**TDDC03 Information Security, Project**
Spring 2006


# Biometric Authentication in Newspapers and Magazines

A.K.M. Hassan Zikrul Haque Bhuiyan
(Program: Computer Science)

Naga Krishna
(Communication & Interactivity)
**Supervisor: Niclas Wadströmer**

# Biometric Authentication in Newspapers and Magazines

**First Author**
A.K.M. Hassan Zikrul Haque Bhuiyan
Program: Computer Science
Troskaregatan 57.23
Lambohov, Linkoping
Email: hasbh671@student.liu.se
Phone:0736975158

**Second Author**
**Naga Krishna**
Communication & Interactivity
nagpa505@student.liu.se
Ryds Alle 21, 106
Ryd, Linkoping
Phone: 0768301538

**ABSTRACT**

*Biometric authentication is a technology, mainly used to identify person. It is kind of buzzword. Day by day it is getting more and more popular. Newspapers and magazines around the world are publishing different reports on biometric authentication such as "biometric passport for identification", "biometric in security checking" and "privacy issues with biometric" etc. This type of report is published based on some motivation and wants to convey some kind of messages to the readers. To full fill the course completion requirement of "Information Security", we have written this paper and tried to find different questions answers, such as what kind of impression is created? Are they presented in right way or flawed way? The purpose of the article is served or not? Will it scare the readers? Several other relevant questions answers tried to find out.*

**INTRODUCTION**

The world is becoming more and more dependent on science and technology. Among different machines and devices, computer became an integral part of our daily life. They are used everywhere starting from home to office to business. Security is a major concern in these systems because the lack of security may cause bearable damage to catastrophic one. The goal of computer security combines mainly three primary properties called confidentiality, integrity and availability. User authentication process is one of the ways to achieve confidentiality. User authentication process ensures the right person to be given access to the machine. An authorised user can be identified by password, PIN number, magnetic card, smart card or biometric authentication options. Biometric authentication is getting more popularity due to their diverse application areas. There are many reports and articles coming on biometric authenticity in newspapers and magazines. Some of the reports are on technological review and some of them about recommendation to introduce biometric authentication in different sectors. Some of the reports are kind of analysis on governmental proposal to introduce biometric authentication and some of them written for novice readers.

**BACKGROUND**

This paper is written to fulfil the passing requirement of "Information Security" course. At the very beginning we starting the topic with almost similar title but the study domain were literatures rather than newspaper and magazine. Due to time consuming search in literatures and unavailability of resources, we shifted to the articles on newspaper and finally we decided to study both newspapers and magazines.

Biometric authentication is very common in action movies especially in Hollywood movies but it is not very much common in the literatures. It is possible to find biometric authentication in literatures but due to shortage of time and resources unavailability obviously it was taking long time to find the resources. Not only searching resource but also reading them and finding the particular chapters deal with biometric authentication would have taken long time. Then we decided to select, newspaper as source of this paper writing. But later we found that apart from newspaper there are good numbers of magazines covering good number of reports on biometric authentication too.

So finally we decided to have articles both from newspaper and magazines. Most of the magazines are business and computer related.

**DEFINING SCOPE**

To limit the scope of this paper, we have decided to select a few reports and articles on biometric authentication from different newspaper and magazines around the world. We read them and tried to analyze them based upon some predefined questions. The analysis was done based on the following questions such as:

What about the report? Who are the readers? What knowledge do they have? Why would they read the article on biometric authentications? What do they expect to learn?
What kind of impression is created? Is the report presented in right way or flawed way? Is it written to scare the readers? Does it show that biometric authentication is very expensive and complex?
We will also consider the purpose of the writer and publisher of the biometric authentication articles. Why are they writing about biometric authentications? What do they want to achieve?

## METHOD

First of all, we have selected several reports on biometric authentication from different newspaper and magazine's internet edition. From there, we tried to select a few very good reports. We gave priority to the renowned site's report. Then we looked into the detail of these few selected reports and then analyzed them. The analysis had been derived by the scope of this paper which is written in the scope paragraph of this paper. By using the scientific knowledge and issues related to the biometric authentication technology, we tried to analyse the different questions on biometric authentication and made summary report of that analysis. The analysis of the report might find whether the report is presented in flawed way or not? We also analysed how the whole situation could be presented in a better way to the readers.

