Trinity Technology Review Apr – Jun 2016

Disclaimer: The views and opinions presented in the articles, case studies, research work and other contributions published in Trinity Tech Review (TTR) are solely attributable to the authors of respective contributions. If these are contradictory to any particular person or entity, TTR shall not be liable for the present opinions, inadequacy of the information, any mistakes or inaccuracies.

Trinity Institute of Professional Studies
An ISO 9001:2008 Certified Institution
(Affiliated to Guru Gobind Singh Indraprastha University, Delhi)

Sector-9, Dwarka, New Delhi-110075

Ph: 45636921/22/23/24, Telefax : 45636925
www.tips.edu.in, tips@tips.edu.in

TRINITY INSTITUTE OF PROFESSIONAL STUDIES
Sector-9, Dwarka Institutional Area, New Delhi-110075, Tel: 011-45636921/22/23/24
Certified as "A" Grade Institution by SFRC, Govt. of NCT of Delhi
ISO – 9001:2008
Certified Affiliated to
GGSIP University

STATEMENT ABOUT OWNERSHIP AND OTHER DETAILS OF TTR/TMR
FORM 5 (RULE 8)

1.	Printer's Name	:	Dr. R.K. Tandon
	Nationality	:	Indian
	Address	:	Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
2.	Place of Publication	:	Delhi
3.	Periodicity of Publication	:	Quarterly
4.	Publisher's Name	:	Dr. R.K. Tandon
	Nationality	:	Indian
	Address	:	Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
5.	Editor's Name	:	Dr. Vikas Rao Vadi
	Nationality	:	Indian
	Address	:	Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
6.	Name and Address of the individual who owns the journal and partners or shareholders holding more than one per cent of the capital.	:	CHAIRMAN Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
7.	Hosted at (url)	:	www.tips.edu.in

I, Dr. R.K. Tandon, hereby declare that the particulars given above are true to the best of my knowledge and belief.

Dr. R.K. Tandon

Confluence of Technologies: NBIC

Charanpreet Kaur

ABSTRACT

In the history of technology, emerging technologies are contemporary advances and innovation in the various fields of technology. Various converging technologies have emerged in the technological convergence of different systems evolving towards similar goals. Emerging technologies are those technical innovations which represent progressive developments within a field for competitive advantage and the converging technologies represent previously distinct fields which are in some way moving towards stronger inter-connection and similar goals.

Convergence simply means amalgamation of different technologies. In the context of Computer Applications we can say that it's a phenomenon when different technologies evolve towards performing a similar task. The rise of convergent technologies is ushering everywhere, today almost every sector is busy in crafting the strategies for convergence. The result is the Big Bang of convergence and it is likely to produce the biggest explosion of innovation since the dawn of internet.

Factors which are responsible for this phenomenon:-

- Relentless evolution of technology
- Technology industry's hunger for growth

In his massive study of the Information Society, Manuel Castells writes, "Technological convergence increasingly extends to growing interdependence between the biological and micro-electronics revolutions, both materially and methodologically"

Although we cannot rule out that convergence could lead to some negative effects and some flop products but a few breakthroughs are sure to happen, paving the way for new technologies and changing the way we work and live.

There are recent examples like (ICT), which is the amalgamation of Information technology and communication technology. Similarly Information technology

integrated with bio-technology has led to Bio-Informatics. The basic idea that scientific and technological innovation can be stimulated through the convergence of two, three technologies. So, in this paper we will discuss the "NBIC" (Nano-Bio-Info-Cogno)

NBIC stays for:

— Nanotechnology: Technology related to features of nanometre scale (10-9 meters), thin films, fine particles, chemical synthesis, advanced microlithography, and so forth;

— Biotechnology: The application of science and engineering to the direct or indirect use of living organisms, or parts or products of living organisms, in their natural or modified forms;

— Information Technology: Applied computer systems – both hardware and software, including networking and telecommunications;

— Cognitive Science: The study of intelligence and intelligent systems, with particular reference to intelligent behaviour as computation.

APPLICATIONS OF NBIC

1) Preventive medicine
2) Disease treatment
3)Disability alleviation

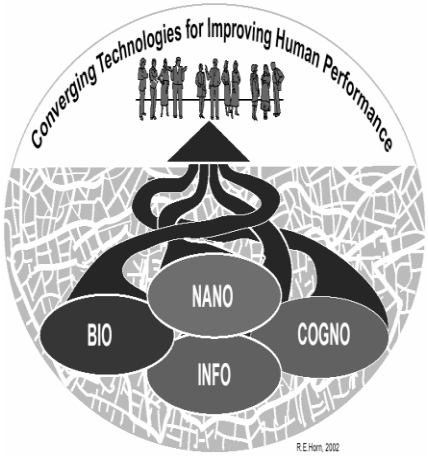
So this paper highlights that how convergent technologies has completely revolutionised the very notion of technology.

Keywords: Nano-Technology, Bio-Informatics, Communication Technology, Cognitive Science

INTRODUCTION

The integration and synergy of the four technologies (nano-bio-info-cogno) originate from the Nano scale, where the building blocks of matter are established. It symbolizes the confluence of technologies that now offers the promise of improving human lives in many ways, and the realignment of traditional disciplinary boundaries that will be needed to realize this potential. NBIC is the newest concept in science. It has been introduced for less than 10 years. Indeed, each of the four components; nanotechnology, biotechnology, information technology and new technologies based on cognitive science, has already proved for its usefulness at present. Establishment of convergence across all fields of science and technology is the important practice at present

(Martin-Sanchez et al., 2009; Bainbridge et al., 2006). The concept of convergence of science seems to be the effective tool in approaching a scientific question. For sure, NBIC can be well applied in biomedical science. Martin-Sanchez et al. recently performed a study to analyse the role that biomedical informatics could play in the application of the NBIC Converging Technologies and concluded that "particular attention should be placed on the ethical, legal, and social issues raised by the NBIC convergence (Martin-Sanchez et al., 2009). Gordijn proposed that the two steps for success in implement of NBIC included a) realizing the novelty of NBIC as the convergence of sciences and b) planning for the prospects of the NBIC projects (Gordijn et al., 2006). National Science Foundation concluded that NBIC will be the hope for enhancing human capabilities and serving human needs.



This picture symbolizes the confluence of technologies that now offers the promise of improving human lives in many ways, and the realignment of traditional disciplinary boundaries that will be needed to realize this potential. New and more direct pathways towards human goals are envisioned in working habits, in economic activity, and in the humanities.

OBJECTIVES

What are the implications of unifying sciences and converging technologies? How will scientific knowledge and current technologies evolve and what emerging developments are envisioned? What visionary ideas can guide research to accomplish broad benefits for humanity? What can be done to achieve the best results over the coming years?

I. UNIFYING SCIENCES AND CONVERGING TECHNOLOGIES

Half a millennium ago, Renaissance leaders were masters of several fields simultaneously. Today, however, specialization has splintered the arts and engineering, and no one can master more than a tiny fragment of human creativity. The sciences have reached a watershed at which they must unify if they are to continue to advance rapidly. Convergence of the sciences can initiate a new renaissance, embodying a holistic view of technology based on transformative tools, the mathematics of complex systems, and unified cause-and-effect understanding of the physical world from the Nano scale to the planetary scale.

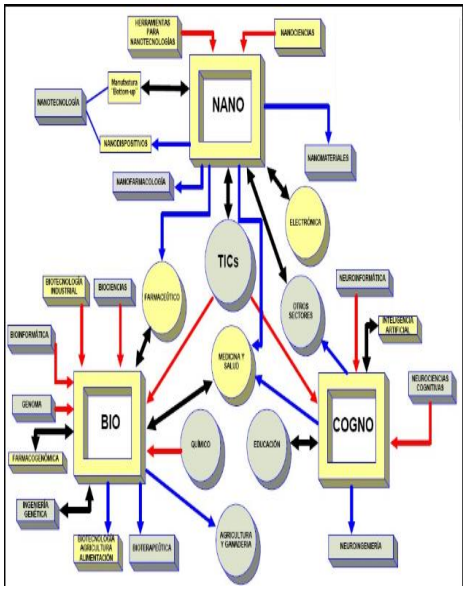
The classical approach can be the first line of approach to clarify the scientific problem. This can be fulfilled for the hard to discover area by using nanotechnology that helps answer the problem in the Nano-area. After getting the information, information technology can help in the management of the data. Accompanied with cognotechnology, interpretation and implication of information to real usage is further integrated together to analyse the problem.

Many of the most powerful developments in biotechnology and biomedicine are taking place at the nanoscale. This is true not merely in genetic engineering (with DNA molecules about 3 nanometers in width), aging (with quantum dots of few nanometers), targeted drugs (with nanoparticles as carriers), and biocompatible prosthesis (with molecules "by design") – but also in those many branches of biotechnology where improved understanding of the processes that give life to cells would be advantageous. Thus, much biotechnology today – and increasingly more in the future – is a variant of nanotechnology.

