INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A., Google Scholar, Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)], Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than **4767 Cities** in **180 countries/territories** are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

Sr. No.	TITLE & NAME OF THE AUTHOR (S)	Page No.
1.	**WORKERS PARTICIPATION IN MANAGEMENT** *DR. CHANDRA SEKHAR GOTLAGUNTA, G. KIRTHY, DR. KESHAMONI SRINIVAS & GURMEET KAUR*	1
2.	**KNOWLEDGE MANAGEMENT STRATEGIES FOR ACHIEVING QUALITY STANDARDS IN EDUCATIONAL INSTITUTIONS** *DR. A. V. NAGESWARA RAO*	5
3.	**COST MANAGEMENT IN SERVICE INDUSTRY** *HEMANT R. DUDHE & DR. SANJAYKUMAR M. GAIKWAD*	9
4.	**KNOWLEDGE MANAGEMENT THROUGH TRANSFORMATIONAL LEADERSHIP IN ARMED FORCES: AN IAF PERCEPTIVE** *DR. ANIL KOTHARI & DR. NIDHI PANDEY*	13
5.	**A STUDY ON RETURNS AND VOLATILITY OF FMCG AND IT SECTORS OF NIFTY** *T. PEDDANNA & S. V. SATYANARAYANA*	17
6.	**MEASURE OF OCTAPACE CULTURE ON JUNIOR LEADERS IN THE ARMY: A STATISTICAL PERSPECTIVE** *DR. ASHA NAGENDRA & BRIGADIER M SRINIVASAN*	26
7.	**DIVIDEND POLICY AND DIVIDEND THEORIES: THE WAY AHEAD** *CHAITRA K. S. & DR. B. BAKKAPPA*	30
8.	**A STUDY ON FINANCIAL PERFORMANCE OF NEW GENERATION PRIVATE SECTORS COMMERCIAL BANKS IN INDIA** *D. KALPANA & R. CHANDRASEKARAN*	34
9.	**OFFENCES AGAINST WOMEN UNDER INDIAN PENAL CODE** *DR. MADHUMITA DHAR SARKAR & BIBHABASU MISRA*	38
10.	**CUSTOMER RELATIONSHIP MANAGEMENT STRATEGY OF BHARTI AIRTEL LIMITED IN COIMBATORE CITY** *A. S. DHIVIYA, V. SUGANTHI & DR. S. KUMAR*	40
11.	**VITALITY OF COMPETENT HR PRACTICES FOR SUSTAINABLE GROWTH POTENTIALITY IN SERVICE INDUSTRY** *T. MYDHILI & B. SATYAVANI*	45
12.	**BIOMETRICS AND RFID BASED E-PASSPORT: BRINGING SECURITY TO THE WORLD** *JAPNEET KAUR & MANEET KAUR*	49
13.	**PERCEPTUAL DIFFERENCES BETWEEN THE USERS AND NON USERS OF INTERNET BANKING** *DR. DEEPA PAUL*	55
14.	**STRESS OF RETAIL SECTOR EMPLOYEES: A STUDY** *SABARI GHOSH*	59
15.	**IMPROVING ASSESSMENT IN HIGHER EDUCATION THROUGH STUDENT INVOLVEMENT** *RUCHI BAJAJ*	66
16.	**RELIABILITY ANALYSIS OF INVESTMENT BEHAVIOR OF INDIVIDUAL INVESTORS AMONG DIFFERENT RELIGIOUS GROUPS IN NCR** *SHWETA GOEL & DR. RAKESH KUMAR SRIVASTAVA*	69
17.	**A STUDY ON DISSATISFIED CONSUMERS OF SMARTPHONE OVER ONLINE PURCHASE IN MADURAI DISTRICT** *DR. R. RADHIKA DEVI & VINODH KUMAR. S.*	74
18.	**BANIYA OR LOCALBANYA: A STUDY ON INDIAN 'GROCERY AND STAPLES' BUYING BEHAVIOUR** *SWAPNA TAMHANKAR*	78
19.	**THE ENTREPRENEURSHIP'S CAPITAL ASSISTANCE IN ENHANCING THE MOTIVATION OF COLLEGE STUDENT TO BE AN ENTREPRENEUR** *MARISKHA. Z, S.E., M.M. & HANIFATI INTAN, S.E., M.M.*	83
20.	**PROBLEMS AND PROSPECTS OF HANDLOOM WEAVERS: A STUDY OF KARIMNAGAR DISTRICT** *ANKAM SREENIVAS & KANDAGATLA SRAVAN KUMAR*	89
	REQUEST FOR FEEDBACK & DISCLAIMER	97

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR

IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF .**

(e.g. Finance/Mkt./HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in one of your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the co-authors of this manuscript have seen the submitted version of the manuscript and have agreed to their inclusion of names as co-authors.