## WHAT IS BIOMETRIC AUTHENTICATION?

Now the current phenomenon is to use the biometric authentication systems in different areas like passport, network, and security systems. Biometric authentication is one of advance identification technology which uses an individual's unique biological traits like include fingers, hands, feet, faces, eyes, ears, teeth, veins, voices, signatures, typing styles, gaits and odors characteristics to determine one's identity. The biometric authentication system can be regarded as a pattern recognition system, including all the hardware and software and interconnecting infrastructure, enables identification by matching a live sample to a stored pattern in a database.

## BIOMETRIC AUTHENTICATION HISTORY

The word biometric itself comes from the Greek words "bio" and "metric" which means "life measurement." It is been included biometric as a field of statistical development since twentieth century. But if we try to look through the history of biometric then we find it goes long back. Here we classify them according to chronologically.

**Egyptian Era:** Though the general perception about this technology is very recent one but in reality the history of the principles behind this technology takes long back to the great Egyptian era. The great pyramids architects in Egypt who used to identify their thousands of workers using not only by name but through also their physical size, face shape, complexion and other noticeable features, such as scars [4]. The Egyptians were really ahead of their time because after that we do not see using of biometric authentication for the next thousands of years.

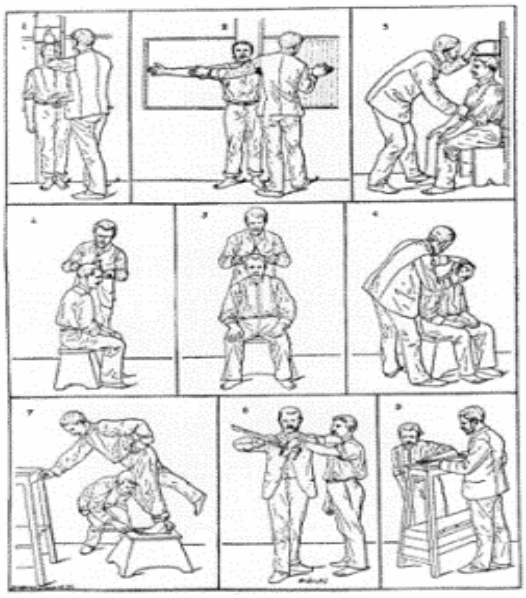

Figure 1: Shows measures of different traits are recorded in old days. Source: www.galwayeducationcentre.ie[4]

**The Chinese:** We find the biometric authentication had been used by the Chinese merchants in 14th century. The referenced is reported by explorer Joao De Barros [4] [5]. The Chinese used the finger print in China by stamping children's palm prints and foot prints on paper with ink to distinguish the young children from each other.

**European History:**. After hundreds of year gap of the Chinese use of biometric authentication, in late 1800s, we find the Europeans started using finger print and other bodily characteristics to identify the criminals. In 1880 a police desk clerk working in Paris named Alphonse Bertillon used to fix the problem of identifying criminals and introduced biometric authentication [6][7].

The process was known as Bertillonage and it was used widely throughout the world up until when it is revealed that some people shared the same measurements. After that the police started using finger printing, developed by Richard Edward Henry of Scotland Yard.

**Modern Days:** People are more concern about the privacy issues. At the same time every other day there is a new technological advancement which triggers the falling price of hardware. Hence no such standardization could be made so far on security concern and hence the laws of different country continue to be drafted. Not like previously only the finger print but in modern day's retina, iris pattern and facial characteristics also considered for pattern matching.

## HOW DOES THE MODERN BIOMETRIC AUTHENTICATION SYSTEM WORK?

As it is mentioned today there are different kind of biometric authentication systems are in used such as fingerprint, iris, voice, face and palm. Normally it sound that the biometric systems complex and high-tech and difficult to understand. But they all use the following common three steps such as enrollment, storage and comparison [15].

**Enrollment**: Like other authentication system biometric authentication system also asks about the name or an identification number for the first time to be recorded. After that it captures one or more samples of specific trait.

**Storage**: Then the system does analyze trait and translate it into a code or graph. Some systems also record this data onto a smart card that we carry with us. In fact it never stores the image as normally we believe.

**Comparison**: When we go to use the biometric authentication system then it compares the trait with the information on file. Based on the checking result it either accepts or rejects the person.

To implement the above following three common steps into the system in total three components are used followed by a sensor, computer and software. The **sensor** used to detects the characteristic being used for identification. Then the **computer** used to read and stores the information and the **Software** used to analyze the characteristic, translates it into a graph or code and performs the actual comparisons.


Figure 2: IBM ThinkPad T43 with built in finger print scanner.

Biometric is gaining more and more popularity in modern days even we find it in different daily used devices such as IBM ThinkPad T43 laptop which has a build in fingerprint biometric authentication system.

## BIOMETRIC AUTHENTICATION IN NEWSPAPER AND MAGAZINE

Here we explain the selected biometric authentication related reports one by one.

**a)** **"Your eyes will see you in"** by Priyanka Joshi / New Delhi April 19, 2006 in **Business Standard** [1]. The report focuses on different features of the biometric authentication. It referred to many comments on biometric authentication, made by different personalities. Among several comments reporter himself made a comment in which he said that biometric authentication used in several action films (like James Bond) and argued the types of tricks showed in the movies are possible in real life or not? It referred to the movie tricks in James Bond movies and asked whether the similar kind of tricks can be done or not? The report focuses on different point such as the uniqueness of biometric authentication, cost of different kind of biometric authentication systems, which is better and reliable than other biometric authentication system, risk factor of using this system and so on. The report showed some statistics about the cost of implementation of biometric authentication technology and the importance of biometric authentication. The report claims that the biometric authentication industry is growing

very fast and biometric market will be $205 billion by 2006 [1].

Business Standard is a leading business news magazine and target readers are those who are normally interested in business and economics [12]. Publisher has created some kind of awareness among its readers community on the latest security measure trend by focusing on different issues of biometric authentication and also by putting different comments about it. They also tried to focus on how it could be implementing in the Indian perspective where cost is one of the major concern to implement any latest technology

In the analysis part, we comment on some of the remarks made in the report.

The reporter asked whether the biometric authentication can be broken or not; like James Bond did in movies? Yes, several action movie such as Dracula (released in 2000), Minority Report (released in 2002) and similar type action movies show the breaking of biometric authentication system. In reality breaking the biometric security measures depend on what kind of biometric authentication system is used whether is it voice or finger or palm or iris or facial biometric? In fact no authentication system in the world is 100% spoof proof. Like other authentication systems biometric authentication systems also have some potential threats and can be faked [14]. For example the threat would be any or all of the following such as [13]

- The communication channels between the sensor and the rest of the system.
- "Attacking specific software modules (e.g. replacing the feature extractor or the matcher with a Trojan horse)."
- Attacking the database of templates.
- "Presenting fake fingers to the sensor."

According to some researcher, they showed that last two types of attacks are possible to spoof the fingerprint recognition systems. The attack can be made to fake the system by making fake finger print with collaboration of the original owner or from a latent fingerprint or by cutting off the finger from the owner. Making latent fingerprint is really difficult but it is not impossible. Fooling various sensors with fake finger is possible. Gelatine fingers works better, because gelatine behaves, electrically, quite like real flesh; sensors that care about conductivity, which capacitive sensors do, aren't terribly likely to be faked out by a silicone finger [14].

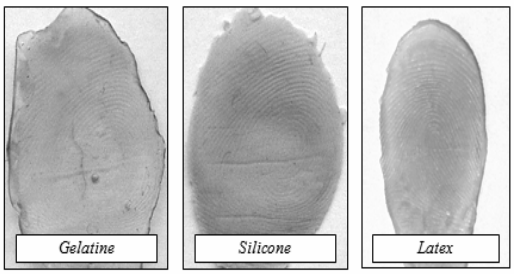


Figure 3: Different fake fingerprints made of gilatine, silicone and latex [13]

The vendor BioLab claims that their system can detect fake fingerprint by odor analysis and skin distortion [13].

If it is voice verification biometric system then it is not feasible for putting into public places. Because the added noise from outside may generate more false rejection. The voice biometric authentication system can be faked easily by advance quality of voice recording of the owner [16].

Figure 4: Movie shows a voice recorder played before the voice biometric system to fake.

The iris biometric is the more accurate invariable of biometric authentication system [29]. "Iris recognition is the top biometrics ID technology, British researchers claim" [28] [29]. Patent company Indian Technology claims that it can match an iris against a database of 100000 reference samples in 2-3 seconds comparable fingerprint database might take 15 minutes [16]. But in reality the iris

biometric system is also can be faked by producing artificial eye or by removing eye from the owner and then place it before the system. It is true that faking iris biometric is bit tough. It is also may be possible by capturing owners eye pattern from distance using sophisticated camera and printing it and then placing before the machine may fake the iris biometric authentication system. One important thing is that it is not necessary to present the natural live eye before the machine.

In the report, the comment from CEO of Mahindra Special Services Groups says "A biometric authentication, I feel represents the new plus ultra of the existing authentication methods". Yes, some extend it is true that biometric authentication system users do not require to remember the password or PIN number or nothing to worry to hacked or copied or stolen or read from the buffer but we should remember at the same time that the this system is not spoof proof and above different explanation shows how easily some of the biometric system can be faked [13][14][15][16]. For an example we move everywhere and leaving our finger print here and there. By some kind of chemical treatment the stain of our finger can be extracted to produce fake finger print [17].

In another comment the commentator believed that the biometric authentication system is better because of its uniqueness and measurement technique. In fact it is found in a research that a strong correlation between the inheritance of fingerprint pattern and the overall size, shape and spacing of the ridges [18]. The identifying ridge features, however, are not inheritable, which makes every fingerprint unique [18]. Table 1 shows different group and their coefficient of correlation. It shows the twins are very much similar that unrelated individuals. Twins are more likely to have same size, shape of finger print but ridges might differ.

Table1: Shows correlation of fingerprint [18].

| Coefficient of Correlation | Group |
|---|---|
| 0.92 | Monozygotic (identical) twins |
| 0.54 | Dizygotic (fraternal) twins |
| 0.60 | Related siblings |
| 0.27 | Unrelated individuals |

Mr. Sanjeev Menon, GM of Lenovo India suggested that including fingerprint biometric may reduce the current cost of helpdesk which is currently 35-50 percent in total. To make user friendly security system in laptop IBM ThinkPad included the biometric fingerprint authentication system and also provided password management software. The password software is able to handle different passwords for different sites and applications for the user. When these different passwords are needed then instead of typing the passwords again and again, user will swipe his or her finger on the scanner. This helps to avoid remembering different password for different sites and applications. It also replaces Microsoft® Windows® and BIOS passwords. The user may use fingerprint to access the web or other application where password is needed. It is a good security feature to include finger biometric but does not eliminate the threats. For example if some one steals the laptop or lost pc then it has no value of having biometric finger print authentication in the system. Easily the person can remove the hard disk and get the data out of it. To solve this problem data encryption may protect the data to be misused or stolen and in this case the data security depends on the encryption algorithm. However vulnerability related to finger prints also remains major concerning issue.

Including fingerprint biometric feature which increases the price around $50 will not be a big burden for those who can afford the laptop. Pointing to the comment of 98% to 99% accuracy of fingerprint analysis would be a matter of concern because the author did not mention in detail whether the percentage given for false rejection or false acceptance. But there are some system

which having even less percentage of false acceptance and false rejection such as Department of Energy's Sandia National Labs and the United Kingdom's National Physical Laboratory which found its system to have equal error rates of 0.1 and 0.4 percent, respectively [20]. In above case is more acceptable.

Finally, the report featured many comments regarding various issues of biometric authentication system. Most of the comments are in very abstract form. The details of pros and cons are not explained. It mostly tried to create positive impression from the technological point of view. But at the comments on the cost factor like iris biometric costing 100,000Rs may create some kind of negative attitude among the readers. Government and people may support to implement iris biometric authentication system in several places but due to shortage of fund so many good ideas fails or never realized. There is another concluding mix comment which says "The promise of improved security with biometric technology is comforting. However, the debate over biometric security will- and should – continue" may have an impact of mix reaction on this technology.

b) **"Concern Over Biometric Passports"** on 30th March, 2004 in **BBC News** [2]. This report is based on the agreement on biometric passport decided by the International Civil Aviation Organization ICAO. It has agreed on an international standard for facial recognition biometric passport for all new passports. It also agreed to have additional pages to be included in the passport to introduce the biometric authentication. It is projected that by 2015 it could create a database of over a billion of people around the world. Biometric authentication system is part of big surveillance infrastructure which monitors the movement of individuals. Hence this concept is opposed by the "American Civil Liberty Union" who fears that end of the day this will violate the basic privacy and liberty of human being. Similar type of comment made by "Privacy International". In the report several concern have been raised by these organizations whose fear this biometric authentication system would violate the individual privacy.

