, ISSN 1746-8094, https://doi.org/10.1016/j.bspc.2021.103354.

[42] Kumari, S. & Muthulakshmi, P. (2022). Transformative Effects of Big Data on Advanced Data Analytics: Open Issues and Critical Challenges. Journal of Computer Science, 18(6), 463-479. https://doi.org/10.3844/jcssp.2022.463.479

[43] Somisetti, K. Tripathi and J. K. Verma, "Design, Implementation, and Controlling of a Humanoid Robot," *2020 International Conference on Computational Performance Evaluation (ComPE)*, 2020, pp. 831-836, doi: 10.1109/ComPE49325.2020.9200020.

[44] S. Midha and K. Triptahi, "Extended TLS security and Defensive Algorithm in OpenFlow SDN," *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2019, pp. 141-146, doi: 10.1109/CONFLUENCE.2019.8776607.

[45] Midha, S., Tripathi, K. (2021). Extended Security in Heterogeneous Distributed SDN Architecture. In: Hura, G., Singh, A., Siong Hoe, L. (eds) Advances in Communication and Computational Technology. Lecture Notes in Electrical Engineering, vol 668. Springer, Singapore. https://doi.org/10.1007/978-981-15-5341-7_75

[46] Midha, S., Tripathi, K. (2020). Remotely Triggered Blackhole Routing in SDN for Handling DoS. In: Dutta, M., Krishna, C., Kumar, R., Kalra, M. (eds) Proceedings of International Conference on IoT Inclusive Life (ICIIL 2019), NITTTR Chandigarh, India. Lecture Notes in Networks and Systems, vol 116. Springer, Singapore. https://doi.org/10.1007/978-981-15-3020-3_1

[47] Mapanga, V. Kumar, W. Makondo, T. Kushboo, P. Kadebu and W. Chanda, "Design and implementation of an intrusion detection system using MLP-NN for MANET," *2017 IST-Africa Week Conference (IST-Africa)*, 2017, pp. 1-12, doi: 10.23919/ISTAFRICA.2017.8102374.

[48] Tyagi, A.K. (Ed.). (2021). Data Science and Data Analytics: Opportunities and Challenges (1st ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781003111290

[49] Tyagi, A.K., & Abraham, A. (Eds.). (2022). Recurrent Neural Networks (1st ed.). CRC Press. https://doi.org/10.1201/9781003307822

[50] Tyagi, A.K., & Abraham, A. (Eds.). (2021). Recent Trends in Blockchain for Information Systems Security and Privacy (1st ed.). CRC Press. https://doi.org/10.1201/9781003139737

[51] Kumar Tyagi, A., Abraham, A., Kaklauskas, A., Sreenath, N., Rekha, G., & Malik, S. (Eds.). (2022). Security and Privacy-Preserving Techniques in Wireless Robotics (1st ed.). CRC Press. https://doi.org/10.1201/9781003156406

[52] Tyagi, A. K., Rekha, G., & Sreenath, N. (Eds.). (2021). Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles. IGI Global. http://doi:10.4018/978-1-7998-3295-9

[53] Tyagi, A. K. (Ed.). (2021). Multimedia and Sensory Input for Augmented, Mixed, and Virtual Reality. IGI Global. http://doi:10.4018/978-1-7998-4703-8

[54] Malik, S., Bansal, R., & Tyagi, A. K. (Eds.). (2022). Impact and Role of Digital Technologies in Adolescent Lives. IGI Global. http://doi:10.4018/978-1-7998-8318-0

[55] Akshita Tyagi, Swetta Kukreja, Meghna Manoj Nair, Amit Kumar Tyagi, Machine Learning: Past, Present and Future, Neuroquantology, Volume 20, No 8 (2022), DOI: 10.14704/nq.2022.20.8.NQ44468

[56] Goyal, Deepti & Tyagi, Amit. (2020). A Look at Top 35 Problems in the Computer Science Field for the Next Decade. 10.1201/9781003052098-40.

[57] Amit Kumar Tyagi and Meghna Manoj Nair. 2022. Preserving Privacy using Distributed Ledger Technology in Intelligent Transportation System. In Proceedings of the 2022 Fourteenth International Conference on Contemporary Computing (IC3-2022). Association for Computing Machinery, New York, NY, USA, 582–590. https://doi.org/10.1145/3549206.3549306