Also, if my/our manuscript is accepted, I agree to comply with the formalities as given on the website of the journal. The Journal has discretion to publish our contribution in any of its journals.

NAME OF CORRESPONDING AUTHOR	:
Designation	:
Institution/College/University with full address & Pin Code	:
Residential address with Pin Code	:
Mobile Number (s) with country ISD code	:
Is WhatsApp or Viber active on your above noted Mobile Number (Yes/No)	:
Landline Number (s) with country ISD code	:
E-mail Address	:
Alternate E-mail Address	:
Nationality	:

NOTES:

a) The whole manuscript has to be in ***ONE MS WORD FILE*** only, which will start from the covering letter, inside the manuscript. ***pdf. version is liable to be rejected without any consideration***.

b) The sender is required to mention the following in the **SUBJECT COLUMN of the mail**:

New Manuscript for Review in the area of (e.g. Finance/Marketing/HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any **specific message** w.r.t. to the manuscript.

d) The total size of the file containing the manuscript is expected to be below **1000 KB**.

e) **Abstract alone will not be considered for review** and the author is required to submit the **complete manuscript** in the first instance.

f) ***The journal gives acknowledgement w.r.t. the receipt of every email within twenty four hours*** and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending a separate mail to the journal.

g) The author (s) name or details should not appear anywhere on the body of the manuscript, except the covering letter and the cover page of the manuscript, in the manner as mentioned in the guidelines.

2. **MANUSCRIPT TITLE: The title of the paper should be **bold typed**, **centered** and **fully capitalised**.

3. **AUTHOR NAME (S) & AFFILIATIONS: Author (s) **name**, **designation**, **affiliation** (s), **address**, **mobile/landline number** (s), and **email/alternate email address** should be given underneath the title.

4. **ACKNOWLEDGMENTS: Acknowledgements can be given to reviewers, guides, funding institutions, etc., if any.

5. **ABSTRACT: Abstract should be in **fully italicized text**, ranging between **150** to **300 words**. The abstract must be informative and explain the background, aims, methods, results & conclusion in a **SINGLE PARA**. ***Abbreviations must be mentioned in full***.

6. **KEYWORDS: Abstract must be followed by a list of keywords, subject to the maximum of **five**. These should be arranged in alphabetic order separated by commas and full stop at the end. All words of the keywords, including the first one should be in small letters, except special words e.g. name of the Countries, abbreviations.

7. **JEL CODE: Provide the appropriate Journal of Economic Literature Classification System code (s). JEL codes are available at www.aeaweb.org/econlit/jelCodes.php, however, mentioning JEL Code is not mandatory.

8. **MANUSCRIPT: Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. *It should be free from any errors i.e. **grammatical, spelling** or **punctuation.** It must be thoroughly edited at your end*.

9. **HEADINGS: All the headings must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

10. **SUB-HEADINGS: All the sub-headings must be bold-faced, aligned left and fully capitalised.

11. **MAIN TEXT**:

THE MAIN TEXT SHOULD FOLLOW THE FOLLOWING SEQUENCE:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESIS (ES)

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

LIMITATIONS

SCOPE FOR FURTHER RESEARCH

REFERENCES

APPENDIX/ANNEXURE

The manuscript should preferably range from ***2000 to 5000 WORDS***.

12. **FIGURES & TABLES:** These should be simple, crystal **CLEAR**, **centered**, **separately numbered** & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. *It should be ensured that the tables/figures are referred to from the main text*.

13. **EQUATIONS/FORMULAE:** These should be consecutively numbered in parenthesis, horizontally centered with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word should be utilised. If any other equation editor is utilised, author must confirm that these equations may be viewed and edited in versions of Microsoft Office that does not have the editor.

14. **ACRONYMS:** These should not be used in the abstract. The use of acronyms is elsewhere is acceptable. Acronyms should be defined on its first use in each section: Reserve Bank of India (RBI). Acronyms should be redefined on first use in subsequent sections.

15. **REFERENCES:** The list of all references should be alphabetically arranged. ***The author (s) should mention only the actually utilised references in the preparation of manuscript*** and they are supposed to follow Harvard Style of Referencing. **Also check to make sure that everything that you are including in the reference section is duly cited in the paper**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parenthesis.
- ***Headers, footers, endnotes*** *and* ***footnotes*** *should* ***not be used*** *in the document.* However, **you can mention short notes to elucidate some specific point**, which may be placed in number orders after the references.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–23