While analyzing the news in detail it is found in the ICAO web site that the unanimous decision was taken by the member countries as follows: "ICAO TAG-MRTD/NTWG RESOLUTION N001 - Berlin, 28 June 2002 ICAO TAG-MRTD/NTWG endorses the use of face recognition as the globally interoperable biometric for machine assisted identity confirmation with machine readable travel documents. ICAO TAG-MRTD/NTWG further recognizes that Member States may elect to use fingerprint and/or iris recognition as additional biometric technologies in support of machine assisted identity confirmation" [23]. The above remark clearly says for facial biometric and as optional member states may include finger or iris biometric.

Normally the digital cameras are used to capture the face image then it is use it in analyzing facial characteristics like the distance between eyes, nose, mouth, and jaw edges. These measurements are broken into facial planes and stored in chip or in database. Face biometric authentication system works mainly two ways such as "Face Appearance" and "Face Geometry". There is another technique also applied called "Facial Thermograms", uses infrared heat scans to identify facial characteristics [26]. Previously smiling, blinking of eyes or movement could lead to false rejection. To get more accurate result many systems require the user to smile, blink, or cry. This technique is gaining support as a potential method but at the same time opponent number is also not less. The newspaper reported the ACLU's opposition because of basic privacy and human right violation and also due to unreliability. "Data on face-recognition test at Palm beach airport further demonstrates systems' fatal flaws" ACLU says in their website [25]. They go on saying "First there were lab tests, then experiments at the Super Bowl and on the streets of Tampa, and now at the Palm Beach airport. In every case, the experience has been the same: facial recognition is a clunker that holds little promise to make us safer" [25]. Their test showed the facial biometric could be faked easily and not reliable because high

rate of false rejection rate. It is true that facial biometric is less reliable because sunglass, angel of head, lighting and motion may lead to wrong result. For an example child's cry can lead to false rejection. Data can be stored in two ways such as in central database which may store the templates to be used for matching and other is smart card in which person instant templates before a reader compared with the card templates [27]. Now doubt remains when the passports will be created digitally then government or authority may preserve this data and may use for wrong purpose. In practical also it is found that several developed country introduced huge surveillance system in every corner of the street and monitoring people movement. It may be debated still while issuing passport in present system authority keeps the data. Reliability of the biometric system, level of security of system including transmission, and storage all makes concerning issues. In that context the ACLU and privacy international is right. ICAO standard in fact does not specifically recommended for database rather it insist on smart card embedded with passport [23]. The card will keep the biometric templates for authentication checking. But for effective authentication checking and effective use of data authority may be insisted to keep data into the database and that leads to the private issue of and individual. The concern related to the privacy issue is also exists in current system but like biometric. Biometric authentication system adds extra information on top of the existing data. The authority will have not only personal data but also persons different organ, different images (blink, smile, cry etc) seems no regard to privacy issue. The facial biometric authentication is not good as iris one and in the iris biometric authentication system there is less privacy issue relates to privacy matter compare to face biometric. Iris could be one solution in this respect of privacy issue.

BBC is the well known largest broadcasting corporation in the world [22]. They have readers and viewers from diverse society. People from all segment of the world read BBC news. So the report may be able to motivate some readers. The report focused on social issues and in abstract form. This report has created some kind of negative impression on biometric authentication implementation in passport. The question remains whether it has presented right way or flawed way? It is technical topic but relates to pubic concern hence it was good decision to ignore technical part of biometric authentication in this issue. But when it is describing the different civil organizations comments then as a good news provider it is obviously expected that they should provide the comments of other side that supports the idea of implementing biometric authentication.

From the technical point of view the report is presented is right way but it is not necessary that the technically right way presented report will eventually create positive impression. After reading and analyzing the report we found it is a very brief report. No details have been provided on biometric authentication. It is not presented in right way because it presented many comments from one side rather than both side. Without providing the words of other side of the news becomes one sided may create the impression in favor of the presented side i.e. negative impression about the biometric passport.

c) **"The future of airport security"** By Jonathan Duffy on 12th November 2003, in BBC News [3]. This report describes about the security systems of the airport in the near future. Among several devices used in airport security system and biometric authentication system is one of that. At the beginning it is explained about the different types of biometric identification such as finger, iris or facial. Later it gave the reference of its implementation in Amsterdam's Schipol airport and as experimental basis at Dubai airport.

In the analysis of this report it is found that the report combines different technology used in the airport security system biometric authentication is just a part of it. It covered small portion of the whole report on biometric issues. It did not explain detail issues related to the biometric which may keep the reader in dark. Biometric authentication system presented in more abstract form.

In this report, it says that facial biometric scanning may be caught into computer and gone through the several checking to find

matches with suspect list! Yes it is true because every biometric system work in three steps such as enrolling, storing and processing. Storing may be possible either in database or else in smart card [15]. But in either storing mechanism, authority can get picture and compared with suspects list.
The report is published couple of years back when it referred that Dubai airport using biometric authentication as experimental basis but when we searched through the net, we found that currently almost all deportation centre and airports of UAE are using iris biometric authentication and several people were deported by checking from the database data [21]. Several other countries such as United States, Uk, Australia, Switzerland and Sweden already started issuing biometric passport or shortly they are going to issue the biometric passport to their citizen [21].
In parallel to some positive comments on biometric authentication author made some negative comments as well. Positive comments such of Paul Crombie of a technology firm called "Novar" claims that their system can measure the distance between mouth and eyes and generates 1700 points before scanning a database of 100,000 and finding a match –all in one second. Yes, today there are plenty of vendors who provide similar type of greater accuracy of biometric authentication system [20]. Regarding the reliability issue the reporter commented that the biometric authentication technology is still in "infancy stage". Definitely this creates a negative impression in respect to the implementation such an infancy machine. But today it is 2006 not 2003 and the technology is not that infancy level at all. It is more reliable and accurate and provides better performance.

Finally from the abstract and small report, the reporter tried to show the real factors of biometric authentication system in 2003. Overall the report created negative impression by quoting the comment on technology at its infancy level. This is really a matter of great concern because if that itself is at the infancy level then few people will support to implement. However If we look into some of the readers comments which also included in this report too clearly show the majority of the readers questioned on reliability of biometric authentication systems. They questioned on the ethical and privacy issue as well. Hence we also do agree with the majority of the readers comment that this report also created some kind of negative attitude towards the biometric system by questing on reliability and ethical issues. As people do care about their privacy and ethical issues hence in that perspective it has served more negative sense than positive.

**d) "Biometric Passports Set to Take Flight"** by Erin Biba on 21st March, 2005 in PCWorld [9]. The report starts with the statement "Your next passport may be electronic, but will it be any more secure?" The report is about the introduction of new biometric passport by the US government. The passport is going to contain RFID chip. It also referred that the new passport is more expensive than the existing one. However if the chip is broken or damaged then there is nothing wrong about that because the same information is available in the passport pages. Some commentators said that this passport may put anyone in danger and make a perfect target even in the crowded public place [9]. Some commentator said when the chip is broken it is nothing but like today's passport.

In response to the headline question about more secured biometric password than existing one or now, we would say every technology has its own pros and cons. Current passport is kind of physical document that travelers need to carry with them. Tokens advantage is that they have neither false acceptance problem nor false rejection like biometric authentication system has. Even if the token such as password, PIN, key, or ID card get lost then each of them can be revoked, changed or reissued where as a biometric measurement can not [28]. Another important advantage of biometric authentication is that biometrics cannot be lost, loaned, or forgotten. "Token-based systems must verify that the presenter is the authorized user, not an unauthorized person who has come to possess the token. " [28]. It is also doubted that the authority may use database but it is already mentioned with or without database the biometric passport can be implemented. On the issue of embedded chip in passport in biometric authentication may create some kind of

security concern. ICAO also concerned this information mishandling issue but strongly recommended that the chip must be able to concealed information as much as possible.

The majority of the readers of this magazine are expected to have basic technical knowledge because the news source is basically technical magazine. The report is not presented such that the readers will get worry about the technology. Hence the report is presented in right way and would create good impression.

## CONCLUSION

"Biometric technology is inherently individuating and interfaces easily to database technology, making privacy violations easier and more damaging" [28]. "Biometrics are no substitute for quality data about potential risks" [28]. "Biometric systems' accuracy is impossible to assess before deployment". Apart from the newspaper reports in this paper, we went through several other reports as well on this issue. Some of them are presented in right way and some are in very abstract form. Some of the reports may create negative impression and some may create positive. But one thing, we observed that technical magazines create more positive impression than the general newspapers. It may be due to the chosen newspaper reports are older than magazine reports. Technical magazines present the story more in detail and balanced way than the normal traditional news sites.

## REFERENCES


1. http://www.business-standard.com/general/storypage.php?&autono=222869 on April 25, 2006
2. http://news.bbc.co.uk/2/hi/technology/3582461.stm on Tuesday, 30 March, 2004, 11:46 GMT 12:46 UK
3. http://news.bbc.co.uk/2/hi/uk_news/magazine/3263343.stm on Wednesday, 12 November 2003, 10:49 GMT
4. http://www.galwayeducationcentre.ie/athenry/a_brief_history_of_biometrics.html on April 21,2006
5. http://ctl.ncsc.dni.us/biomet%20web/BMHistory.html on April 21,2006
6. http://ntrg.cs.tcd.ie/undergrad/4ba2.02/biometrics/history.html on April 23,2006
7. http://en.wikipedia.org/wiki/Biometrics last modified 17:51, 1 May 2006.
8. http://www.technologyreview.com/read_article.aspx?id=16684&ch=biztech Tuesday, April 11, 2006
9. http://www.pcworld.com/news/article/0,aid,120112,00.asp May 4th,2006.
10. http://news.zdnet.com/2100-1009_22-6062828.html
11. http://www.computerworld.com/securitytopics/security/story/0,10801,110564,00.html?source=other
12. http://www.business-standard.com/bsonline/aboutus.php?leftnm=11 May 12th,2006
13. http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=7&pathSubj=111%7C%7C7&Req=& May 14th,2006
14. http://www.dansdata.com/uareu.htm May 14th,2006
15. http://science.howstuffworks.com/biometrics.htm May 14th,2006
16. http://www.eff.org/Privacy/Surveillance/biometrics/ May 15th,2006
17. http://bias.csr.unibo.it/maltoni/handbook/ May 15th,2006
18. http://www.sciam.com/askexpert_question.cfm?articleID=0008E9CF-3762-11F1-B76283414B7F0000&catID=3&topicID=3 May 15th, 2006.
19. http://www.pc.ibm.com/us/security/fingerprintreader.html May 15th, 2006.
20. http://www.biometricgroup.com/in_the_news/06_01_03.html May 15th, 2006.
21. http://www.businessempowered.com/issues/2005/01/en/feat_biometric.shtml May 16,2006-05-20
22. http://en.wikipedia.org/wiki/Bbc May 19,2006-05-20
23. http://www.icao.int/mrtd/download/documents/Biometrics%20deployment%20of%20Machine%20Readable%20Travel%20Documents%202004.pdf May 19,2006-05-20
24. http://www.cs.auckland.ac.nz/~pgut001/pubs/biometrics.pdf May 19,2006-05-20
25. http://aclu.org/privacy/spying/14864prs20020514.html May 19,2006-05-20
26. http://icbmp.uaeu.ac.ae/Proceedings/PDFPAPERS/63_ICBMP.pdf May 19,2006-05-20
27. http://www.dataprotection.ie/viewprint.asp?fn=/documents/guidance/bio.htm May 19,2006-05-20
28. http://www.eff.org/Privacy/Surveillance/biometrics/ May 19,2006-05-20
29. http://www.theregister.co.uk/2001/05/18/iris_recognition_is_best_biometric/ May 20,2006-05-20