IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203077 |

Biometrics Recognition

Harsh Jain [1], Dr. MN Nachappa [2]

PG Student, School of CS & IT, Jain(Deemed-to-be-University), Bengaluru, India [1]

Professor, School of CS & IT, Jain(Deemed-to-be-University), Bengaluru, India [2]

ABSTRACT: In the realm of modern security protocols, biometric recognition stands as a beacon of advancement, offering unparalleled authentication precision through the analysis of unique biological traits. This comprehensive report navigates through the intricate landscape of biometric authentication, shedding light on its multifaceted facets. The discourse begins by dissecting the pivotal phases of biometric authentication: enrollment and verification. During enrollment, individuals' distinctive biometric data are meticulously captured and transformed into digitized templates. Subsequently, the verification process scrutinizes presented biometric data against these templates, ensuring a robust authentication mechanism. Delving deeper, the report surveys the expansive array of applications spanning finance, healthcare, government, and law enforcement sectors. It delineates the diverse biometric modalities, with fingerprint recognition reigning supreme for its reliability and ubiquity. Moreover, it examines emerging modalities like facial recognition, catering to evolving security paradigms. Beyond functionality, the report unravels the intricacies of biometric devices, assessing their efficacy, ease of use, and error rates. Furthermore, it contemplates the dichotomy of biometrics in bolstering national security while confronting challenges of forgery and privacy infringement. In essence, this report encapsulates the transformative potential of biometric recognition in fortifying authentication protocols, heralding a new era of security prowess in the digital age.

I. INTRODUCTION

Reliable authentication is an important factor in virtual online world. The consequences of unreliable authentication system in today's world where maximum transactions are made online may cause loss of denial of service, confidential information leak and bring catastrophe to the business. User authentication is not only restricted to accessing a device or system. User authentication is used in various field, such as banking. There are some drawbacks to the prevalent user validation methods, which include the use of passwords and user IDs. By direct covert observation, passwords and PINs may be illicitly obtained. Once the user ID and the password are obtained by an intruder, the intruder has unlimited access to the resources of the user. For example, when a password and user ID is shared then the other person has full access to your bank account. So, the user ID and password system are insufficient. More accurate and reliable user authentication method can be obtained by fingerprint technology. [8][2][5]

Figure 1 National ID

Biometrics is the authentication of distinctive measurable characteristics that are used onto identify people for high security. In other words, it is the use of Science and technology to measure measurable biological characteristics for automated recognition. Biometrics work on basis of pattern recognition. It is the study of pattern recognition.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203077 |

Ophthalmologist Frank Burch proposed the idea of using patterns for personal identification in 1936. Biometrics comes under complex system as studying and identifying human behavior and studying it to replace password system involves assumptions. (Cornes, 2011) Unlike, Password they are the part of us which cannot be borrowed, lost or forgotten. They are safer than passwords and cannot be hacked easily. [11]

Aims and Objectives:

The main aim of the report is as follow:

- To find the different types of biometrics.

The main objective of the report is as follow:

- Research on published books, report and journals about biometrics.
- Evaluate the advantages and disadvantages of biometrics from research paper.

II. LITERATURE REVIEW

The literature review focuses on different modes and types of biometrics and its application in real world dealing with accuracy. All the research paper used for the report are taken from reliable and legal sources like IEEE, ACM, Research gate and other online databases of research papers and journals.

According [7] to the biometrics recognition is actually pattern recognition system which works by acquiring biometric data from a person, extracting and comparing a feature set from the acquired data. The data in template set is compared with the feature set. Biometrics works on either identification mode or verification mode. In verification mode, the distinctive features are mined from biometric image to generate users live biometrics pattern. The previously stored pattern is compared with new live biometrics pattern and numeric matching score is created. Whereas in identification mode, the templates in the database of all the users is searched by the system in order to match an individual. The report compares various biometrics such as retina, iris, face, fingerprint, gait, keystroke, signature etc. The comparison table on biometrics based on the authors perspective is given below where H denotes high, L low and M medium.

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

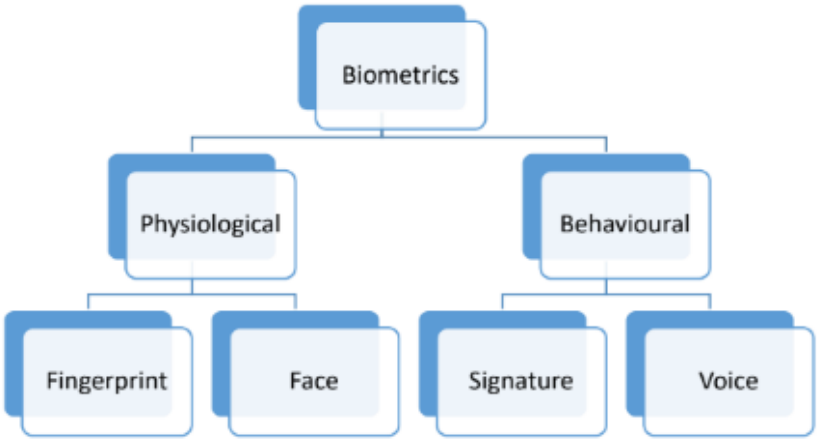
Figure 2 Biometrics based on authors perspective [7]

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203077 |

The research talks how biometrics authentication is based on behavioral and physiological characteristics of an individual. Further explaining, the physiological biometrics is the study and measurement of unique physical body parts as a means of verifying a personal identity which includes shape, hand geometry, fingerprint, iris pattern, skin pores, palm prints, hand veins, hand geometry etc. Whereas, Behavioral Biometrics is described as the analysis of the unique pattern of our behavior or character as a means of verifying personal identity which includes the signature, typing, voiceprint, how we walk, and our gestures. The author also proposed a work on iris identification through which a person in a crowd can be recognized through iris. [3]



According to the research paper Multispectral Imaging of Biometrics written by Raju Shrestha, the multispectral imaging makes biometrics more effective. The stack of images representing the intensity of an image at given wavelength which is multichannel (has more than three images) is known as multispectral image. Unlike traditional imaging which captures RGB (Red, Blue and green), multispectral imaging captures the wavelength of image in electromagnetic spectrum. The writer also provided the example of fingerprint of a dead person being used and added the data breaching in biometrics can be detected by multispectral imaging. The concept of multimodal biometrics is also introduced. Figure 4 Multiple Biometrics include uses of multiple applications to capture different biometrics. The combination of two or more types of biometrics recognition makes the system more secure and is difficult to hack. It could be combination of fingerprint verification, voice recognition or any other grouping of biometrics. The report is concluded with writer signifying multispectral imaging is more efficient, also detects spoofing and multimodal biometrics is more effective and has more accuracy than unimodal biometrics. [12]

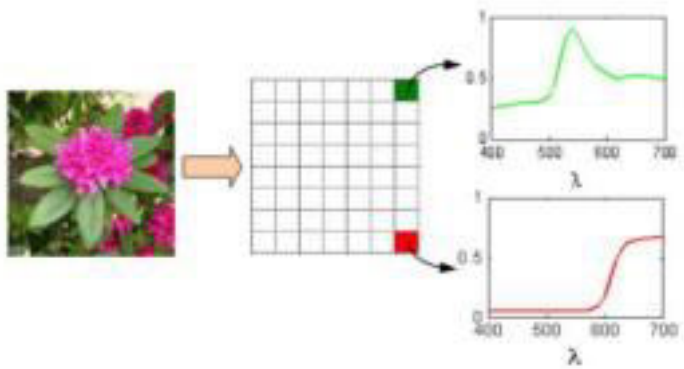


Figure 3 Illustration of varied wavelength [12]

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203077 |

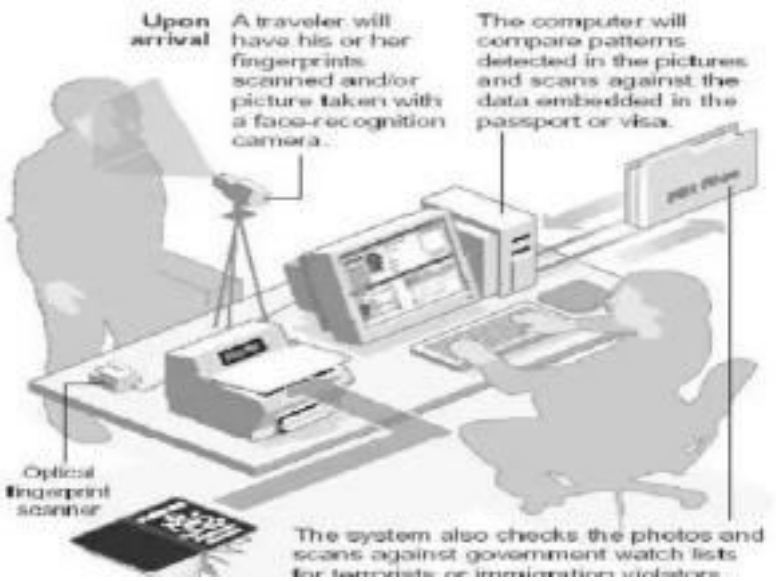


Figure 4 Multiple Biometrics

Similarly, Biometrics devices and application along with biometrics accuracy. According to Vadi, Biometrics devices are those machines which identify and authenticate the identity of the person. They have automated verification and algorithm for different devices. The security level differs from device to device and difference in algorithm. Similarly, different biometrics have different biometrics devices. To create biometrics template unique features are extracted from biometrics image. The biometrics template is stored in database or machine which is further used in verification process. The previously stored template is compared with new live biometrics template. Biometrics accuracy is the system's efficiency to separate the user from frauds. Every system has their own threshold verification value which is measured by False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR refers to the probability of false accepts allowing imposter in the system whereas FRR includes the statistical probability of rejecting the legitimate user. The writer further gave an example of mismatching fingerprint being accepted and matching being rejected which are false accepts and false rejects. If the threshold is varied to lower one error, the other automatically increases. For high security, biometrics work at low FAR than ERR (Equal Error Rate) where FRR=FAR.

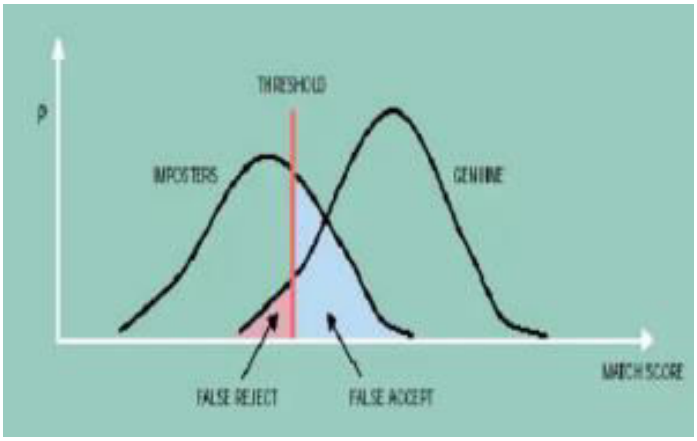


Figure 5 Error Rate[15]

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203077 |

The overviews the aspects of biometrics and discusses about its real-world application and the problem of scalability in large scale systems. The paper starts with how biometrics authentication is more reliable than traditional authentication system further describing each biometrics in detail such as face recognition which uses Euclidean distance and Bunch graph mapping algorithm. Iris recognition hamming distance matching algorithm which represents key point extraction and is the most secure. Fingerprint uses String matching algorithm. Voice recognition uses Hidden Markov model and Gaussian Mixture model algorithm. Biometrics is vulnerable to attacks which are zero-effort attack and adversary attack. Zero effort attacks talk about the possibility of two people's biometrics data to match. The author presents the example of fingerprint which may match to other user in case of a large database of fingerprints. Degrees of pattern of freedom space is minutiae configuration space. The fingerprint having n minutiae their location represented by (x, y). If C denotes the area of Tolerance and A denotes area of overlap Figure 6 then the chances of matching q minutiae in each position is computed as:

$$p_{(M,m)^n,q'} = \sum_{p=q}^{\min(m'n)} \left(\frac{\binom{m}{p}}{\binom{m}{m}} \right) \binom{p}{q} l^q (1-l)^{p-q}$$

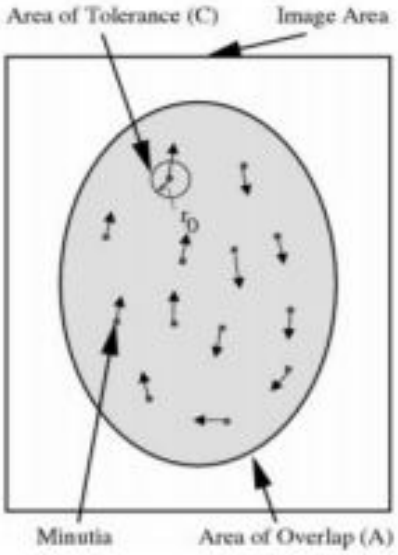


Figure 6 Illustration of area of overlap and area of tolerance[7]

The journal reviews biometrics and cyber security. The journal starts with the introduction of biometrics, it's identification and verification, error rates (FAR and FRR) then describes cyber security as the guard to internet. The writer purposes a micro strip radio wire. Using a 3-D full-wave electromagnetic programming called High Frequency Structure Simulator (HFSS). Cyberwar as web-based attacks have become an ordinary. Cloud legal science is an informative development of advanced legal science that protects against digital misconduct. The assortment and conservation of integrated data limits the unwavering accuracy of computerized evidence. The paper suggests observable engineering for Infrastructure-as-a-Service (IAAS) that uses Software-Defined Networking (SDN) and Block Chain Innovation. The paper concludes with describing cybercrime is a normal phenomenon that often occurs and to protect data using biometrics technology as it is more secure. [10]

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203077 |

The paper purposed the pros and cons of various biometrics authentication system. According to the journal, face recognition does not require direct contact with the machine and is easy to use. Hence is widely used but it cannot operate with low resolution images and state of poor lighting, shades and objects covering face. Iris Recognition has the highest security and accuracy, it also non-intrusive but the distance between object and eye should be of less than 10cm.The scanner is also expensive and lightings affects the accuracy. Fingerprint Recognition is described as easy to use and install along with high accuracy and verification. Whereas cuts, wounds, grease and dryness affect its effectiveness. Only a certain part of the finger is scanned which makes it easier for frauds. Lips identification examines lip prints which has small template. It is passive biometrics which does not require a person to be present, it can be used in a long distance. Lips biometrics is mostly affected by smile, teeth and even movement of lips which makes it difficult. Voice Biometry does not require trainings for any users and is useful for people can talk but cannot write. Its downside is that prerecorded voices are also authenticated noise and cold may affect the system. The paper compares the different biometrics and then concludes it. [9]

The research paper by explains user authentication in conventional cryptosystems to be based on secret keys and passwords which fails easily if confidentiality is not maintained and can be lost and forgotten and defines biometrics to be more secure. The paper purposes methods through which cryptographic key is binded with biometrics template and cannot be disclosed without effective biometric confirmation. The paper reviews an algorithm proposed by David on iris biometrics which introduces the theory of iris code. The paper also analyses on method proposed by Monrose which combines passwords with keystroke biometrics. The paper also reviews on key binding algorithm in fingerprint authentication. The user's fingerprint is binded with cryptographic key through the algorithm. An experiment was carried out with 450 fingerprints from database with sensor 500 dpi resolution. The vault size is calculated as:

$$r = \frac{4\rho p^2}{\pi d^2} \approx 660$$

The probability of FNMR due to vault is given as:

$$P_e \geq \sum_{i=\delta}^{t} \binom{t}{i} \exp\left(\frac{-\rho p^2}{2\pi r\sigma^2}\right)^i \left(1 - \exp\left(\frac{-\rho p^2}{2\pi r\sigma^2}\right)\right)^{(t-i)}$$

The paper is then concluded with simple biometrics key not being useful in cryptographic systems as they involve unsecured channel and input of unencrypted biometrics information. The practical existence of crypto biometrics cannot be taken as evidences based on biometrics components. [14]

III. ANALYSIS OF FINDINGS

The concept of biometrics has been found while learning pattern recognition. Biometrics security and complexity level depends on the type of biometrics such as Iris and Retina has the highest level of accuracy whereas some face recognition is forged using pictures. Many people prefer to use fingerprint, signature and voice recognition although iris and retina has higher accuracy than them. Similarly, every biometrics has its own advantages and disadvantages. There are many cases where biometrics have helped to solve many criminal and national security issues whereas there also has been cases of error and forgery in biometrics. The advantages of biometrics vary from applications for commercial positive recognition that can function either in verification or identification modes and applications for government and forensic recognition that involve identification which solves nation security and border security issues. Some advantages are High Security and User Experience, Accuracy, Untransferable and near to spoof-proof etc.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203077 |

Biometrics like iris, fingerprint recognition are nearly impossible to fake. Among billions of people there is likely a chance for someone's biometrics to match with others.

The drawbacks of biometrics are Cost, Data breach and privacy, System performance depends on speed, cost and accuracy rate which vary from system to system. It does not guarantee the same result in all devices. For example, A device X can detect face even in light and dark whereas device Y cannot. It can take false accepts allowing the imposter to access the system and sometimes make false rejects preventing the owner to access the system. Some companies which make biometric devices sell our personal information. The biometrics database still can be hacked. [11][6]

Comparison Table:

Biometrics	Accuracy	Ease of use	User acceptance	Error
Fingerprint	High	High	High	Dirt, Dryness, Perspiration, Age
Face	Medium	Medium	Medium	Age, filter, lighting
Signature	High	High	High	Changing Signature
Retina	Very High	Low	Low	Glass
Iris	Very High	Medium	Low	Lighting
Voice	High	High	High	Cold, Noise

IV. CONCLUSION

From studying the various books, journals and reports on biometrics and its advantages and disadvantages, we can conclude that biometrics is an immerging topic all over the globe which started with pattern recognition. It makes daily activities easier, faster and secure but also with it comes the concern of data breach and privacy. In conclusion, biometrics has huge impacts on issues concerning national security. It needs to improve in terms of privacy and glitches but currently it is also the growing need of the world where passwords are hacked easily.

REFERENCES

[1] Dharavath, K., Talukdar, . F. A. & Laskar, R. H., 2013. Study on biometric authentication systems, challenges and future trends: A review, Enathi: IEEE International Conference on Computational Intelligence and Computing Research.
[2] Matyas , V. & Rhia, . Z., 2011. Security of Biometric Authentication Systems. International Journal of Computer Information Systems and Industrial Management Applications, Volume 3, pp. 174-184.
[3] Sharma, . K. A., Raghuwanshi, A. & Sharma, V. K., 2015. Biometric System- A Review, Bhopal: International Journal of Computer Science and Information Technologies.
[4] Cornes, R., 2011. Biometric Measurement of Human Emotions, England: Rachel Cornes.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203077 |

[5] Dharavath, K., Talukdar, F. A. & Laskar, . R. H., 2013. Study on Biometric Authentication Systems, Challenges and Future Trends: A Review, India : IEEE International Conference on Computational Intelligence and Computing Research.
[6] Iqbal , I. & Qadir , B., 2012. Biometrics Technology, Sweden: Blekinge Institute of Technology.
[7] Jain, A. K., Ross, A. & Pankanti, S., 2006. Biometrics: A Tool for Information Security. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 1(No 2).
Jain, A. K., Ross, A. & Prabhakar, S., 2004. An Introduction to Biometric Recognition. 02 01.14(Circuits and Systems for Video Technology, IEEE Transactions).
[8] Kartik, S., 2017. Seminars Topic. [Online] Available at: https://www.seminarstopics.com/seminar/7264/biometrics-seminar-report-pdf
[Accessed 11 11 2020].
[9] Kumar, A. & Nayaki , D., 2018. Pros & Cons of Various Bio-Metric. International Journal of Scientific & Engineering Research, 9(4), p. 104.
[10] Kumar, L., Nagar, G. & Dave, D., 2019. THE STUDY OF BIOMETRICS AND CYBER SECURITY. Journal of Gujarat Research Society, 21(14), pp. 494-509.
[11] Markotwiz, J. & Gravell, W., 2007. Report of the Defense Science Board Task Force on Defense Biometrics, Washington, DC: Defense Science Board.
[12] Shrestha, R., 2011. Multispectral Imaging for Biometrics–A Review, Norway: Raju Shrestha.
[13] Sunghyuck , H., Han, J. & Kim, G., 2019. Security Issues Related to Biometric Security. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(8S2), p. 865.
[14] Uludag, U., Pankanti , S., Prabhakar, S. & Jain, A. K., 2004. Biometric Cryptosystems: Issues and Challenges. PROCEEDINGS OF THE IEEE, 92(6).
[15] Vadi, H. G. A., 2017. BIOMETRICS, RAJKOT - GUJARAT: Department of Computer Engineering ATMIYA INSTITUTE OF TECHNOLOGY AND SCIENCE.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details