UNPUBLISHED DISSERTATIONS

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

BIOMETRICS AND RFID BASED E-PASSPORT: BRINGING SECURITY TO THE WORLD

JAPNEET KAUR
ASST. PROFESSOR
GUJRANWALA GURU NANAK INSTITUTE OF MANAGEMENT & TECHNOLOGY
LUDHIANA

MANEET KAUR
ASST. PROFESSOR
GUJRANWALA GURU NANAK INSTITUTE OF MANAGEMENT & TECHNOLOGY
LUDHIANA

ABSTRACT

The advent of Radio-Frequency Identification (RFID) and biometrics in E- PASSPORT has brought in a harbinger of a wave for next-generation travel documents. The use of biometrics and RFID based e passport for identification makes the lives easier by ensuring the world as a safer place to live in. The biometric passport hinders travelers from taking an illegal entry into any country, limiting the use of counterfeit documents by more precise identification of an individual. This paper analyses the various cryptographic features as face, fingerprint, palm print and iris used as effective security measures in e-passports. Palm print is more secured as compared to finger print since it has more features such as wrinkles, principle lines, texture etc. RIFD and Biometric based e-Passport assures confidentiality, authenticity and consistency as compared to other technologies but still are not fully protected. This paper provides impending issues regarding security and effectiveness that are still unaddressed such as Eavesdropping, Clandestine Scanning &Tracking, Cloning ,Cryptographic Weaknesses and Skimming etc.

KEYWORDS
biometrics, clandestine scanning, eaves dropping, e-passport, skimming.

1. INTRODUCTION

A Biometric & RFID based digital passport represents a major shift in technology that can be used to authenticate the citizenship of travelers A biometric based e-passport can be recognized by the logo.

FIGURE 1.1: A BIOMETRIC BASED PASSPORT

The RFID contain a microchip and radio frequency identification (RFID) antenna which stores a digitized image of the passport holder as well as the relevant biographical details such as name, date of birth, digital photograph of the holder and others biographic information printed on the passport. The critical information related to passport is printed both on the data page of the smart passport as well as stored in the chip. This chip is contactless which allowing secret information to be read without connecting wires. After assessment of various biometrics, the current effective security measures used for identification in e-passports are fingerprint, facial, iris and palm print recognition.

2. REVIEW OF LITERATURE

- Kolahan and Thapaliya (2011) discussed that E-passports contain entirely the private information, so it is essential to protect the data. For that Authenticity, confidentiality and data integrity are the some of the most crucial factors and are maintained by using cryptography.
- Kumar et al (2012) suggested that biometric passport though increased the robustness against identity theft but additional security measures are still needed.
- Bhatia (2013) focused on biometric system which determines the authentication by using the different biological features i.e. Fingerprint, retina-scan, iris scan, hand geometry, and face recognition which are physiological biometrics but it is essential to locate factors that reduce and affect system performance such as in fingerprint Dry/oily finger and in Iris-scan due to too much movement of head or eye etc.

3. OBJECTIVES

1. To Analyse the various cryptographic features used as effective security measures in e-passports.
2. To Determine various issues regarding security and effectiveness.

4. TECHNICAL BACKGROUND

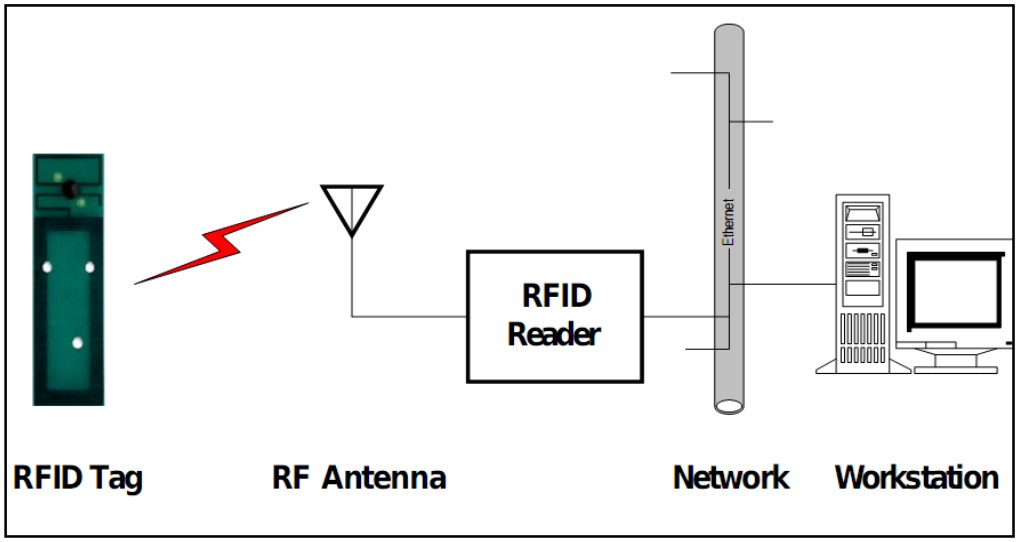
4.1 RFID TECHNOLOGY

The governments of the world are currently changing and reforming their immigration and migration laws and regulations. The conventional methods of paper-only passports and visas have become too easy to forge, allowing criminals to travel between countries, and to reside and work in them illegally. So, to tackle one

of the methods being implemented in most countries at this time is the use of Radio Frequency Identification (RFID) memory chips embedded in passports. A RFID chip is a very small contactless microchip, just like a memory chip or memory which are smaller than a grain of rice. The chip communicates with the reader/scanner through an RFID antenna that is embedded in the cover page of the passport. It is an automatic identification wireless technology i.e. radio frequency waves to transfer data between the reader and a movable item to identify, categorize and track. The characteristics of RFID are: It Uniquely identify an individual item.