Modern information technology is based on microelectronics, which is rapidly evolving into Nano electronics. As a first step, computer chips are manufactured by processes such as photolithography that deposit many thiners of substances on the chip, then etch away unneeded areas. The layers on the chips, as well as

the layers on magnetic disks that store data, have become nanoscale thin, and this very thinness gives them unique electric properties. The current advances on nanolayers with special insulation or conducting properties will evolve to three-dimensional nanostructures and devices and may lead to replacing the information carrier from electron charge to new carriers such as electron spin, photon, or quantum state. Recently, the width of the transistors on a chip has also moved into the nanoscale, with some being only 50 nanometers wide. Currently, researchers are exploring a number of avenues for achieving molecular computing – such as building transistors out of carbon nanotubes – that could form the basis of a new generation of computing, achieving much greater information densities.

Nanotechnology and information technology are enablers, as well as creative fields in their own right, giving other branches of science and technology new powers. Biotechnology and cognitive science directly concern the human body and mind and have the



ssible implications for human physical and mental health.

Figure 1 - Convergence of technologies

II. VISION FOR ENHANCING HUMAN ABILITIES AND SOCIETAL PERFORMANCE

Fundamental scientific discovery needs at least ten years to be implemented in new technologies, NBIC convergence within our own lifetimes, now is the right time to begin. Each scientific and

engineering field has much to contribute to enhancing human abilities, to solving the pressing problems faced by our society in the twenty-first century, and to expanding human knowledge about

our species and the world we inhabit; but combined, their potential contribution is vast. Following are twenty ways the workshop determined that convergent technologies could benefit humanity in a time frame of 10 to 20 years.

- Fast, broadband interfaces directly between the human brain and machines will transform work in factories, control automobiles, en sure military superiority, and enable news ports, art forms and modes of interaction between people.
- Comfortable, wearable sensors and computers will enhance every person's awareness of his or her health condition, environment, chemical pollutants, potential hazards, and information of interest about local businesses, natural resources, and the like.
- Robots and software agents will be far more useful for human beings, because they will operate on principles compatible with human goals, awareness, and personality.
- People from all backgrounds and of all ranges of ability will learn valuable new knowledge and skills more reliably and quickly, whether in school, on the job, or at home.
- Individuals and teams will be able to communicate and cooperate profitably across traditional barriers of culture, language, distance, and professional specialization, thus greatly increasing the effectiveness of groups, organizations, and multinational partnerships.
- The human body will be more durable, healthier, more energetic, easier to repair, and more resistant to many kinds of stress, biological threats, and aging processes.
- Machines an d structures of all kinds, from homes to air craft, will be constructed of materials that have exactly the desired properties, including the ability to adapt to changing situations, high energy efficiency, and environmental friendliness.
- A combination of technologies and treatments will compensate for many physical and mental disabilities and will eradicate altogether some handicaps that have plagued the lives of millions of people.

- National security will be greatly strengthened by lightweight, information-rich war fighting systems, capable uninhabited combat vehicles, adaptable smart materials, invulnerable data networks, superior intelligence-gathering systems, and effective measures against biological, chemical, radiological, and nuclear attacks.
- Anywhere in the world, an individual will have instantaneous access to needed information, whether practical or scientific in nature, in a form tailored for most effective use by the particular individual.
- Engineers, artists, architects, and designers will experience tremendously expanded creative abilities, both with a variety of new tools and through improved understanding of the wellsprings of human creativity.
- The ability to control the genetics of humans, animals, and agricultural plants will greatly benefit human welfare; widespread consensus about ethical, legal, and moral issues will be built.
- The vast promise of outer space will finally be realized by means of efficient launch vehicles, robotic construction of extra-terrestrial bases, and profitable exploitation of the resources of the Moon, Mars, or near-Earth approaching asteroids.
- New organizational structures and management principles based on fast, reliable communication of needed in formation will vastly increase the effectiveness of administrators in business, education, and government.
- Average persons, as well as policymakers, will have a vastly improved awareness of the cognitive, social, and biological forces operating their lives, enabling far better adjustment, creativity, and daily decision making.
- Factories of tomorrow will be organized around converging technologies and increased human-machine capabilities as “intelligent environments” that achieve the maximum benefits of both mass production and custom design.
- Agriculture and the food industry will greatly increase yields and reduce spoilage through networks of cheap, smart sensors

that constantly monitor the condition and needs of plants, animals, and farm products.

- Transportation will be safe, cheap, and fast, due to ubiquitous real-time information systems, extremely high-efficiency vehicle designs and the use of synthetic materials and machines fabricated from the nanoscale for optimum performance.

The work of scientists will be revolutionized by importing approaches pioneered in other sciences, for example, genetic research employing principles from natural language processing and cultural research employing principles from genetics. Formal education will be transformed by a unified but diverse curriculum based on a comprehensive, hierarchical intellectual paradigm for understanding the architecture of the physical world from the nanoscale through the cosmic scale.

The developments in these fields not just complement each other - the fields are gradually merging.

APPLICATIONS OF NBIC

These days health sector is crippled with failures, inefficiency and adverse reactions due to insufficient disease prediction and prevention. advancement in technology and introduction of NBIC filled the lacunae of health sector and raised new opportunities in the emerging fields of personalized medicine (in which disease detection, diagnosis and therapy are tailored to each individual's molecular profile) and predictive medicine (in which genetic and molecular information is used to predict disease development, progression and clinical outcome).

CHALLENGES AND OPPORTUNITIES IN NBIC

The uncertain, cross-disciplinary environment of emerging advanced technology makes for very complex planning that how the pieces of a complex technological system fit together, interact, and evolve. Both challenges and opportunities lie in juxtaposition for the future of society and science.

The way these technologies are complementing and merging with

each other, it seems that it will completely revolutionize our socio-economic side by side improve the quality of life.

CONCLUSION

Although NBIC is at the nascent stage of exploration, still various applications of this new holistic models seems appealing. It holds significant promise in shaping the future development."The timing and full nature of the NBIC impact is still unclear but when it happens, change will be rapid, leaving little chance for catching up."

REFERENCES

1. Managing nano-bio-info-cogno innovations, Edited by williamsimsbainbridge, mihail c. Roco.
2. Converging Technologies for Improving Human Performance nanotechnology, biotechnology, information technology and cognitive science, Edited by Mihail C. Roco and William Sims Bainbridge.

Voice Biometric: A New Trend to Enhance Security

Roopal Kalra

INTRODUCTION

Security has always been a primary concern whether be it home or office. With the advent of information technology security over the information acquired takes a prime concern. Security breaches are prevailing from technical to business field. Information technology has inundated the business sector and education world and every possible area one can think of. Consider the case of CERT-I n where, Hours ahead of its planned protest against certain incidents of internet censorship in India , hacker collective Anonymous attacked and brought down the website run by Computer Emergency Response Team India (CERT-I n). Amongst the most disastrous information leakage breach was the hacking of data for 1.5 million Master & VISA card users. VISA & MASTER card alerts banks about the security breach at Global Payments. The alert clearly stated that full Track 1 & Track 2 information was taken and could have been abused for counterfeit new cards. This information had been compromised from a period of January 21,2012 to February 25,2012. Yet it was not the company who disclosed the security breach, the security blogger Brian Krebs in security reported the event on 30,March,2012, This pattern is common for all security breaches as the conclusion who are impacted are the last ones to know about it. These threats to business need a stronger mechanism of security to counter them. Biometrics has offered new venues to resolve these issues.

Biometrics refers to the physiological or behavioral characteristics of a person to authenticate his/her identity. This Biometrics is the most prominent and promising technique used for authenticating a person's identity. Voice Biometrics, Finger printing, facial ognition area few biometrics that are used for security purposes. This paper majorly cover Voice Biometrics. voice biometrics uses the pitch, tone, and rhythm of speech. Background noise, illness, age, and differences in telephones and microphones can cause problems with voice identification and authorization.[Paper: exploration - voice -biometrics_1436] This is mostly used by Banks and Call Centres to authenticate there users. A telephone or microphone is required to proved your identity. Voice

Biometrics is mostly adopted by the customers as they find it as a normal telephonic conversation. Remotely any customer from any location can login or use his/her ID.

Each person has a unique voice and that can be easily stored in form of bits. So, this provide a better option for the developer or programmers to authenticate their software, databases etcusing Voice Biometrics. Number of methods are used to apply these Biometrics. As a first step the new user has to record his/her speech by calling a telephone collection script. Once there is an existent recording the user is allowed to invoke an enrolment form and specify personal data, such as passwords and answers to questions on various topics, as suggested by the server. The answers can be selections from predetermined value lists, e.g. selected cities or colours, or user's own new keywords. It is also possible to add new questions within the existent topics or dynamically generate these based on contexts or history of previous transactions or other events.

I. INTRODUCTION

In the information age, information is an asset and needs to be secured from attacks. With the advent of information technology age, the entire business community is transforming their physical data to electronic storage. Consequently, securing information has become a prime concern for organizations. Nonetheless, security breaches are prevailing right from the technical to the business domain. Consider the case of Computer Emergency Response Team India (CERT-I n) where hours ahead of its planned protest against certain incidents of internet censorship in India, the hacker, collective Anonymous, attacked and brought down the website run by CERT-I n[2].