- Identify items without direct line-of-sight
- Identify many items (up to 1,000s) simultaneously
- Identify items within a vicinity of between a few centimeters to several meters

FIGURE 1.2



Systems that make use of RFID technology are composed of three key elements:

4.1.1 **RFID TAG**: An RFID tag uses a silicon microchip to store a unique serial number and it is read-only (RO), write-once, read-many (WORM), or read-write (RW the chip may be read. Attached to the chip is the antenna, whose purpose is to absorb radio-frequency (RF) waves from the reader's signal to send and receive data. A RFID tag can be attached to anything that includes items, goods, vehicles, assets, livestock etc.

There are basically two types of RFID Tag's

- **PASSIVE RFID: TAGS**: Passive tags consist of three elements: an integrated circuit or chip, an antenna, and a substrate. The passive tags wait for an interrogating signal from an RFID reader and once the tag comes in range of the interrogation zone, the RFID tag's antenna draws energy from the electromagnetic waves. The tag's microchip once it becomes powered, it transmits a signal. The change in the electromagnetic wave is detected by the reader's antenna which interprets the information. For the proper processing of work, the antennas in both the tag and reader must be at least within several meters of each other; however, the read range depends on the transmit frequency, equipment settings, and other environmental factors. The major performance factors include the antenna's size and antenna shape. The larger the size of antenna, the more energy it can collect and then send back out. Larger antennas have higher read ranges but not as high as active tags. In Antenna shapes, the Low- and high-frequency antennas are usually coils because these frequencies are predominantly magnetic in nature. On the other hand Ultrahigh-frequency (UHF) antennas, look similar to old-fashioned TV antennas because ultrahigh frequencies are solely electric in nature.

The **PASSIVE RFID TAGS** operate at three distinct frequencies:

a) Low Frequency (LF) -125 -134 kHz
b) High Frequency (HF) -13.56 MHz
c) Ultra High Frequency (UHF) -856 MHz to 960 MHz's

As frequency increases, the radio wave's ability to penetrate liquids and metals decreases, and, generally, read range increases as frequency increases. With advancements in technology the UHF RFID tags can operate around water and on-metal surfaces with minimal interference. Substrate, the third component of the passive RFID Tag consists of Mylar or plastic film. The antenna and the chip both are attached to the substrate that holds all of the tag's pieces together. The passive RFID tag does not include an onboard source of power instead it receives its power from the energizing electromagnetic field of an RFID reader (or interrogator). The energy coupled from the electromagnetic field undergoes rectification and voltage multiplication in order allows to be used to power the passive tag's microelectronics. Passive tags are smaller and inexpensive.

- **ACTIVE RFID TAGS**: Active RFID tag's consists of two major Components a microchip and an antenna. The chips in RFID tags as compared to chips in passive tags are larger in size and have greater capabilities. They have onboard built-in power supply (long life battery) allows the tag to transmit data to a reader on its own, without the need to draw power from the reader itself like passive tags do. Active tags can be read from distances of 100 feet or more, whereas passive tags can only be read from up to about 20 feet. Whether we use active or passive tags in our RFID system depend primarily on two factors the application and our budget. The barcode technology will soon become obsolete as RFID proliferates through organizations, making them more efficient, reliable and well equipped for accuracy.

FIG. 1.3: A COMPARISON OF ACTIVE VS. PASSIVE RFID TAG

	Active RFID	Passive RFID
Tag Power Source	Internal to tag	Energy transferred from the reader via RF
Tag Battery	Yes	No
Availability of Tag Power	Continuous	Only within field of reader
Required Signal Strength from Reader to Tag	Very Low	Very High (must power the tag)
Available Signal Strength from Tag to Reader	High	Very Low

	Active RFID	Passive RFID
Communication Range	Long range (100m or more)	Short or very short range (3m or less)
Sensor Capability	Ability to continuously monitor and record sensor input; data/time stamp for sensor events	Ability to read and transfer sensor values only when tag is powered by reader; no date/time stamp
Data Storage	Large read/write data storage (128KB) with sophisticated data search and access capabilities available	Small read/write data storage (e.g. 128 bytes)

4.1.2. An RFID tag reader, or transceiver, that reads and writes tag data.
4.1.3. A back-end database, that stores records associated with tag contents.

4.2 THE RFID MECHANISM OF THE E-PASSPORT

Each tag contains a unique identity code. An RFID reader emits a low-level radio frequency magnetic field that energises the tag. The tag responds to the reader's query and announces its presence via radio waves, transmitting its unique identification data. This data is decoded by the reader and passed to the local application system via middleware. The middleware acts as an interface between the reader and the RFID application system. The system will then search and match the identity code with the information stored in the host database or backend system. In this way, accessibility or authorization for further processing can be granted or refused, depending on results received by the reader and processed by the database. Although RFID chips used in e-passport promises protection they still have lots of technical flaws are they are vulnerable to skimming and eavesdropping.

4.3 BIOMETRICS IN BRIEF

The airline industry sector is considered as one of the most globally threatened, and that is why new methods and tools are constantly sought in order to enhance security. These methods contain the latest technology, including contactless smart cards (RFID), with encrypted biometric information. Biometrics refers to measurable biological or behavioral aspects of a person and can be used for automated recognition. They are powerful identifiers since the are unique and it is not possible to be shared or duplicated. Biometrics can be used either as for identification or for authentication/verification. In case of identification, a computer system compares a person's biometric characteristic eg fingerprint, with all biometric samples stored in database. If it matches with one of them then person is identified. This type of match is called one-to-many match. In case of authentication, the person is scanned and is compared with one to a previously stored sample. This type of match is called one-to-one match in contrast to identification process which is one-to-many. Biometrics-based technologies include identification based on physiological characteristics complying with ICAO standards that consists of a mandatory facial images, fingerprints, hand geometry,palm, retina, irises etc.

4.3.1 PHYSICAL BIOMETRIC TECHNIQUES

A) FINGERPRINT IDENTIFICATION

Fingerprints is one of the reliable measures of biometrics used to identify an individual and verify their identity. Fingerprints are made of a series of ridges and furrows on the surface of the finger and have a core around which patterns like swirls, loops, whorls, or arches are curved to ensure that each print is unique. An arch is a unique pattern in which the ridges enter from one side of the finger and then rise in the center forming an arc, and finally exit the other side of the finger The loop on the other side is a pattern where the ridges enter from one side of a finger, and then form a curve, and tend to exit from the same side they enter in. In the whorl the ridges form a circularly pattern around a central point on the finger. It has been proven that fingerprints of even monozygotic twins are different. That means the identities of twins can be distinguished by simply matching the corresponding fingerprint with its stored digital representation. With digital scanning, a one presses their finger against a small optical surface where fingerprint information is taken from the digital scan and sent it to a database for both verification and identification comparison. The future of fingerprinting is very bright, as you will continue to see widespread usage at ATMs for withdrawing and depositing money and at grocery stores for fingerprint scan checkout and billing to a registered user's credit card or debit account are some of examples of how fingerprint will be used.

B) HAND GEOMETRY

The hand geometry is a biometric technique which reads a person's hand and/or fingers for access. Hand geometry is just like fingerprinting, which is generally completed in 5 second process. It offers many advantages such as ease of use, small data collection, resistant to attempt to fool a system, difficult technology to emulate a fake hand, and provides for the elimination of buddy punching in workforce management solutions.

There are however several challenges to the technology.

- The first challenge is high proprietary hardware costs and size, the aging of the hands and fingers of individuals poses a challenge.
- The inability of the machines to cater hands with injuries is a second challenge; the inaccuracy of the technology s a third challenge,
- The final challenge deals with the biometrics inability to recognize a fake hand. The future of hand scanning appears to be static. From a cost standpoint, it is quiet expensive than fingerprint technology and just as effective.

C) FACIAL RECOGNITION: Facial recognition analyze the several characteristics of a person's face . The process works as follows: The person faces a digital video camera, usually standing about two feet from it, where the overall facial structure, including distances between eyes, width of the nose, mouth, and jaw edges are measured. These measurements are saved in a database and used for comparison in future when a user stands before the camera again. The several advantages of facial recognition are easy integration into existing access control or time and attendance systems; verification and/or identification being accomplished in a short span time period. Face recognition system is a system, which turns your face to computer code so that it can be compared with thousands of faces• In order for face recognition system to work it has to know what a basic face looks like. Face recognition system is based on ability to first recognize faces and then measure the various features of each face. If you look into mirror you can see that your face has certain distinguishable landmarks sometimes called as nodal points. There

are about 80 nodal points on human face like 1. Distance between eyes 2. Width of nose 3. Depth of eye sockets 4. Cheek bones 5. Jaw line 6. Chin etc. These nodal points are used to create numerical code, a string of numbers that represents the face in database (called face print). Only 14-22 nodal points are needed to complete the recognition process. The parameters measured are translated into digital codes called the fingerprint and face print which is used to represent the face in the database.