Another most disastrous information leakage breach was reported by Brian Kerbs where the data was hacked for 1.5 million Master and VISA card users. This breach happened at the US based credit card processor Global Payments. VISA & MASTER card hence forth alerted banks about the security breach. The alert clearly stated that full Track 1 & Track 2 information was retrieved and could have been abused to counterfeit new cards. This information was

compromised from a period of January 21,2012 to February 25,2012. Yet, it was not the company who disclosed the security breach, the security blogger, Brian Krebs, reported the event on 30 March, 2012[2]. This pattern is common for all security breaches where the ones who are impacted are the last ones to know about it.

Security breaches are accompanied with copious costs. They can be anything from lost business due to compromised information, lost productivity, labour and legal expenses, public relations costs, higher insurance premiums, defence against lawsuits and security upgrades to prevent future attacks and then add to that intangible costs such as loss of trust, negative publicity and competitor access to confidential information[3]. These threats to business need a stronger mechanism of security to counter them.

Biometrics has propounded new avenues to resolve such issues. Biometrics refers to the physiological or behavioral characteristics of a person to authenticate his/her identity. Biometrics is increasingly becoming the most prominent and promising technique used for authenticating a person's identity[4]. Voice Biometrics, finger printing, facial recognition are few biometric techniques that are being employed for security purposes. The biometric system comprises of three components where the input is used to acquire signals. These signals are then filtered to remove redundant and irrelevant information. These features are then compared with reference data to either accept or reject the characteristic being corroborated. The biometric characteristics like iris pattern, retina pattern, skin spectrum, finger prints or voice are characteristic of a particular person and hence are difficult to impersonate. These abilities differentiate biometrics from all other forms of automated authentication; hence systems implementing the security using these measures are more secure.

Speech prevails as the only modality amongst all the biometrics which can be used for remote authentication. Speech has inundated almost every industry - from checking a flight schedule, to completing a bank transaction.It is an extremely cost effective solution since the ubiquitous telephone system provides a familiar network of sensors for obtaining and delivering the speech signal. There is no need for special signal

transducers or networks to be installed at application access points since a cell phone gives one access almost anywhere [11].Even for non-telephone based applications, sound cards and microphones are low-cost and readily available. Hence as compared with other biometrics, no special hardware is required. Evenusers find interacting with systems using voiceeasy and non-invasive which is not the case with other biometrics. Hence we focus on voice biometrics and the corresponding industry is the focus of this paper.

II. VOICE BIOMETRIC

Speech processing applications extract acoustic information from the stream of speech to perform recognition of words being spoken. The speech recognition techniques are able to extract the words and the speaker identity; along with the accent, expression, style of speech, emotion and the state of health of the speaker;from the immensely rich speech signal. The emphasis in speech recognition techniques is on the speech production and recognition whereas in the case of voice biometric the physiological features of voice print are captured to verify the identity of the caller. The voice models include information about resonance pattern and relationships that reflect size and shape of the mouth, nose and throat. The voice model is analysed from the purely acoustic purpose without considering the content being spoken. The model does not represent entire sample, hence it cannot be reverse engineered to recreate original biometric sample nor can it be used as input to biometric system which expects to receive a biometric sample for analysis. The factors like background noise, illness, age, and differences in telephones and microphone scan cause problems with voice identification and authorization [5].The voice biometrics portrays two parallels in its industry: Speaker Verification and Speaker Identification.

III. SPEAKER VERIFICATION

Speaker Verification is the task of verifying the identity claim of a speaker based on his or her voice[7].Voiceprints analyse the unique geometry of speaker's vocal tract length, capacity of nasal cavity, ratio of larynx to sinuses, resulting harmonics, pitch and range to

verify users[3]. Verification can take place continuously or periodically in the background as needed or at any time. Speaker verification is performed in two phases: Enrolment followed by Recognition phase. In the enrolment phase or training phase, a sample of the user's voice is recorded to create the voice model. The voice model consists of representations of the minimum set of features required to build a model for the speaker. These features from the voice model are extracted depending on the algorithm; removing the redundant information. Upon the successful enrolment the model is stored in the database.

The recognition phase, the incoming speech goes through the same phase of feature extraction. These extracted features are then compared with the models in the database. This is followed by a scoring procedure, and depending on the target application, a decision is made based on the scores. The verification task involves an auxiliary set of models to model potential impostors.

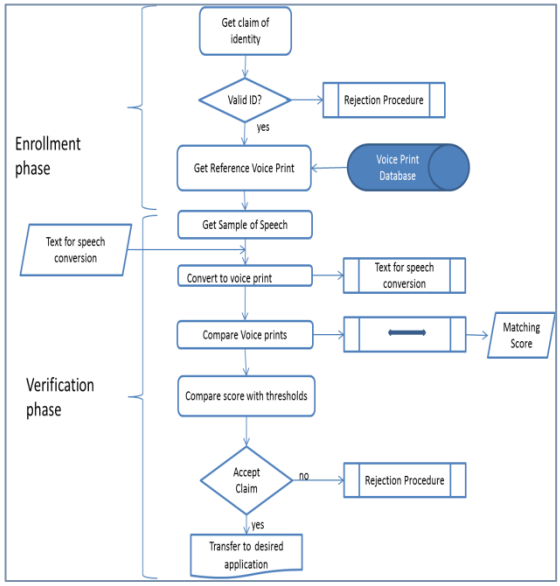


Figure 1: Speaker Verification Process

Speaker verification corroborates three basic types of user input: text dependent, text prompted and text independent.

Text dependent input is the most widely deployed variant. The speech sample is the same during the enrolment and recognition phase. The text dependent speaker verification uses the statistical method – Hidden Markov Model(HMM) – to compare the two samples. This model uses the spectral content of the speech signal determined by the physical and dynamic configuration of the vocal tract [8].

Text prompted speaker verification works on the principle that each time a user wants to access a particular application, he is prompted to articulate a

new sentence each time. The system accepts the utterance only when the registered speaker repeats the prompted sentence. The sentence can be displayed or can be spoken by a synthesised voice. This verification system was proposed in order to ward off the replay of recorded messages. The algorithms deploy Gaussian Mixture continuous HMMs or tied mixture HMMs models to implement this form of speaker verification[9].

Text independent speaker verification supports the development of unobtrusive and intermittent voice authentication. These applications require examining the on-going speech of an individual to determine his or her identity. These applications are difficult to implement in comparison to their text dependent or text prompted application since the sample and the spoken phrase are not the same. There are no constraints on the intended customers' utterance. Changes in the acoustic environment and technical factors as well as the variation of the speaker tone due to his health, mood or aging are some of the undesirable factors impacting the speaker recognition. Hence longer samples of speech are required for proper matching with the reference sample. These schemes allow background verification of the speaker and henceforth are suitable for applications like banking transactions. The user's speech is modelled by the stochastic model –the Gaussian mixture model.

The verification can also occur in an incremental manner and the user can be granted higher privileges on the application; if higher verification scores are obtained with more speech data collected as the dialog progresses.

IV. SPEAKER IDENTIFICATION

Speaker verification as we have already seen is accepting or rejecting the identity claim of an individual. Speaker identification, on the other hand, matches the spoken utterances with the ones that are available in the voice print database and tries to identify the unknown person. Speaker identification can be classified into open-set and closed set. In the closed set, the speaker to be identified is amongst the set of N enrolled speakers. The open-set speaker identification is that the speaker has to identified besides the N enrolled speakers[10].

In most cases, speaker identification is more difficult than speaker verification, because it involves multiple comparisons of utterances that are likely to be different from each other and may not have been recorded with comparable equipment. Speaker identification does not expect to receive a claim of identity. Processing begins when a sample of speech from of an unknown speaker is presented to the system; the sample may be live or recorded and systematically compares the new voiceprint with all or with a specified subset of the system's reference voiceprints. It is text-independent.

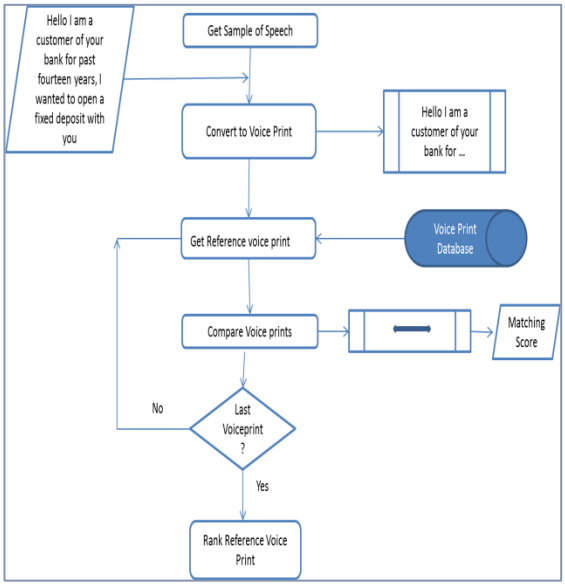


Figure 2 : Speaker Identification

V. ACCURACY OF VOICE BIOMETRIC SYSTEM

The recognition of speech becomes a daunting task in the face of uncooperative speakers and uncontrolled environmental parameters such as noise in the transmission channel; background noise etc. especially when the user is accessing an application. The performance of a biometric is fundamental to the implementation of security for an application. Hence, accuracy of a biometric system is gauged by the errors encountered.

There are two types of error that can occur during a verification task:

(a) False acceptance rate or false match rate.

(b) False rejection rate or false non-match rate.

False acceptance rate is where an unauthorized user is able to access the system. False rejection rate defines the rejection of even the authorized user. Both types of errors are a function of the decision threshold where the voice may be either accepted or rejected.The rejection rate of automatic speaker recognition increases with the background noise as it impacts the

acoustic index in the recognition phase[12, 13].Hence the decision of the threshold value is critical to a secure system; as choosing a high threshold will result only in a few users being authenticated by the application i.e. a high false rejection rate. However, having a low threshold value would result in compromising security i.e. a high false acceptance rate.

The decision threshold or equal error rate is the operating point where the false acceptance rate and the false rejection rate become equal. It determines how much variability it will allow before the identity claim is questioned or actually rejected. The voice biometric application has to be tuned around this equal error rate to allow rejection or acceptance rate based on the security of the requisite application.

VI. SECURITY OF APPLICATIONS: TWO-FACTOR OR MULTIFACTOR AUTHENTICATION

Authentication is a process where the user proves his or her identity. This verification of a person is dependent on factors like knowledge of the user, something the user possesses or on the unique features of the user [16]. The user knows passwords and PIN numbers that are allocated to him. He or she may possess smart cards, tokens or PKI certificates for strong authentication. Voice biometrics as we know captures the physiological feature – voice- of the person for authentication.

The login ID and password is the most prevalent method of authentication. This form of authentication is also called single factor authentication as each of these factors are deployed individually. But, single factor authentication is highly susceptible to malware attacks, key logger Trojans, replay attacks and shoulder surfing. [17].

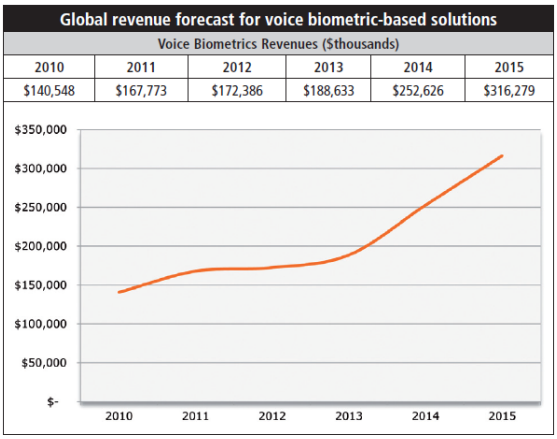
The traditional and prevalent method of authentication is an easy target for hackers, but the level of security can be increased with two factor authentication. Two-factor authentication provides a significant increase in security over the traditional username/password combination. The security of an application can be improved tremendously by combining two factors such as the password and a biometric recognition system. The threat of eavesdropping on passwords is reduced

as even if it is hacked, the hacker will not be able to challenge the biological characteristic of the user. Hence, on remote transactions and on applications where the phones can be used, voice becomes an inexpensive tool for security.

However, the strongest form of authentication occurs with multi-factor authentication. These authentication mechanisms are strong deterrents to fraudsters and are a combination of several single factor authentications. It is used for priority customer information and high-risk financial transactions [18].

VII. INDUSTRIES IN VOICE BIOMETRICS

Voice offers the best combination of precision, ease and cost effectiveness. Many industry watch dogs have shown a significant growth for voice biometrics in general and voice-based identification. This new market segment has a potential to grow to $500 million[14]. Opus Research shows the exponential increase graph for voice biometrics [15]. They have projected a market of $350 million by year 2015 as shown in figure. Hence this increases our interest to look out for various companies that deal with voice biometric.



Source: Opus Research (2011)

The industry in this segment caters to two sectors of speech recognition - Speech Processing and Biometric Security. Speech processing tools capture the samples to understand the lexical meaning of the spoken words to convert them into text. Even voice biometrics works on the same principle like the other speech-processing tools; extracting information from the stream of speech to accomplish their work. The captured model, however, does not represent the entire sample, hence it is difficult to reverse engineer the sample to recreate original biometric sample. It can, also, not be utilised as input to biometric system which expects to receive a biometric sample for analysis.

Based on the previous sections, we have identified the various parameters to draw an analysis in the spectrum of available products of various companies checking for the various security features. These parameters include the possible techniques the fraudster employ to cross the authentication barriers.

A. FRAUDSTER TECHNIQUES

With speech recognition being used as an authentication mechanism, the fraudsters deploy many techniques to rupture the authentication mechanism. They can cheat into recognizing the voice for identification using the following techniques: Spoofing, Replay attacks, Noise Interference.

B. SPOOFING ATTACK

A spoofing attack occurs when one person or program successfully masquerades as another by falsifying data and thereby gains an illegitimate advantage. Spoofing is the biggest challenge to speaker recognition, especially in situations where a user has a close same-sex relative with similar voice physiology and DNA.

The products designed should have mechanisms to handle spoofing by cleaning and correcting the sound from changes caused voice deviations. This adaptation should lead to a clear voice print.

C. NOISE INTERFERENCE

Noise interference is not a sophisticated way of bypassing security efforts, though the fraudsters have used it quite effectively. Noise can become part of the mobile while travelling by trains or walking in crowded places. A fraudster can try to inject noise expressing his inability to use the automated system and then gains to access the financial accounts by sweet-talk an inexperienced call centre agent into providing confidential data or even wiring funds. The voice biometrics products should be able to handle noise interference to make the transactions secure.

D. REPLAY ATTACKS

Replay attacks or the tape attacks occur when someone records the voice of an authorized person to fool the system by playing that recording into the phone.

This can be amended with liveness testing where the application provides for a mechanism to compare between the sample voice provided by a live human being and a copy of a feature provided by an object. Liveness testing for voice can be attained via text prompting in the form of challenge-response handles these attacks effectively. With this form of testing the physical presence of a person can be verified since the person is asked to respond to randomly generated requests which may involve repeating a sequence of words or digits. For e.g. 10, 125 or park, traffic, car. The randomness of the selection renders it very difficult for the fraudster to record and play them quickly as well as naturally. Some systems might handle these attacks using a knowledge based question; such as what school did you study in at the age of12? Some questions may be such that were never asked to the user before.

Besides the above areas of breach, speech architecture for verification and identification, itself, creates vulnerabilities in the software. Consider the files created at the time when a caller is using the system. These speech system log files are a rich repository for sensitive information at risk. Logging suppression suppresses the contents of these files to help combat the security issue.

Tuning of the speech applications, for better performance, involves capturing the audio file as well as transcribing what the system thought it heard into a text format. These files may contain social security information, personal identification numbers or other sensitive data that needs to be protected through encryption. The DTMF input to a speech system where the users are allowed to enter information through the keypad is also a log which needs to be protected.

Speech verification applications also support DTMF input for a caller, who for security reasons, prefer to enter an account number, for example, with telephone keypad. In many cases these DTMF strings will be maintained in a log file and be accessed over the network. Computer Telephony Integration where the information recorded in the system is retrieved by the agent for further analysis presents a potential area of risk. The highly distributed architectures of VoiceXML browsers, media servers and application servers spanning across local and remote networks are points on the

transmission media from data become accessible.

The security of financial, banking and other speech based applications requires that audit trails be maintained. It can be used to ensure that the authorization originated from an identified source. In case of repudiation, audit trails are exercised as a proof. Speaker recognition when used as a security mechanism for editing or saving a digital document, such as a database record, might be marked with tags relating to the speaker verification procedure or these tags could be recorded in a separate audit trail. This provides a verified record of access to and modification of the protected document, record etc. [19]

Industry

There are many companies that are dealing with speaker verification and identification. We have drawn a comparative analysis of the various companies depending on their algorithmic features as

well as their security features. These features have been picked up from the brochures of the individual companies.

The security features are concerned with the kind of authentication the product offers such as suppression of logs, whether it maintains the audit trails or encrypts for further security.

VIII. SPEAKER VERIFICATION TABLE

Vendors Criteria	IBM Websphere Voice Server	Nuance Voice Verifier	Voice Vault VoiceVault Server	Voice Trust Voice.Trust Server	Diaphonics SpikeCore Server	Persay FreeSpeech	Loquendo Speaker Verification	Armorvox Speaker identity system
Algorithmic Features								
Speech Recognition and Verification	√		√ (Speech Recognition optional)	√	√		Verification only	Voice authentication and verification
Liveness testing		√	√	√		√		√
Multilingual	√	√	√			√	√	√
Text dependent			√				√	
Text Independent	√	√	√			√	√	√
Background Verification		√	√					
Explicit Verification	√	√		√	√	√	√	
Tuning or Voice Print Adaptation		√						√
Security Features								
Multifactor Authentication		√	√	√		√	-	_
Two-factor Authentication	√		√	√	√		-	√
Audit Trail	√	√			√	√	-	
Encrypted Voice Prints and Speaker IDs		√		√	√	√	-	√
Logging Suppression			√				-	
Support for VoIP					√	√	-	√
Operative in TDM (phones)	√	√	√	√	√	√	√	√
Operating System	Is a part of Webspher e Applicati on server	Window s Server 2003 and Red Hat Linux	IVR flow well windows	call as Open platform can be integrated with oracle,SAP etc			Windows 2000, XP, Linux Red Hat	Windows ,linux and also implemented on cloud

SPEAKER IDENTIFICATION TABLE

IX.CONCLUSION

From the above, it can be seen that each of the products have their own set of features and each is different from the other. Each company have their own set of parameters and features that make their product different. Nuance is one of the leading company when we talk about Voice Biometrics and its Speech Verification tool is being used by most of the companies.

Standalone biometric doesn't provide us sufficient information to authenticate a person. We need other parameters to detect and trace the person. Unimodel authentication often suffer from enrolment problems due to non-universal biometrics traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data . One of the methods to overcome these problems is to make use of multimodal biometric authentication systems, which combine information from multiple modalities to arrive at a decision. Multi sample or multi instance algorithms use multiple samples of the same biometric. Multi sample has advantage that using multiple samples may overcome poor performance due to one sample that has unfortunate properties. Acquiring multiple samples requires either multiple copies of the sensor or the user availability for a longer period of time.

Two or more biometrics are used to authenticate a person in a better way. Face and Voice biometrics are mostly used in forensic fields. We have proposed tri-modal biometric system with fingerprint, voice and teeth. A personal identification using teeth image, which is relatively new biometric traits considered for authentication was first proposed by Tae-Woo KIM and Tae-Kyung CHO (2006) based on Linear Discriminant Analysis (LDA) as sequential steps. Other method that is used in digital signature is speech and signature model. In this model a digital pen is used and a person's signature is taken on a particular sensor tab. When signature is made that is taken as first input for authentication and the sound produced that can only be sensed by highly equipped technology is the second input. Combination of both provide us a better way to identify a person's identity.

X. REFERENCES

1. Markowit J. A., “Voice Biometrics”, Communications of the ACM, September 2000, Vol 43, no. 9.,66-73
2. Speaker Authentication: Voice Biometrics over the Telephone
3. Basha, A. Jameer, V. Palanisamy, and T. Purusothaman. "Multimodal Personal Authentication with Fingerprint, Speech and Teeth Traits using SVM Classifier." *European Journal of Scientific Research* 76.3 (2012): 463-473.

4. An Exploration of Voice Biometrics, By Lisa Myers in 2004
5. Li, Francis F. "Sound-Based Multimodal Person Identification from Signature and Voice." *Internet Monitoring and Protection (ICIMP), 2010 Fifth International Conference on*. IEEE, 2010.
6. Pelecanos, Jason, JiříNavrátil, and Ganesh Ramaswamy. "Conversational biometrics: A probabilistic view." *Advances in Biometrics* (2008): 203-224, Springer.
7. González-Rodríguez, Joaquín, DoroteoToledano, and Javier Ortega-García. "Voice biometrics." *Handbook of Biometrics* (2008): 151-170, Springer.
8. Furui, Sadaoki. "An overview of speaker recognition technology." *KLUWER INTERNATIONAL SERIES IN ENGINEERING AND COMPUTER SCIENCE* (1996): 31-56.
9. Rosenberg A E Automatic speaker verification: A review. *Proc. IEEE* 64(4): 475–487
10. Bimbot, Frédéric, et al. "A tutorial on text-independent speaker verification." *EURASIP Journal on Advances in Signal Processing* 2004.4 (2004): 101962.
11. F. Beritelli. Effect of background noise on the snr estimation of biometric parameters in forensic speaker recognition. In Proceedings of the International Conference on Signal Processing and Communication Systems (ICSPCS), 2008.
12. Kichul Kim and Moo Young Kim. Robust speaker recognition against background noisein an enhanced multi-condition domain. Consumer Electronics, IEEE Transactions on,56(3):1684 –1688, aug. 2010.
13. Klie, L. (2011). Voice R&D Speaks to Homeland Security. *Speech Technology Magazine*, *16*(3), 14
14. D.Miller, "Voice Biometrics Update 2011:Attacking Adjacent Markets", Opus Research 2011.
15. Kim, Jae-Jung, et al. "A method of risk assessment for multi-factor authentication." Journal of information Processing Systems, JiPS7.1 (2011): 187-198.
16. Smart Card Alliance (Randy Vanderhoof), "Smart Card Technology Roadmap for secure ID applications", 2003.

17. A.JameerBasha, V. Palanisamy, T. Purusothaman, Multi Model Personal Authentication with Fingerprint, Speech and Teeth Traits using SVM classifier, European Journal of Scientific Research ISSN 1450-216X Vol.76 No.3 (2012), pp.463-473.

A Proposed Monitoring System to Aid Bipolar Patients Using Sensor Network

Akhil Kumar

ABSTRACT

Bipolar disorder is a chronic mental illness that has a significant impact on the individual and society. The disease has detrimental effects on patient quality of life, and a high cost for social and health care. Long-term self-monitoring of patients with the illness has been shown to benefit patients, care providers, and researchers, but is not a panacea. Patients have been taught to self-monitor using paper-based forms, and recently, computerized versions of the forms for handheld devices have been developed and validated against traditional paper-based versions. Unfortunately, the efficacy of self-monitoring systems has inherent issues.

In this paper, a methodology to improve living conditions of patients affected with Bipolar disorder in presented. The methodology involves collection of body statistical data and further used by clinical physician to treat such patients in due course of time. The collection of body statistical data, reporting & response byclinical physician is done with sensors implanted in patient's body and at several other points.

Keywords: PAMS, WSN, Nodes, Bipolar Disorder

INTRODUCTION

Bipolar disorder [1] is a chronic mental illness that has a significant impact on the individual and society. The disease has detrimental effects on patient quality

of life, and a high cost for social and health care.

Long-term self-monitoring of patients with the illness has been shown to benefit patients, care providers, and researchers, but is not a panacea. Patients have been taught to self-monitor using paper-based forms, and recently, computerized versions of the forms for handheld devices have been developed and validated against traditional paper-based versions. Unfortunately, the efficacy of self-monitoring systems has inherent issues. There is therefore, considerable value in enhancing self-monitoring systems with ambient-monitoring solutions to detect depressive prodromes early enough to intervene, reduce the effort required by patients and care providers to monitor effectively through ambient monitoring, and monitor physiological and contextual details.

The Personalized Ambient Monitoring System (PAMS) [2] will be used to investigate the feasibility of reducing the incidence of debilitating episodes through personalized ambient monitoring of patients in their homes. In Personalized Ambient Monitoring System i will collect patient activity signatures in an ambient and unobtrusive manner. It is planned to deploy miniature physiological and environmental sensors, worn by patients, and placed in their homes to collect the data. A "PAMS" solution could provide patients and clinicians with greater insights into the patterns of mental illnesses. Patients could be given control over the monitoring system via their mobile phones, or other handheld devices. These devices could be used as gateways to relay important information and alerts from the sensors to the patients and their care providers, and to program and monitor the network. Sensor readings could be fused with self-reported data from electronic forms, and augment existing systems. The ambient collection of signature data could be supported by a wireless sensor network (WSN) infrastructure, and a programming architecture that allows the development of novel, context-aware, adaptive sensor configurations.

PROPOSED WORK

The following sensor network infrastructure is proposed for ambient mental health data collection and

reporting meaningful information to patients and care providers. This system is based on wireless communication. Wireless sensor networks (WSN) have various dimensions and no single solution has been provided to cover every aspect.

I. CHARACTERISTICS OF THE PAMS WSN

A collection of sensing nodes will be used to collect data from different types of sensors, identify behavioral signatures in real-time, and transfer wirelessly the signature information. Sensing nodes can communicate with each other and a mobile gateway that relays data between the network of sensors and the Internet. Sensing nodes are composed of three types of components: communications transceivers, sensors, and ultra-small computing boards featuring power source, limited memory, and I/O connections.

This model addresses a number of characteristics including: the sensing platform's form factor and resource constraints, mobility, connectivity and coverage requirements, communication modality and network topology, deployment methodology and system lifetime, service quality constraints.

The sensors used will vary from patient to patient and the software architecture will allow the registration and substitution of a wide variety of devices. Whilst the sensors will be heterogeneous, we expect that the nodes will have homogeneous characteristics including processors, memory and transceivers. Each node will have a matchbox size form factor, have a radio-based communication modality, and have enough computing resources to support the behavior processing and middleware. The deployment of the nodes will be handled manually by technicians in accordance to service level contracts agreed to by patients and care providers. The types, numbers and positions of the nodes may change over time. The lifetime of the system is expected to be long term.

The network will adapt to partial, occasional and passive node mobility. Some of the sensing nodes will be deployed in the patients' living

environments and some will be worn or carried. Sparse coverage of the areas of interest may result in node isolation and limit communication to intermittent levels as the mobile gateway passes within range of isolated nodes.

II. THE PERSONAL AMBIENT MONITORING SYSTEM INFRASTRUCTURE

The Personal Ambient Monitoring System Infrastructure (PAMSI) displayed in figure 1 fuses body sensor data, environmental data and patient-reported data. The results are recorded securely in a long-term data store and can be examined by health care professionals. Technicians will also be able to access the network for maintenance purposes. PAMSI is composed of five key technologies: the body sensing platform, wireless environmental sensors deployed in the home and other patient monitoring environments, the network gateway, an ad hoc communications network, and the query stations.

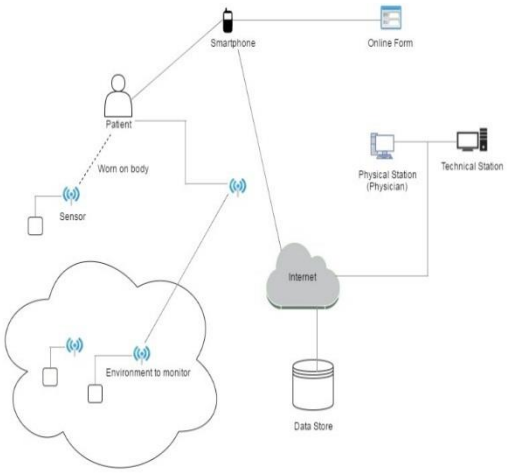


Figure 1

III. BODY SENSING

Body sensor networks (BSN) [3] have emerged as a technology to incorporate sensors located within the personal area of an individual. The sensors can be used to track physiological data such as heart rate and blood oxygen levels, as well as contextual information such as light levels and user motion tracked through accelerometers. Sensing nodes can be worn by patients and used to track changes to physiology. BSN technology is still experimental and active research topics include power-management related issues, signal processing, security, data-fusion and decision support.

IV. ENVIRONMENTAL SENSING

Sensors in the patient environment can be used to track conditions such as light levels and temperature, and be used to track patient behavior in the environment. This can be accomplished by monitoring how the patient moves through their homes, and the ways they perform their activities of daily living (ADL). Multiple sensing nodes can be placed in the environment and can use different sensors, for different tracking tasks.

V. THE NETWORK GATEWAY

Sensing nodes need somewhere to communicate data to and also need to receive updates to their operating procedures. In PAMI, this information gets routed via a mobile gateway to the network. Monitoring instructions and application rules are routed from physician and technician stations to the gateway. The gateway, deployed on the patient's mobile phone, includes software and a sink node radio that allows a standard smartphone to communicate with the sensing nodes. All communication between the gateway and the Internet must be secure and private.

VI. QUERY STATIONS

Clinicians need to monitor their patients, and technicians need to make sure that the monitoring equipment and network is operational. In order to meet these needs, applications will be developed to alter monitoring patterns and query historical patient data, as well as report the current state of the system.

VII. MIDDLEWARE PROTOCOLS

To perform monitoring, maintenance, and data fusion tasks, we will need to develop sensor network protocols. These protocols might be implemented on top of existing WSN middleware [4] such as COUGAR, or employ middleware solutions involving OSGi, EQUATOR's EQUIP platform, or a custom made solution.

The Sensor Management Protocol (SMP) [5] will regulate the data aggregation, time synchronization, and secure data transmission. SMP will also report the state of the sensors and control the systems on/off state.

EXPECTED OUTCOME(S)

i. Feasibility check of present day body sensors such as Micra 85.

ii. Impact of Body Implantable Sensors on the bodies of patients trialed.

iii. The need of Task Assignment & Data Advertisement protocols for sharing of data between sensor nodes and terminals.

iv. Feasibility check of Sensor Factor(s) such as Specific Absorption Rate (SAR) on the bodies of patients trialed.

v. Communication modality required for Body Area Networks.

vi. Finding of Power Dissipation factor in Body wearable & Body Implantable Sensors.

vii. BSN characteristics such as sensing platform form factor, mobility and network topology, security and data fusion; and decision support should also be addressed with the implementation of the proposed research work.

REFERENCES

1. Smith AL, Weissman MM. Epidemiology. In: Paykel ES, ed. Handbook of Affective Disorders. 2nd ed. New York, NY:The Guilford Press; 1992: 111-129.

2. A. Jurik and A. Weaver, "Remote Medical Monitoring," *Computer*, Apr. 2008, pp. 96-99.

3. T.G. Zimmerman, "Wireless Networked Digital Devices: A New Paradigm for Computing and Communication," *IBMSystems J.*, vol. 38, no. 4, 1999, pp. 566-574.

4. WassimMasri., ZoubirMammeri., "Middleware for Wireless Sensor Networks: A Comparitive analysis," IFIP International Conference on Network and parallel Computing workshops Pages349-356 (2007).

5. Cuevas-Martinez, J.C.; Gadeo-Martos, M.A.; Fernandez-Prieto, J.A.; Canada-Bago, J.; Yuste-Delgado, A.J. Wireless Intelligent Sensors Management Application Protocol-WISMAP. Sensors 2010, 10, 8827-8849

Big Data – The New Oil of 21st Century

Neetu Narang Mahajan

INTRODUCTION

Big data is a term that refers to data sets or combinations of data sets whose size (volume), complexity (variability), and rate of growth (velocity) make them difficult to be captured, managed, processed or analyzed by conventional technologies and tools, such as relational databases and desktop statistics or visualization packages, within the time necessary to make them useful. While the size used to determine whether a particular data set is considered big data is not firmly defined and continues to change over time, most analysts and practitioners currently refer to data sets from 30-50 terabytes(10 12 or 1000 gigabytes per terabyte) to multiple petabytes (1015 or 1000 terabytes per petabyte) as big data. Figure No. 1.1 gives Layered Architecture of Big Data System. It can be decomposed into three layers, including Infrastructure Layer, Computing Layer, and Application Layer from top to bottom.

3 VS OF BIG DATA

Volume of data: Volume refers to amountof data. Volume of data stored in enterprise repositories have grown from megabytes and gigabytes to petabytes.

Variety of data: Different types of dataand sources of data. Data variety exploded from structured and legacy data stored in enterprise repositories to unstructured, semi structured, audio, video, XML etc.

Velocity of data: Velocity refers to thespeed of data processing. For time-sensitive processes such as catching fraud, big data must be used as it streams into your enterprise in order to maximize its value.

PROBLEM WITH BIG DATA PROCESSING

I. HETEROGENEITY AND INCOMPLETENESS

When humans consume information, a great deal of heterogeneity is comfortably tolerated. In fact, the nuance and richness of natural language can provide valuable depth. However, machine analysis algorithms expect homogeneous data, and cannot understand nuance. In consequence, data must be carefully structured as a first step in (or prior to) data analysis. Computer systems work most efficiently if they can store multiple items that are all identical in size and structure. Efficient representation, access, and analysis of semi-structured data require further work.

II. SCALE

Of course, the first thing anyone thinks of with Big Data is its size. After all, the word "big" is there in the very name.

Managing large and rapidly increasing volumes of data has been a challenging issue for many decades. In the past, this challenge was mitigated by processors getting faster, following Moore's law, to provide us with the resources needed to cope with increasing volumes of data. But, there is a fundamental shift underway now: data volume is scaling faster than compute resources, and CPU speeds are static.

III. TIMELINESS

The flip side of size is speed. The larger the data set to be processed, the longer it will take to analyze. The design of a system that effectively deals with size is likely also to result in a system that can process a given size of data set faster. However, it is not just this speed that is usually meant when one speaks of Velocity in the context of Big Data. Rather, there is an acquisition rate challenge

IV. PRIVACY

The privacy of data is another huge concern, and one that increases in the context of Big Data. For electronic health records, there are strict laws governing what can and cannot be done. For other data, regulations, particularly in the US, are less forceful. However, there is great public fear regarding the inappropriate use of personal data, particularly through linking of data from multiple sources. Managing privacy is effectively both a technical and a sociological problem, which must

be addressed jointly from both perspectives to realize the promise of big data.

V. HUMAN COLLABORATION

In spite of the tremendous advances made in computational analysis, there remain many patterns that humans can easily detect but computer algorithms have a hard time finding. Ideally, analytics for Big Data will not be all computational rather it will be designed explicitly to have a human in the loop. The new sub-field of visual analytics is attempting to do this, at least with respect to the modeling and analysis phase in the pipeline. In today's complex world, it often takes multiple experts from different domains to really understand what is going on. A Big Data analysis system must support input from multiple human experts, and shared exploration of results. These multiple experts may be separated in space and time when it is too expensive to assemble an entire team together in one room. The data system has to accept this distributed expert input, and support their collaboration.

HADOOP: SOLUTION FOR BIG DATA PROCESSING

Hadoop is a Programming framework used to support the processing of large data sets in a distributed computing environment. Hadoop was developed by Google's MapReduce that is a software framework where an application break down into various parts. The Current AppacheHadoop ecosystem consists of the HadoopKernel, MapReduce, HDFS and numbers of various components like Apache Hive, Base and Zookeeper. HDFS and MapReduce are explained in following points.

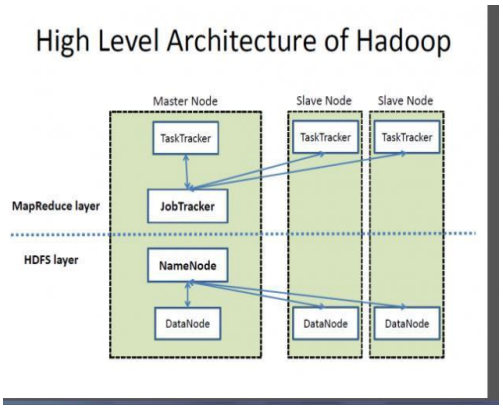


Figure1: Hadoop Architecture

HDFS ARCHITECTURE

Hadoop includes a fault-tolerant storage system called the Hadoop Distributed File System, or HDFS. HDFS is able to store huge amounts of information, scale up incrementally and survive the failure of significant parts of the storage infrastructure without losing data. Hadoop creates *clusters* of machines and coordinates work among them. Clusters can be built with inexpensive computers. If one fails, Hadoop continues to operate the cluster without losing data or interrupting work, by shifting work to the remaining machines in the cluster. HDFS manages storage on the cluster by breaking incoming files into pieces, called "blocks," and storing each of the blocks redundantly across the pool of servers. In the common case, HDFS stores three complete copies of each file by copying each piece to three different servers.

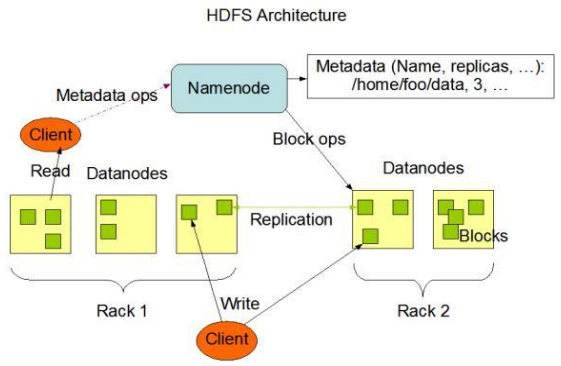


Figure 2: HDFS Architecture

MAPREDUCE ARCHITECTURE

The processing pillar in the Hadoop ecosystem is the MapReduce framework. The framework allows the specification of an operation to be applied to a huge data set, divide the problem and data, and run it in parallel. From an analyst's point of view, this can occur on multiple dimensions. For example, a very large dataset can be reduced into a smaller subset where analytics can be applied. In a traditional data warehousing scenario, this might entail applying an ETL operation on the data to produce something usable by the analyst. In Hadoop, these kinds of operations are written as MapReduce jobs in Java. There are a number of higher level languages like Hive and Pig that make writing these programs easier. The outputs of these jobs can be written back to either HDFS or placed in a traditional data warehouse.

MAPREDUCE :PROGRAMMING MODEL

There are two functions in MapReduce as follows:

map–the function takes key/value pairs asinput and generates an intermediate set of key/value pairs

reduce–the function which merges all theintermediate values associated with the same intermediate key.

The input of a HadoopMapReduce job is a set of key-value pairs (k, v) and the map function is called for each of these pairs. The Map function produces zero or more intermediate key-value pairs (k′, v′). Then, the HadoopMapReduce framework groups these intermediate key-value pairs by intermediate key k′ and calls the reduce function for each group. Finally, the reduce function produceszero or more aggregated results. The beauty of HadoopMapReduce is that users usually only have to define the map and reduce functions. The framework takes care of everything else such as parallelisation and failover.

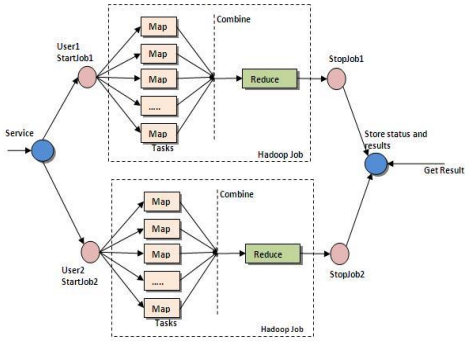


Figure3 MapReduce Architecture

MAPREDUCE: EXECUTION OVERVIEW

The *Map* invocations are distributed across multiple machines by automatically partitioning the input data into a set of M *splits*. The input splits can be processed in parallel by different machines. *Reduce* invocations are distributed by partitioning the intermediate key space into R pieces using a partitioning function (e.g., hash(key) mod R). The number of partitions (R) and the partitioning function are specifed by the user. Below, Figure 4 shows the overall _ow of a MapReduce operation in our implementation. When the user program calls the MapReduce function, the following sequence

of actions occurs (the numbered labels in Figure 4 correspond to the numbers in the list below):

EXECUTION OVERVIEW

1. The MapReduce library in the user program first splits the input files into M pieces of typically 16 megabytes to 64 megabytes (MB) per piece (controllable by the user via an optional

parameter). It then starts up many copies of the program on a cluster of machines.

2. One of the copies of the program is special the master. The rest are workers that are assigned work by the master. There are map tasks and R reduce tasks to assign. The master picks idle workers and assigns each one a map task or a reduce task.

3. A worker who is assigned a map task reads the contents of the corresponding input split. It parses key/value pairs out of the input data and passes each pair to the user-defined *Map* function. The intermediate key/value pairs produced by the *Map* function are buffered in memory.

4. Periodically, the buffered pairs are written to local disk, partitioned into R regions by the partitioning function. The locations of these buffered pairs on the local disk are passed back to the master, who is responsible for forwarding these locations to the reduce workers.

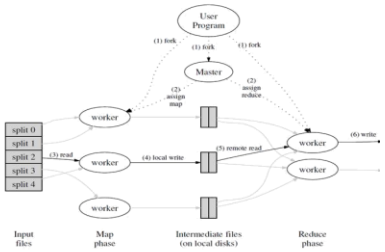


Figure 4

5. When a reduce worker is notified by the master about these locations, it uses remote procedure calls to read the buffered data from the local disks of the map workers. When a reduce worker has read all intermediate data, it sorts it by the intermediate keys so that all occurrences of the same key are grouped together. The sorting is needed because typically many different keys map to the same reduce task. If the amount of intermediate data is too large to fit in memory, an external sort is used.

6. The reduce worker iterates over the sorted intermediate data and for each unique intermediate key encountered, it passes the key and the corresponding set of intermediate values to the user's *Reduce* function. The output of the *Reduce* function is appended to a final output file for this reduce partition.

7. When all map tasks and reduce tasks have been completed, the master wakes up the user program. At this point, the MapReduce call in the user program returns back to the user code.After successful completion, the output of the mapreduce execution is available in the R output files (one perreduce task, with file names as specified by the user).Typically, users do not need to combine these R outputfiles into one file . they often pass these files as input to another MapReduce call, or use them from another distributed application that is able to deal with input that is partitioned into multiple files.

CONCLUSION

We have entered an era of Big Data. The paper describes the concept of Big Data along with 3 Vs, Volume, Velocity and variety of Big Data. The paper also focuses on Big Data processing problems. These technical challenges must be addressed for efficient and fast processing of Big Data.

The challenges include not just the obvious issues of scale, but also heterogeneity, lack of structure, error-handling, privacy, timeliness, provenance, and visualization, at all stages of the analysis pipeline from data acquisition to result interpretation. These technical challenges are common across a large variety of application domains, and therefore not cost-effective to address in the context of one domain alone. The paper describes Hadoop which is an open source software used for processing of Big Data. The MapReduce programming model has been successfully used at Google for many different purposes. We attribute this success to several reasons. First, the model is easy to use, even for programmers without experience with parallel and distributed systems, since it hides the details of parallelization, fault-tolerance, locality optimization, and load balancing. Second, a large variety of problems are easily expressible as MapReduce computations.

Reinforcement Learning

Ruchi Sharma

INTRODUCTION

Reinforcement learning is learning what to do--how to map situations to actions--so as to maximize a numerical reward signal. The learner is not told which actions to take, as in most forms of machine learning, but instead must discover which actions yield the most reward by trying them. In the most interesting and challenging cases, actions may affect not only the immediate reward but also the next situation and, through that, all subsequent rewards. These two characteristics--trial-and-error search and delayed reward--are the two most important distinguishing features of reinforcement learning.

FEATURES OF REINFORCEMENT LEARNING

Reinforcement learning is defined not by characterizing learning methods, but by characterizing a learning *problem*. Any method that is well suited to solving that problem, we consider to be a reinforcement learning method. Clearly, such an agent must be able to sense the state of the environment to some extent and must be able to take actions that affect the state. The agent also must have a goal or goals relating to the state of the environment. The formulation is intended to include just these three aspects--sensation, action, and goal--in their simplest possible forms without trivializing any of them.

Reinforcement learning is different from *supervised learning*, the kind of learning studied in most current research in machine learning, statistical pattern recognition, and artificial neural networks. Supervised learning is learning from examples provided by a knowledgeable external supervisor. This is an important kind of learning, but alone it is not adequate for learning from interaction. In interactive problems it is often impractical to obtain examples of desired behaviour that are both correct and representative of all the situations in which the agent has to act. In uncharted territory--where one would expect learning to be most beneficial--an agent must be able to learn from its own experience.

One of the challenges that arise in reinforcement learning and not in other kinds of learning is the trade-off

between exploration and exploitation. To obtain a lot of reward, a reinforcement learning agent must prefer actions that it has tried in the past and found to be effective in producing reward. But to discover such actions, it has to try actions that it has not selected before. The agent has to *exploit* what it already knows in order to obtain reward, but it also has to *explore* in order to make better action selections in the future. The dilemma is that neither exploration nor exploitation can be pursued exclusively without failing at the task. The agent must try a variety of actions *and* progressively favour those that appear to be best. On a stochastic task, each action must be tried many times to gain a reliable estimate its expected reward. The exploration-exploitation dilemma has been intensively studied by mathematicians for many decades. For now, we simply note that the entire issue of balancing exploration and exploitation does not even arise in supervised learning as it is usually defined.

Another key feature of reinforcement learning is that it explicitly considers the *whole* problem of a goal-directed agent interacting with an uncertain environment. This is in contrast with many approaches that consider sub problems without addressing how they might fit into a larger picture. For example, we have mentioned that much of machine learning research is concerned with supervised learning without explicitly specifying how such an ability would finally be useful. Other researchers have developed theories of planning with general goals, but without considering planning's role in real-time decision-making, or the question of where the predictive models necessary for planning would come from. Although these approaches have yielded many useful results, their focus on isolated sub problems is a significant limitation.

A good way to understand reinforcement learning is to consider some of the examples and possible applications that have guided its development.

- A master chess player makes a move. The choice is informed both by planning--anticipating possible replies and counter replies--and by immediate,

intuitive judgments of the desirability of particular positions and moves.

- An adaptive controller adjusts parameters of a petroleum refinery's operation in real time. The controller optimizes the yield/cost/quality trade-off on the basis of specified marginal costs without sticking strictly to the set points originally suggested by engineers.
- A gazelle calf struggles to its feet minutes after being born. Half an hour later it is running at 20 miles per hour.
- A mobile robot decides whether it should enter a new room in search of more trash to collect or start trying to find its way back to its battery recharging station. It makes its decision based on how quickly and easily it has been able to find the recharger in the past.
- Phil prepares his breakfast. Closely examined, even this apparently mundane activity reveals a complex web of conditional behavior and interlocking goal-sub goal relationships: walking to the cupboard, opening it, selecting a cereal box, then reaching for, grasping, and retrieving the box. Other complex, tuned, interactive sequences of behaviour are required to obtain a bowl, spoon, and milk jug. Each step involves a series of eye movements to obtain information and to guide reaching and locomotion. Rapid judgments are continually made about how to carry the objects or whether it is better to ferry some of them to the dining table before obtaining others. Each step is guided by goals, such as grasping a spoon or getting to the refrigerator, and is in service of other goals, such as having the spoon to eat with once the cereal is prepared and ultimately obtaining nourishment.

These examples share features that are so basic that they are easy to overlook. All involve *interaction* between an active decision-making agent and its environment, within which the agent seeks to achieve a *goal* despite *uncertainty* about its environment. The agent's actions are permitted to affect the future state of the environment (e.g., the next chess position, the level of reservoirs of the refinery, the next location of the robot), thereby affecting the options and opportunities available to the agent at later times. Correct choice requires taking into account indirect, delayed

consequences of actions, and thus may require foresight or planning.

At the same time, in all these examples the effects of actions cannot be fully predicted; thus the agent must monitor its environment frequently and react appropriately. For example, Phil must watch the milk he pours into his cereal bowl to keep it from overflowing. All these examples involve goals that are explicit in the sense that the agent can judge progress toward its goal based on what it can sense directly. The chess player knows whether or not he wins, the refinery controller knows how much petroleum is being produced, the mobile robot knows when its batteries run down, and Phil knows whether or not he is enjoying his breakfast.

In all of these examples the agent can use its experience to improve its performance over time. The chess player refines the intuition he uses to evaluate positions, thereby improving his play; the gazelle calf improves the efficiency with which it can run; Phil learns to streamline making his breakfast. The knowledge the agent brings to the task at the start--either from previous experience with related tasks or built into it by design or evolution--influences what is useful or easy to learn, but interaction with the environment is essential for adjusting behaviour to exploit specific features of the task.

Beyond the agent and the environment, one can identify four main sub elements of a reinforcement learning system: a *policy*, a *reward function*, a *value function*, and, optionally, a *model* of the environment.

A *policy* defines the learning agent's way of behaving at a given time. Roughly speaking, a policy is a mapping from perceived states of the environment to actions to be taken when in those states. It corresponds to what in psychology would be called a set of stimulus-response rules or associations. In some cases the policy may be a simple function or lookup table, whereas in others it may involve extensive computation such as a search process. The policy is the core of a reinforcement learning agent in the sense that it alone is sufficient to determine behaviour. In general, policies may be stochastic.

A *reward function* defines the goal in a reinforcement learning problem. Roughly speaking, it maps each perceived state (or state-action pair) of the environment to a single number, a *reward*, indicating the intrinsic desirability of that state. A reinforcement learning agent's sole objective is to maximize the total reward it receives in the long run. The reward function defines what are the good and bad events for the agent. In a biological system, it would not be inappropriate to identify rewards with pleasure and pain. They are the immediate and defining features of the problem faced by the agent. As such, the reward function must necessarily be unalterable by the agent. It may, however, serve as a basis for altering the policy. For example, if an action selected by the policy is followed by low reward, then the policy may be changed to select some other action in that situation in the future. In general, reward functions may be stochastic.

Whereas a reward function indicates what is good in an immediate sense, a *value function* specifies what is good in the long run. Roughly speaking, the *value* of a state is the total amount of reward an agent can expect to accumulate over the future, starting from that state. Whereas rewards determine the immediate, intrinsic desirability of environmental states, values indicate the *long-term* desirability of states after taking into account the states that are likely to follow, and the rewards available in those states. For example, a state might always yield a low immediate reward but still have a high value because it is regularly followed by other states that yield high rewards. Or the reverse could be true. To make a human analogy, rewards are like pleasure (if high) and pain (if low), whereas values correspond to a more refined and farsighted judgment of how pleased or displeased we are that our environment is in a particular state. Expressed this way, we hope it is clear that value functions formalize a basic and familiar idea.

Rewards are in a sense primary, whereas values, as predictions of rewards, are secondary. Without rewards there could be no values, and the only purpose of estimating values is

to achieve more reward. Nevertheless, it is values with which we are most concerned when making and evaluating decisions. Action choices are made based on value judgments. We seek actions that bring about states of highest value, not highest reward, because these actions obtain the greatest amount of reward for us over the long run. In decision-making and planning, the derived quantity called value is the one with which we are most concerned. Unfortunately, it is much harder to determine values than it is to determine rewards. Rewards are basically given directly by the environment, but values must be estimated and re-estimated from the sequences of observations an agent makes over its entire lifetime. In fact, the most important component of almost all reinforcement learning algorithms is a method for efficiently estimating values. The central role of value estimation is arguably the most important thing we have learned about reinforcement learning over the last few decades.

Although all the reinforcement learning methods we consider in this book are structured around estimating value functions, it is not strictly necessary to do this to solve reinforcement learning problems. For example, search methods such as genetic algorithms, genetic programming, simulated annealing, and other function optimization methods have been used to solve reinforcement learning problems. These methods search directly in the space of policies without ever appealing to value functions. We call these *evolutionary* methods because their operation is analogous to the way biological evolution produces organisms with skilled behaviour even when they do not learn during their individual lifetimes. If the space of policies is sufficiently small, or can be structured so that good policies are common or easy to find, then evolutionary methods can be effective. In addition, evolutionary methods have advantages on problems in which the learning agent cannot accurately sense the state of its environment.

Nevertheless, what we mean by reinforcement learning involves learning while interacting with the environment, which evolutionary methods do not do. It is our belief that

methods able to take advantage of the details of individual behavioural interactions can be much more efficient than evolutionary methods in many cases. Evolutionary methods ignore much of the useful structure of the reinforcement learning problem: they do not use the fact that the policy they are searching for is a function from states to actions; they do not notice which states an individual passes through during its lifetime, or which actions it selects. In some cases this information can be misleading (e.g., when states are misperceived), but more often it should enable more efficient search. Although evolution and learning share many features and can naturally work together, as they do in nature, we do not consider evolutionary methods by themselves to be especially well suited to reinforcement learning problems. For simplicity, in this book when we use the term "reinforcement learning" we do not include evolutionary methods.

The fourth and final element of some reinforcement learning systems is a *model* of the environment. This is something that mimics the behaviour of the environment. For example, given a state and action, the model might predict the resultant next state and next reward. Models are used for *planning*, by which we mean any way of deciding on a course of action by considering possible future situations before they are actually experienced. The incorporation of models and planning into reinforcement learning systems is a relatively new development. Early reinforcement learning systems were explicitly trial-and-error learners; what they did was viewed as almost the *opposite* of planning. Nevertheless, it gradually became clear that reinforcement learning methods are closely related to dynamic programming methods, which do use models, and that they in turn are closely related to state-space planning methods. Modern reinforcement learning spans the spectrum from low-level, trial-and-error learning to high-level, deliberative planning.