- **Face Recognition Types: There** are two types of Face recognition -**2D System and 3-D system.**

a) The Basic facial recognition used two dimension (2D) paradigm picture to compare it with the image sorted in the data base, but these programs did not succeed only if the person is looking just to the camera. So anyone who is suspect will be warned that he/she will see a camera in place, and here lies the problem where this fails by depending on the 2D system. Besides, the additional changes in the environment surrounding the person, such as light will produce images the computer cannot have in the corresponding memory, also the changes in the same person due to age, accidents, surgeries etc can cause a system failure in face recognition.

b) 3D System for face recognition is based on the concept where the special cameras will capture images of three-dimensional views of the suspected person, and using the special main features of each face that generally does not changed significantly with time, such as eye hole, the basic distance between the eyes, width and shape of the nose etc. These features are the strongest source of information as these measurements are not subject to lighting or surrounding environmental, for example: These 3d system does not suffer from lighting conditions even if the place was dark and even if the person is not in the face of camera.

D) IRIS SCAN: Iris recognition is one of the richest source of biometric data since it is a protected organ whose random texture is stable throughout the life and hence can be used as an identity document offering high degree of identity assurance. It is based on the distinct colored ring surrounding the eye of biometric identification that uses mathematical pattern-recognition techniques on video images of the irises of an individual's eyes. It involves a user, which stands around 2 feet away, looking into a device where their iris is scanned and compared. The comparison is conducted at more than 200 points and checked for similar rings, furrows and freckles of the eye.

The main advantage of iris scanning involves the extreme accuracy of the technology. Since Irises is unique of every individual and not only differ between identical twins, but also between the left and right eye. It involves non-invasive technology; an ease of use since irises can never be stolen, unlike keys, access cards, and password systems.

The main challenges of Iris are:

- It involves its high cost
- The bad readings due to poor lighting, surface positioning if behind a curved, wet, or reflecting surface;
- The possibility of obscured irises due to eyelashes or drooping eyelids.

The future of iris scanning seems to be very bright as the ease of use and accuracy of the technology will open the new windows for iris scanning in correction facilities, county jails, airports, banks, colleges and police stations around the country. It is also possible that in the near future everyday people will use iris scanner a daily basis for entering the office and logging onto corporate networks.

E) RETINAL SCANNING

Retinal scanning devices are one of the most accurate physical biometric since there is no known other way to replicate a retina. Similar to iris scanning, it simply scans the layer of blood vessels at the back of the eye. It involves using a low-intensity light source and an optical coupler that reads the patterns of a person's retina. A new and primarily new technology that is used for high-risk security areas. In Retinal scanning the user looks through a small opening in the device that has a small green light. The user must keep their head still and eye focused on the light for several seconds during which time the device will verify the user identity. This process takes around 10 to 15 seconds only.

Besides being the most accurate biometric technique available, retinal scanning provides for several additional advantages.

The main advantages are the capability of providing viewing assistance to those who are visually impaired; Providing greater degree of accuracy, and the technology being seen as a great long term cost alternative to some other biometric techniques.

The several challenges are:

- They include the invasive screening process and user discomfort. Such as it requires a user to stand within inches of a device to get an accurate reading.
- It requires a user to remove glasses and requires a user to place their eye close to the retinal scanning device.
- It requires a user to focus on a certain point for a specific period of time.

The future of retinal scanning seems to be bright. However, it needs to be more refined, non-intrusive, and cost effective for acceptance.

F) PALM PRINT

Palm print is inner part of an individual's hand. Since many years the palm line patterns have been used for predicting the person's future. Palm print is also one of the reliable modality since it has unique features as principal lines, orientation, singular points etc. The other features of palm are geometric features, delta point's features, ridges and creases. Principal lines are namely heart line, head line and life line. Palm print contains three principal lines which divides palm into three regions: Interdigital, Hypothenar and Thenar. An Interdigital region of the palm lies above the Heart line. The Thenar lies below the Life line. And Hypothenar is between Heart and Life line. From palm print principal lines, minutiae, ridges features can be extracted for identification.

Advantages of palm print

- It is is hardly affected by persons age.
- It contains more reliable information and can use low resolution devices.
- It is a rapidly developed method of biometrics.
- Face Identification

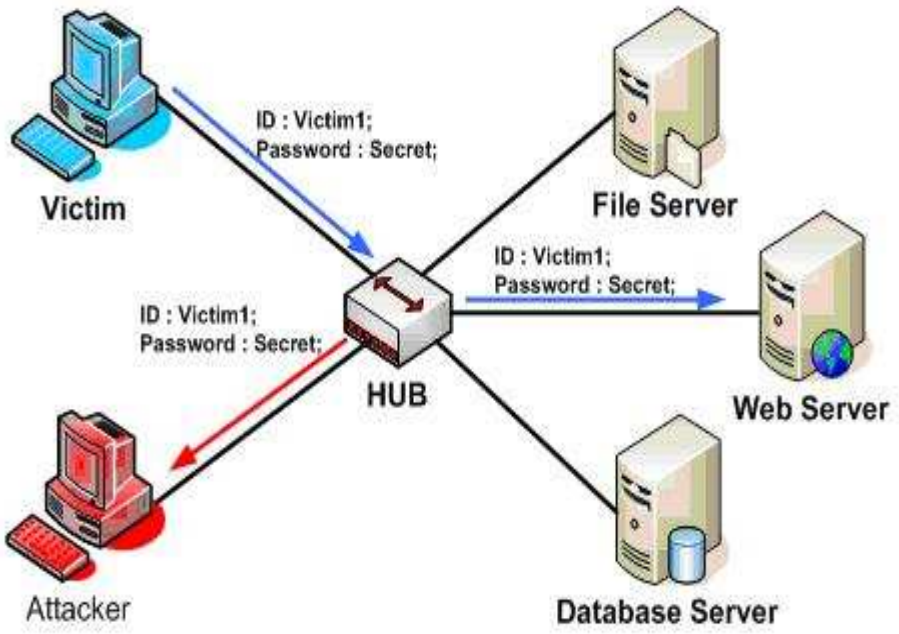
5. PRIVACY AND SECURITY ISSUES

With the development of RIFD system, Security in e-passport system has become a critical issue. Contactless and RFID chips were used without connecting wires which is vulnerable to be exposed at a distance. There is a greater chances of attacks in communication network, chip or at backend system. E-passport guarantees confidentiality and authenticity of information based on some cryptographic tools. As compared to others, biometric system provides better aspect for user authentication but it is not fully protected. In current years, some drawbacks are evolving related to data privacy issues. There is a possibility of several attacks at hardware and software levels like Eavesdropping, Reverse Engineering, Clandestine Scanning and Tracking, Cloning, Biometric Data-Leakage, Cryptographic Weaknesses and Skimming.

5.1 EAVESDROPPING

Eavesdropping refers to the unauthorized monitoring of a private communication, such as a phone call, emails, messages, videoconference, fax transmission and other internet services. The majority of network communications occur in an unsecured format, which allows an attacker to secretly listens the communication link and intercepts the information by using unauthorized device during the communication between chip and legitimate reader. This kind of attack is hard to acknowledge because there is no emission of powered signals. It has been observed that up to at least of two meters of area attacker can eavesdrop on the communication network of RFID cards and when an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor and interpret ate the network is generally the biggest security problem that an administrators face in an organization. Without strong encryption services that are based on cryptography, your important data can be stolen by others through the network.

FIGURE 1.4: EAVESDOPPING



5.2 REVERSE ENGINEERING

Reverse engineering is also called as back engineering. It is the process of extracting design information from man-made and re-producing anything based on the extracted information. Biometric chip uses a unique id as a private key that is hardcoded in chip manufacturing process so are very difficult to reverse engineer but if the attacker has the technical knowledge than they can reverse engineer and has access to equipment which is not rarely found in commercial market. Potential reverse engineering of biometric template is an important issues need to be addressed that could lead to a reconstruction of the images of physical characteristics. Although it is considered to be impossible but research is carrying on to reduce the set of potentially matching images of the physical characteristic using the template.

5.3 CLANDESTINE SCANNING AND TRACKING

Clandestine scanning is an unauthorized way of reading the electronic data of an identity card without the consent of the card holder. Private information like as address, name, date, marital status, date of birth, and nationality can be leakage easily by anyone. Clandestine tracking has an ability to track an individual and it can easily reveal the location of the person. Tracking is possible if the data on the chip cannot be read. We also show that the ICAO Active Authentication feature enables tracking when used with RSA or Rabin-Williams signatures. Clandestine tracking is more harmful as compared to clandestine scanning because the attacker can keep track record of an individual globally.

5.4 CLONING

Cloning attack is one of the attack pattern of acquiring the data from an authorized identity card where typically the attacker makes the fake accounts of the real users by thieving and copying their profiles, and sends friend requests to the friends and relatives of the cloned victim and it is difficult for an individual to detect these fake identities due to the same identical names and profile information of the user and making an unauthorized copy of the captured sample in a new chip and also for cloning threats, the active authentication is used as the counter measure but it can be bypassed by amending the EF.COM file of the passport chip.

5.5 BIOMETRIC DATA-LEAKAGE

Biometric data are constant and replacement is actually impossible if the biometric data are compromised. Just because of this features, it is used in e-passports to enhance privacy and security concerns. Data-hiding is one of the technique used for security of the data. In order to protect biometric data from misuse and attacks, the approaches which were widely used is watermarking-based multimodal biometric. In this, iris template is watermarked in the face image which makes the face image visible for verification and the watermarked iris for cross-authentication and biometric data security. Existing and proposed deployments of e-passports will always facilitate automation, and perhaps, a weakening of human oversight. This helps in making secrecy of biometric data.

5.6 SKIMMING

A skimming is the act of obtaining encoded data without the consent of individual by using electronic storage device. The data from e-passport can be retrieved by beaming power at the passport at most a few feet and also the Digital signatures required on e-passport data by ICAO regulations. such signatures allow the reader to verify that the secret data came from the correct passport-issuing authority.Digital signatures do not bind the important data to a passport or chip, so there is no defense against passport cloning.

6. SCOPE FOR FUTURE RESULTS

Future E-passport incorporate more biometric features into one device to ensure the quality of an automatic processing of personal identities to build more secure biometric passports. Proposed features for a future use are primarily based on an iris recognition (use of the iris recognition has been already prepared in current passports, however the real application is still not common), veins of fingers recognition, body shape recognition, analysis of other electrical and magnetic fields, created by man's body or of its reactions to such fields, analysis of face and head vibrations during speaking. and combinations of these features with time-proven fingerprints. Moreover, scanning of veins of a finger during a fingerprint scanning process should also provide liveness detection at the same time—that is a very important aspect in a fake fingerprint detection

7. CONCLUSIONS

The work represents an account for the presence on e-passport using unique biometrics recognition towards their improved identification. The application of various cryptographic features such as facial, fingerprint, palm print and iris recognition in passports highly requires accuracy rates; secure data storage, and reliable generation of biometric data. An RFID chip will be embedded into the passport from which Border guards will be able to compare the face of the person standing in front of them with the image of the individual stored into the RFID chip. This image must match with the image printed into the passport page. Biometric are one of the promising identification measures because absolute identification could eliminate mismatched computer records and stolen identities. The state of differences in privacy laws between different countries is a huge barrier for global implementation of biometric passports. The use of biometrics in e-passport protects the data from being stolen. The inclusion of biometric identification information into machine readable passports though increased robustness against identity theft if additional security measures are implemented so that the limitations of the biometric technologies are compensated.

REFERENCES

1. Ahsan K, Shah S and Kingston P, "RIFD Application: An introductory and exploratory study", International Journal of computer science issues, Vol 7, Issue1, No3,ISSN-1694-0814,2010,PP 1-7.
2. Castro L, Wamba S F," An Inside look at RFID technology", Journal of technology management and Innovation, Vol 2, Issue1, ISSN:0718-2724, 2007.
3. E-passport overview, White paper TrustedID_e-passport_2015
4. Gaba G S, Gupta N, Sharma G, Gill H," Intelligent cars using RIFD Technology, International Journal of science and engineering Research, Vol 3,Issue 7, 2012,ISSN 2229-5518
5. Juels A," RIFD security and privacy: A research survey" IEEE journal on selected areas in communication, Vol 24, No.2,2006,pp1-14
6. Kumar P, Agarwal M, Nagar S," A survey on Face recognition system – A challenge," International Journal of Advanced Research in computer and communication Engineering, Vol2,Issue 2, 2013, PP2167-2171.
7. Kumar V.k, Srinivasan B, Narendran P, "Efficient implementation of electronic passport scheme using cryptographic security along with Multiple Biometrics,2012,PP 18-24.
8. Kumar V.K, Srinivasan B," Design and development of E-passport using Biometric access control system, International journal of advanced smart sensor network system, Vol 2, No.3, 2012, PP 51-62.
9. Laurie, A.: RFIDIOt (May 2007), http://www.rfidiot.org/
10. Lyer S," RFID: Technology and Applications" www.it.iitb.ac.in/~sri, RFID 2005
11. Nambiar A N, "RIFD technology:- A Review of its Application," world congress on engineering and computer science, Vol11,2009, pp 1-7.
12. Robroch, H.: ePassport Privacy Attack (2006), http://www.riscure.com
13. S Arora, "National eID card schemes – a European overview", Information Security Technical Report, vol 13, issue 2, May 2008, pp.46-53.
14. Sandhu M, Kaur M, Mohan N, Sandhu P,"RIFD technology Principles, Advantages, Limitation and its applications", International Journal of computer and electrical Engineering, Vol.3,No.1,ISSN 1793-8163,2011.
15. Vakalis I, "Privacy and Biometric Passports", The Scientific World Journal, ISSN 1537-744X, 2011, pp 478–489.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue, as well as on the journal as a whole, on our e-mail **infoijrcm@gmail.com** for further improvements in the interest of research.

If you have any queries, please feel free to contact us on our e-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward to an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, neither its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal are exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals