ARTIFICIAL ANALYSIS AND COMPUTATION

SMITA GHOSH



BlueRose ONE .com
Stories Matter
NewDelhi • London

BLUEROSE PUBLISHERS
India | U.K.

Copyright © Smita Ghosh 2026

All rights reserved by author. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the author. Although every precaution has been taken to verify the accuracy of the information contained herein, the publisher assumes no responsibility for any errors or omissions. No liability is assumed for damages that may result from the use of information contained within.

BlueRose Publishers takes no responsibility for any damages, losses, or liabilities that may arise from the use or misuse of the information, products, or services provided in this publication.



For permissions requests or inquiries regarding this publication, please contact:

BLUEROSE PUBLISHERS
www.BlueRoseONE.com
info@bluerosepublishers.com
+91 8882 898 898
+4407342408967

ISBN: 978-81-6744-096-9

Cover Design: Ajay Dhyani

First Edition: November 2026

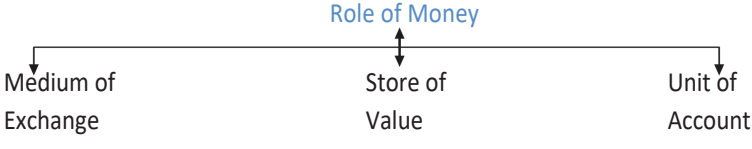
BLOCKCHAIN AND IT'S APPLICATION

1st Author:Smita Ghosh. e-mail : smitaghosh04@gmail.com

ABSTRACT: In this research investigate into the Blockchain Technology ; it's current use and explore other possible implementation of this protocol. Block chain offer opportunities for developing advanced digital services. While current research on this becoming the most important issue which must be well addressed. As part of the fourth industrial revolution since the invention of steam engine, electricity, information technology, Blockchain Technology has been applied in many areas such as finance, judiciary and commerce . This current paper we focused on it's potential Voting Application and explore how Blockchain Technology can be used to solve Health Care Issues, Land Registry, Any Financial Sector etc. Some innovative applications of using blockchain technology for different sectors we also discussed.

Keywords: What is blockchain,Why use blockchain,How blockchain is created, Financial sector favour, Blockchain in voting, Blockchain in healthcare, Blockchain in land-registery.

Introduction :



As first let's know some history of exchange policies :

Credit card : Term 'Credit Card' used by "Edward Bellamy's" science fiction "Looking Backward" in 1887.

Charge plates and credit coins [late 1880s-1960s]

First Bank Card Charge it first National Bank Brooklyn, 1946

Merchant Credit Cards [late 1920s-2000s]

Now what is blockchain ?

Blockchain is the core technology to create "Cryptocurrency" like Bitcoin, through the maintenance of immutable distributed ledgers in thousand of nodes proposed by "Satoshi Nakamoto" in 2008.

"_____a way for one internet user to transfer a unique piece of digital property to another internet user, such that the transfer is guaranteed to be safe and secure, everyone know that the transfer has taken place and nobody can challenge the legitimacy of the transfer_____"

THEINTERNET : CRYPTOGRAPHICPROTOCOL

SSL/TLS – 1996

HTTP -1990

	Amazon	1994
TCP/IP – 1974	CISCO	1984
Ethernet – 1974	3COM	1979

Fundamental of Blockchain Technology:

The technology of Block chain, like the internet, offers a global infrastructure of secure network that may allow the users to make transaction in a way that may allow the users to make transaction in a way that the middleman may be evicted and this making the cost of any transaction to come down. The whole structure of block chain enables a digital ledger of information to be shared within a network, between the distributed nodes.

How blockchain works:

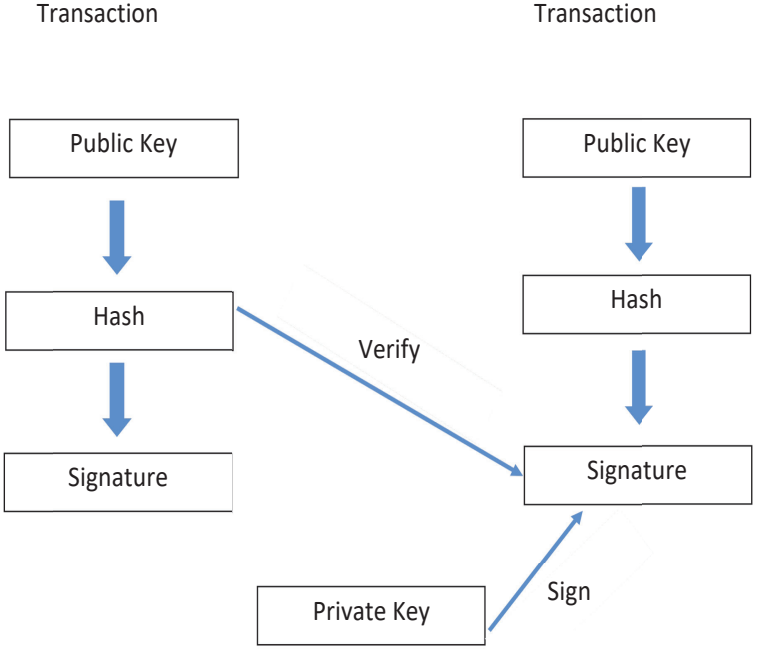
Database : a database is an organized collection of data. A relation database more restrictively is a collection of schemas, table, quires, reports, views and other elements.

Clients → server → database (It's master copy)

1.Private key Cryptography	2.P2p network	3.Program(the block chain protocol)
Cash vs plastic	Tree falls in a forest	Tragedy of the commons
Identity	System of record	Platform

Bitcoin ≠ Blockchain

Online distributing system . Data stores in # is used for identifying any property.



Which Blockchain should i use ?
“Ethereum”

“Ethereum” is global, open-source platform for decentralizes applications on “Ethereum” you can write code that control digital value, runs exactly as programmed and it accessible anywhere in the world.

Which programming language for block chain ?

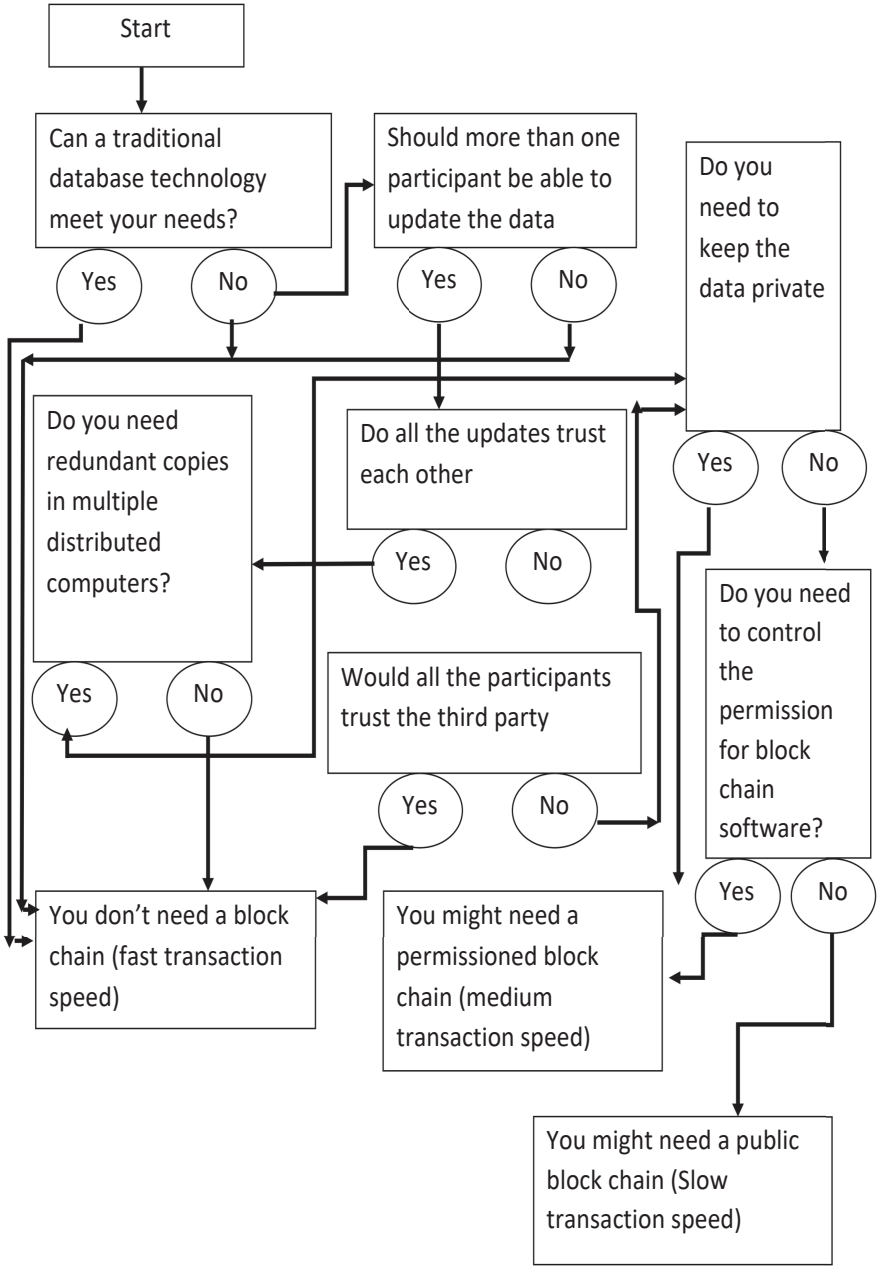
- Solidity c
- java script
- Python
- Go
- Rust
- C++

Solidity : solidity was influenced by c++,python and java script and it’s designed to target the ethereum virtual machine[evm] solidity is statically typed, supports inheritance, libraries and complex used-defined types among other features with solidity you can create contracts for user such as voting, crowd funding, blind auctions and multi-signature wallets.
We deploying contracts, you should use the latest released version of solidity this is because breaking changes as well as new features and bug fixed are introduced regularly. We current is use a o.x version number to indicates the fast pace of change.

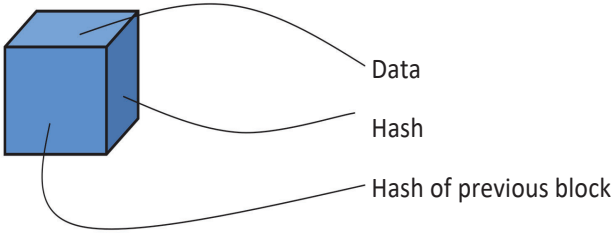
Why use blockchain?

- Transparency/verifiability
- Trust less
- Secure

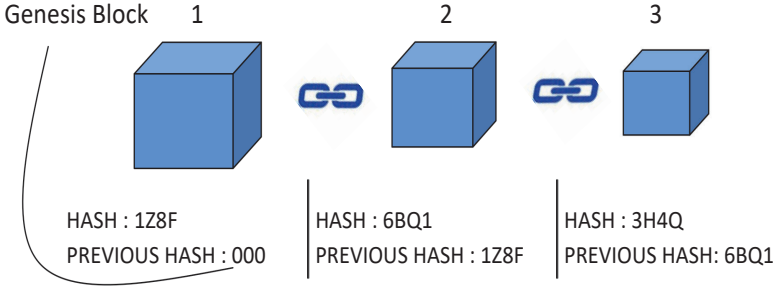
NEED OF BLOCKCHAIN?



HOW TO BLOCK IS CREATED:

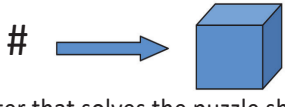


HOW TO BLOCKCHAIN IS CREATED :

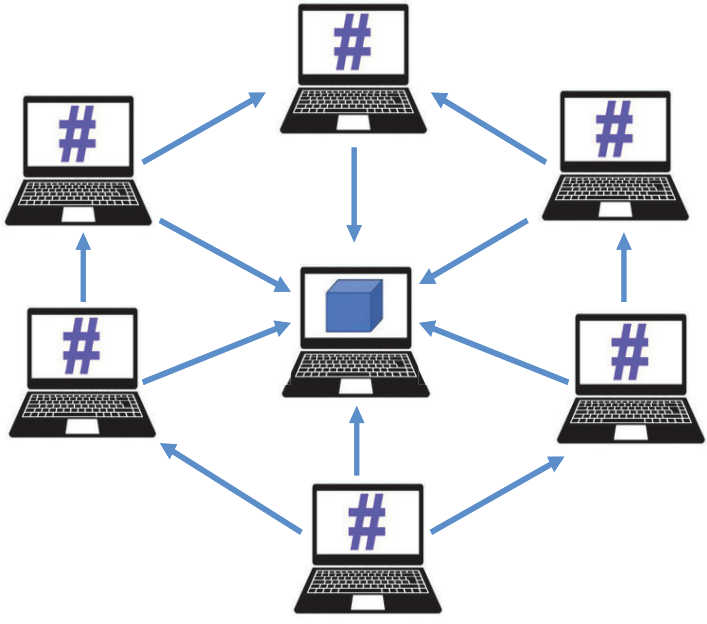


Genesis block computer this days are very fast and can calculate 100- 1000 of # per second. In "Bitcoin" case it take about 10 min to calculate the required proof of work and a new block to the chain . So, let check the process

1. A cryptographic puzzle must be solved, thus creating block



2. The computer that solves the puzzle shares the solution to all the other computers on the network . This is call proof – of – work.



3. The network verified the proof – of – work . If correct , the block will be added to the chain.

The combination of these complex math puzzles are verified by many computers ensures that we can trust each and every block on the chain because the network does the trust building for us we now have opportunity to interact directly without data in real-time and that brings us to the third reason blockchain technology is such a game changer : no more intermediaries.

BLOCKCHAIN APPLICATION

What do people use blockchain for ?

Finance

Crypto currency

Payment

Defi

Supply chain

Digital estate

Real estate

Health care

More!

Finance: Financial sector challenges

Blockchain potential opportunities

Repeated crises and instability

Fiat currency instabilities associated with unsound policies

Centralized intermediaries concentrate risk and economic rents .

Clearing and settlement costs and counterparty risks

Financial inclusion

Pay stem costs : ½ - 1% global G.D.P.

Financial sector costs : 7½ % of us G.D.P.

Financial sector favors :

Permissioned block chain

Vs

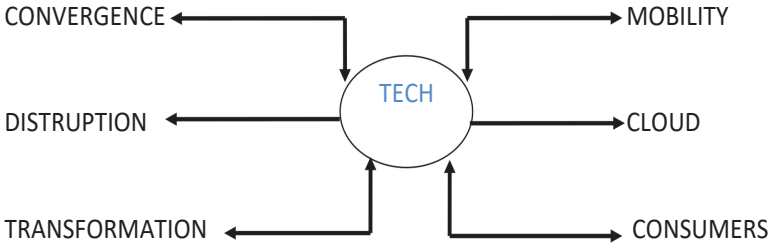
Permission less blockchain

Known set of participants

No proof of work mining

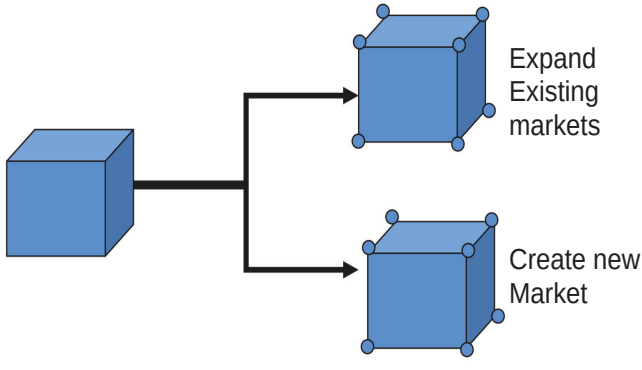
No need for a native currency

Distributed database technology



Transformation

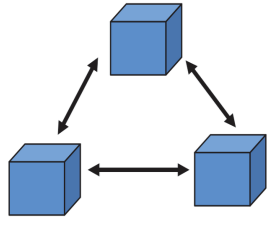
Blockchain technology is revolutionizing the financial services landscape are creating opportunities for both new and established players.



BLOCKCHAIN IN VOTING :

In the current system, Voting is generally done either by writing your opinion on the paper or by electronic voting machine. Replacement of this traditional system is necessary to limit the voting froude and to make the voting as well as the counting process more transparent. Further a system is required the make voting containment for the voters a system that minimizes the cost of conducting elections as money spent on the national election is huge. A system which allows us to vote even when we travelling abroad or are not present in our home state. We are now a

Society that prefers to live online right from ordering food, to booking Cabs, to booking Cabs, to shopping our daily groceries and even finding our life partners. Then why can't we cost our votes ad select our click on a screen? Why can't there be a system where we can vote online through the comfort of our homes. Though many on time voting solution have been proposed in the past but we don't see them in reality. There such online e-voting or remade voting system faces. Let us first have a look at these challenges— Remote electronic voting requires stringent measures for the voting process. Because in this case risk of large scale manipulation is simply too high. There is a risk of hacking activities by hackers who could directly infect and hack the servers. Block chain can
help to implement and electronic voting system that is immutable,
transparent and can not be hacked into

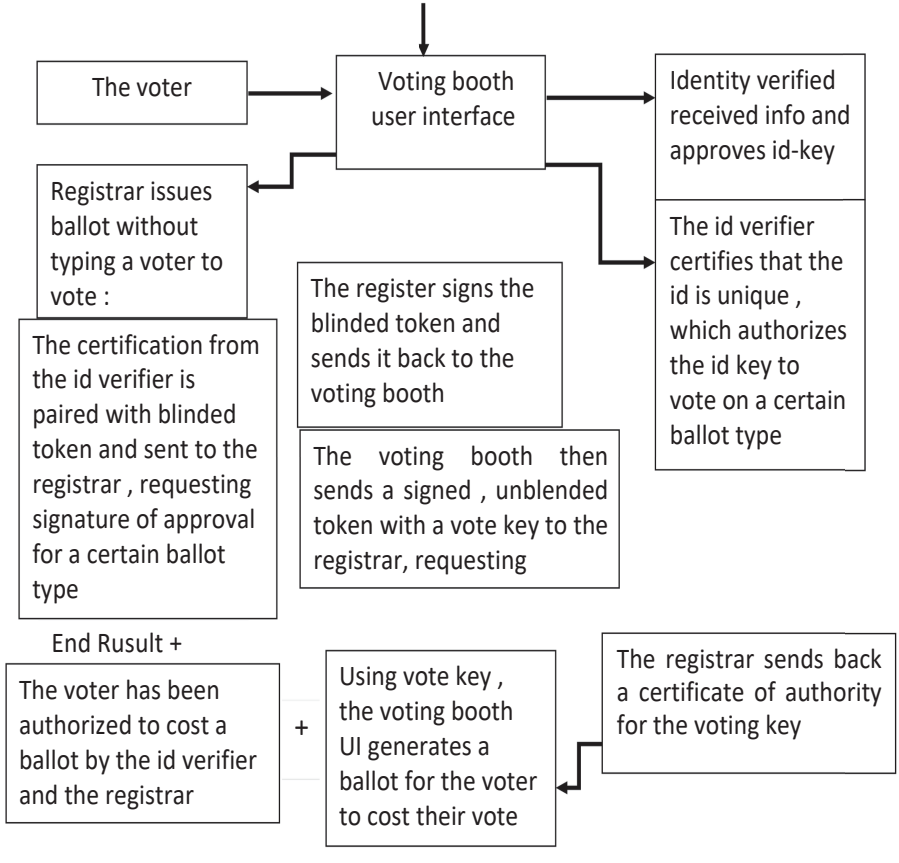


In order to change the results Blockchain voting is an effective means and foremost step in this block chain based voting system is to validate the identity of the voter at is very important to ensure that someone's identity is not being faked because here every vote counts and is epually important. To keep a check an this voter needs to download the remote voting booth on his mobile, laptop or any other smart advice. After that, he needs to submit his identity information which gets verified by the organization conducting these elections. The organization will refer to the details of the registered voters and verified it the person is registered on their database and is eligible to vote. Then all the information of the voter blockchain. After his identities verified, a smart contract will be executed that will issue a ballot so that he can vote and submit it to the ballot box.

Blockchain based voting system will ensure that a user does not vote
multiple times.

Many countries and states are running a pilot to adopt Blockchain Technology for a secure voting system. For example West Virginia, Sierra Leone tested mobile voting through Black chain in 2018. Apart from states elections, this Block chain based voting system could also facilitate, voting processes inside private companies organizations and college elections.

"In democracy was designed with todays technology , what would it look like ?" A firm "horizon state " launched a unique solution to answer the question . The company is currently preparing an ICO. Horizon's secure digital ballot box represents a cost – effective and smart solution to the problems inherent in today's voting procedures.
Now we show how block chain technology can prevent "voter- fraud"



Convenient notification is sent when your ballot is ready

For our design we tried to create a system that doesn't entirely replace the current voting but rather integrates within a current system . We decided to do this to allow for as many different ways to vote as possible ,this is so voting can be accessed by the majority of the population.

Block chain in healthcare :

In the world of healthcare today , there are two major focuses that must be addressed :

- Data security and data ownership
- Sensitive medical records currently lack a secure structure Leading to data breaches with severe consequences .research about block chain and healthcare system is currently limited, but block chain is on the brink of transforming the healthcare system
- The healthcare system is losing $300 billion each year in poor data integration

> " Statistics show that up to one in five patient records are not accurately matched even within the same healthcare system as many as half of the patient records are mismatched when data are transferred between the healthcare " – Shaun Grannis

Why do we care and what do we want?

- Data at right time and place (intro-probability)
- Improve personal treatment outcome
- Advance medical research by enabling precision medicine and AI – driven healthcare
- Patient's privacy guaranteed

Challenges

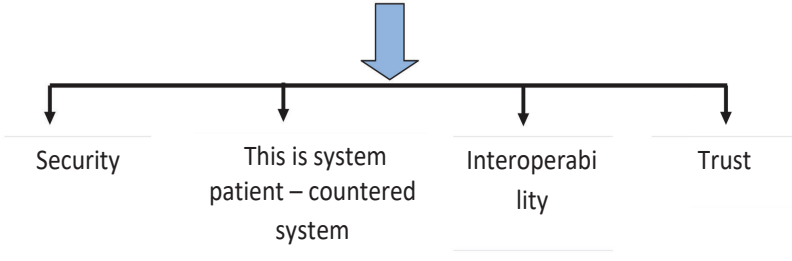
- Achieving interoperability and privacy simultaneously seems contradictory

How to ensure data availability and exchange when required while letting patients to control who can access their data for which purpose

How to effectively prove that patients have given their consent?

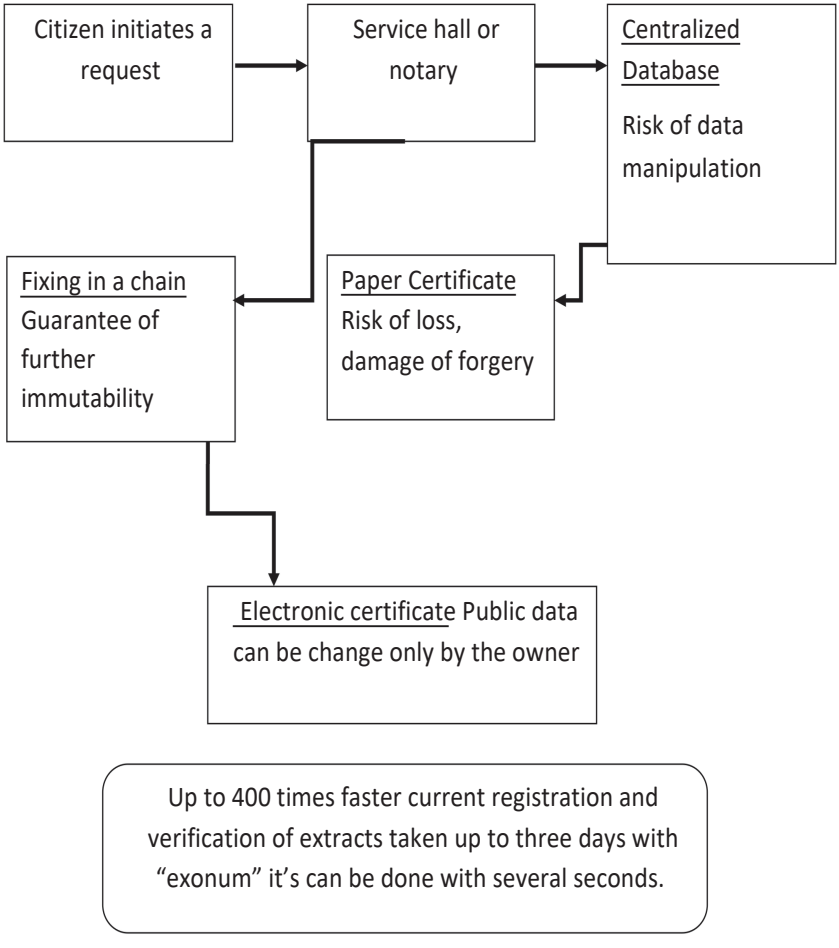
Demo : scenario

Healthcare providers collect information from the patients
The data is stored in exiciting database
A “hash” is created from each source of data and is redirected to the block chain
The patient decides who has access to this medical record
Healthcare stakeholder can query the block chain to access to the information



Block chain in Land Registry: Indian land record system is still inspired by the one introduced by Raja Todarmal (one of the 9 gems in the court of akbar) . This land record maintenance numerous records, each of which would potentially be records could be mutated without the consent of the owner niti aayog recently announced that “block chain technology” will bring out a discussion paper on leveraging this technology for land record management. Andhra Pradesh is currently working with the private firms to secure land records in it’s new capital , Amaravati using Block Chain.

Exonum: the “exonum” platform is a leading block chain framework designed to bring efficiency and security to your operations.



Therefore, Land Registry (Record from National Agency of Public Registry Republic of Georgea)

BEFORE	AFTER
1-3 daysto register property	< 3 minutes To register property
Up to $80 cost of transaction	$8 new transaction cost reduction
10 days for property transfer	Online property transfer
Risk of data loss or modification.	digital certificate
	Stored on public blockchain

Key – outcomes :

3000 Transaction processed	3 min Per transaction	90% Cost optimization

Therefore we may say , making future title searches faster and more efficient with block chain technology

Title in the USA-conveyance :

"peer to peer "+notary

No governmentparticipation

Not include → Taxes
→ Lines
→ Recording

Relatedtobutseparate from : payment / value exchange Escrow.

Title in theUSA–Recording:

"publicnotice"

Govt.Countyrecorder or clerk line and other encumbrances

Optional,sortof

Oftencombinedwith transfer tax and other fees or taxes.

Assessing Block Chains:

1. Permission less and open source
2. Real estate functionality
3. Currency/payment system
4. Proof of work consensus
5. Performance
6. Decentralization
7. Immutability
8. Stability
9. Track record and network affect
10. Price and liquidity (Market cap)

[Date from IRRER]

Action steps :

Buy bit coin on coin base or cash app.

Send to wallet (s)

Mobile - samouri (android) green address (ios)

Desktop (electrum)

Hardware (trazor or ledger)

Get active in IBREA

Some Remarks:

With blockchain , we can imagine a world in which contracts are embedded in digital code and stored in transparent , shared database , where they are protected from deletion , tampering and revision . The parallels between blockchain and TCP/IP are clear . Just as e-mail enabled bilateral massaging bit coin enable bilateral financial transactions . The development and maintenance of block chain is open, distributed and shared just TCP/IP's. A team of volunteers around the world maintains the core software [Harvard business review]. Block chain already has many varied applications , and here's some examples :

1. Bitcoin
2. Spotify
3. Maersky
4. Aeternity
5. Match pool
6. Siemens
7. Loyyal
8. Simply vital health
9. De beers
10. Circle
11. BASF
12. Bit Give
13. Ubiquity
14. Medi Ledger
15. AIA insurance
16. Guts

Conclusion :

Our study has recognized some limitations . First, this paper only analyzed the literature in web of science core collection database (WOS) , which may lead to incompleteness of the relevant liter nature . Second, we filter our literature base on the subject category in wos. In this process , we may have omitted some relevant research . Third, our recommendation have subjective limitations . We hope to unitate more research and discussions to address these paints in the future. Furthermore , we indicated the security and privacy issues have been a central research topic.

The technology of blockchain first emerged during the 2008 financial crises , at a time when people's trust in institutions, in particular financial institutions , was very low , and it came to prominence as the technology underpinning bitcoin cryptocurrency . Now the term 'block chain' itself hides a complex reality.

Reference:

Images of tally sticks @ cambriege university

Continental note @ beyond by ken cc by – sa

Harvard business review

Data from IRRER

MIT "BLOCK CHAIN" lectures by prof. Gary Gensler.

Health Bank - A workbench for Data Science Applications in Health Care

Author : Smita Ghosh (M.sc Mathematics),
WEST BENGAL SCHOOL DEPARTMENT
e-mail : smitaghosh04@gmail.com

Abstract :

Data science is rapidly growing to occupy all the industries of the world today. Medicine and healthcare are two of the most important part of our human Lives. Traditionally, the medicine solely relied on the discretions advised by the doctors.

"Information is the oil of the 21st century, and analytics is the combustion engine." Data generated by every Human Body is 2 TB per day. I am going to let you know how data science touches our daily lives. Everyone would be amazed to know how data Science is transforming our lives through the healthcare sector. Our mission le to educate, inspire and empower leaders to apply exponential technologies to address humanity's grand challenges. clinical Data Repository is a real time database that consolidates data from Ola variety of clinical sources to present a unified view of a single patient. I believe that HEALTH BANK has the potential to promote a growing industry around the development of data science applications. Aggregated data will be fed into a pipeline for open e-access, while non-aggregated data will be provided to researchers within an ethical permission frame work.

Introduction :

IMO 2012 report "Best care of Lower cool" : The Path to continuously Learning Health it care in America."

- Generated and apply the best evidence for the collaborative healthcare choices of each patient and provider

- Drive the process of discovery as a natural out growth of patient care

- Ensure innovations, quality, Safety and value in health care. Requires fundamental commitments to incentives, culture and leadership that foster continuous learning.

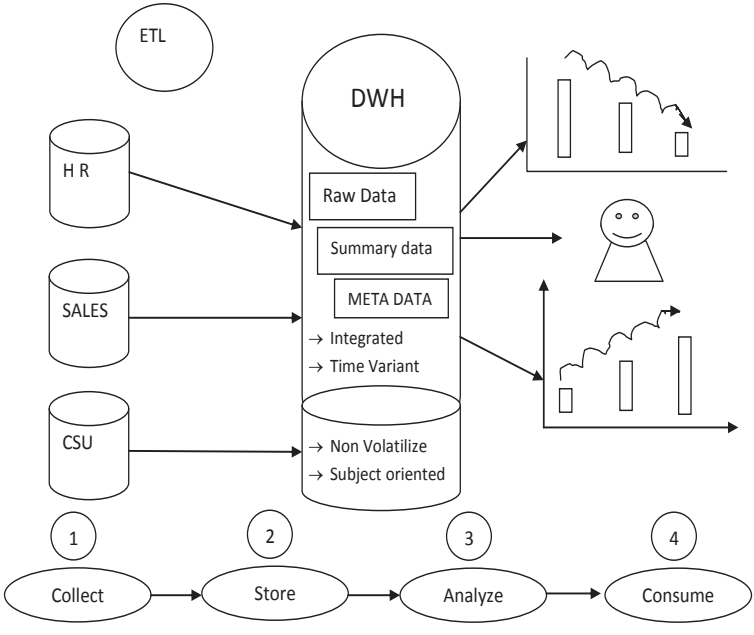
Clinical Data Warehouse

What is Data ware house?

Data ware house is the place where valuable data assets are tire Stored. A data ware house is tee Single source of Data truth.

Defining features of a data warehouse

Subject - Oriented → In data ware house. data is stored by Subject o not by application



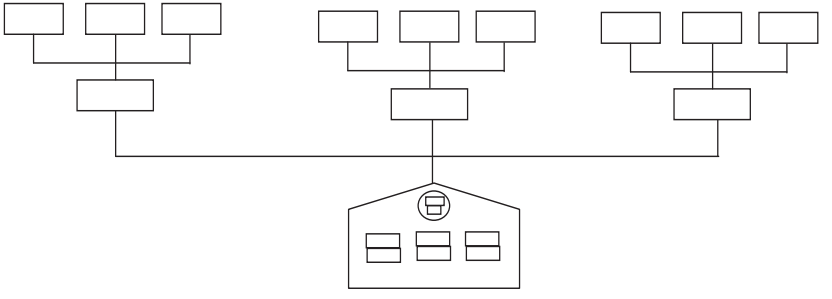
314 e brings Muspell CDR, an integrated FHIR based solutions suite that provides seamless access to all of the patient's data at the point of care in one easy-to-use interface. As you transit to a new EHR, Misspell helps in data archival and data migration in a Seams manner.

SINGLE SOURCE OF TRUTH :

Structuring all the best quality data in one place.

INTEQRATED :

Master Data Governance



Large massive competing and storage System that combine information from several sources into one comprehensive database. Example : Cloud data ware house (oracle , Microsoft, Azure, Google, Big Query)

TIME – VARIANT :

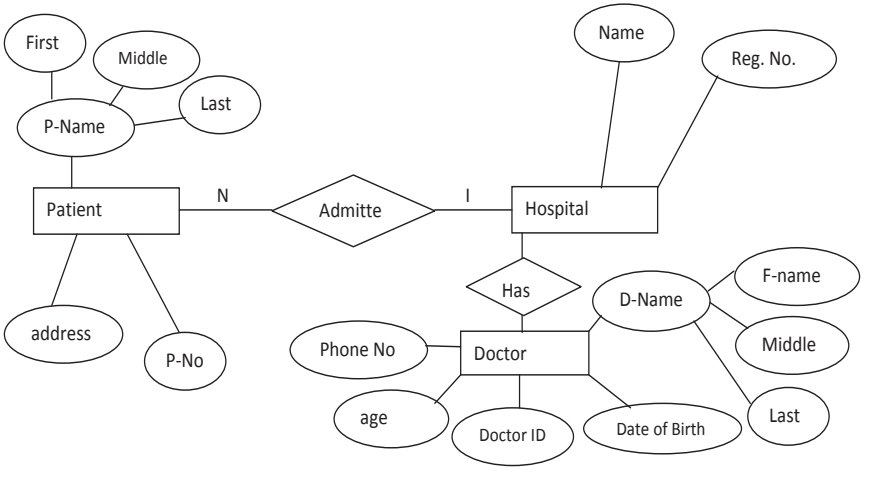
Report from 5 or 10 years ago. (Historical data)

NON VOLATILE :

Can't be changed, can't be deleted

Summarized :

Aggregated or segmented for analysis and reporting.



Hospital ER Diagram (Entity Relationship Diagram)

Entity Relationship model as a tool of conceptual design entities and entity set, set relationship and relationship set, attributes, mapping.

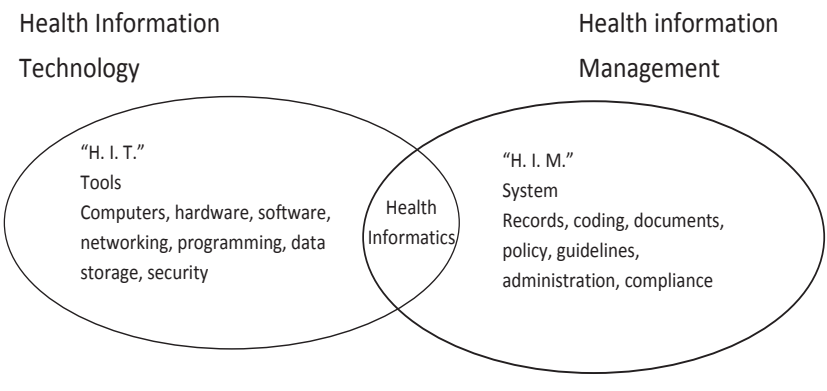
What is the reality?

Different hospitals utilizes varying EHR from different HIS provident. Gap in clinical data exchange with organization that do not share similar platforms. Healthcare data interoperability is the ability of different information technology systems and software applications to communications exchange date and use the information that has been exchanged.

Data - Warehouse is a structural and non-volatile Single Source of truth.

FUNDAMENTAL :

Healthcare informatics, relates to the ecosystem of data and Systems that support operational and clinical workflows rather than the analysis of data found there in



There is a lot of excitement about Data Science and health.

* Artificial intelligence, predictive analytics, precision medicine are all hot areas with huge potential
* A wealth of data is now available in every area of public health and medicine, from new machines and assays, Smart phones, Smart Watches.

* Already, there have been good successes in data science in pathology radiology and other diagnostic Specialties.

Healthcare Analytics :

Analysis of the data to inform decisions, improve quality and performance of the healthcare origination

Increase access to care and decrease costs using business analytic.

Overcome re-imbursement challenges using smart algorithm.

Improve patient outcomes using big data analytics.

Optimize resources using descriptive analytics

Conduct research using advanced analytics.

Improve clinical quality using operational analytics.

Detect fraud using proscriptive and real time analytics.

The Biology in Bioinformatics Genotype :

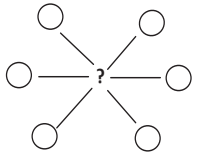
Genotype ⟶ Phenotype



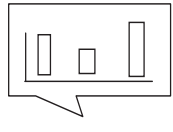
Given DNA and genome sequences, how can we find the genes in the - vast genome? How can we compare What are the Synthetic regions between two genomes are differentially expressed between two Organs or tissues, between tumor and normal tissues, or between two different development stages ? At the level of proteins, how do you identify



Manage data
(Collect store)



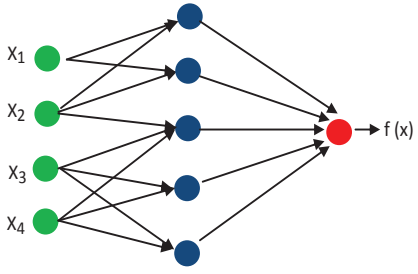
Interpret data
(create Data Model)



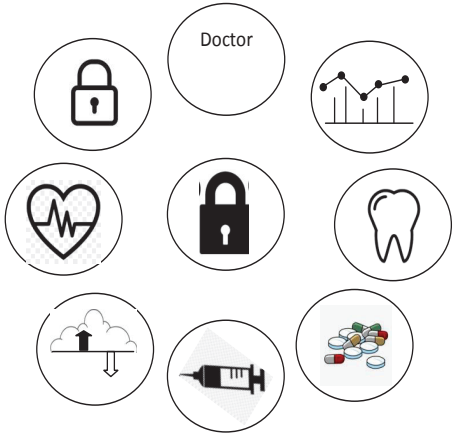
Communicate data
(Code and Classify)

Deep Nets /Deep Learning

(Input layer L1) (Hidden layer L2) (Output layer L3)



Neural network diagram with a single hidden layer. The hidden layer derives transformations of the inputs - nonlinear transformations of linear combinations - which are then used to model the output.



The whole cycle is about Of Epidemiology, Statics, Mathematics, Informatics, computer Science. Health Systems are under pressure to "do more with less ".

- Many more patients needing care.
- Shift to value based care.
- Growing shortage in nurses and physicians.
- increasing consumer expectations of quality and the overall experience

Implications :



Improve Access



Reduce wait time



Reduce Cost

Challenges with Conventional Approaches :

Increase the effective capacity of the health system-new building, expanded facility, extended hours more people.

Benefits

- ❖ Meets the growing demand for healthcare.
- ❖ Puts the capital and human resources capacity and prevent wait times from getting worse.

Challenges

- ❖ Takes months/years to design, build and permit new facilities.
- ❖ Puts pressure on the capital and operating expense budgets.
- ❖ Confronts the real difficulties of identifying and recruiting nurses and providers.

Keys to Accelerating Operational Excellence:

1. **Velocity Matters :**

Excellent service processes have short cycle time.

2. **Demand profiles can be shaped :**

We can bend beams-demand curves can't be harder.

3. **Begin with individual departments :**

Optimize the nodes before worrying about the interconnections.

4. **Co-exist with the existing E H R :**

Build operational optimization on top of the HER not inside it.

5. **Sophists Mathematics is needed :**

It requires serious data science to solve these problems.

Velocity Matters

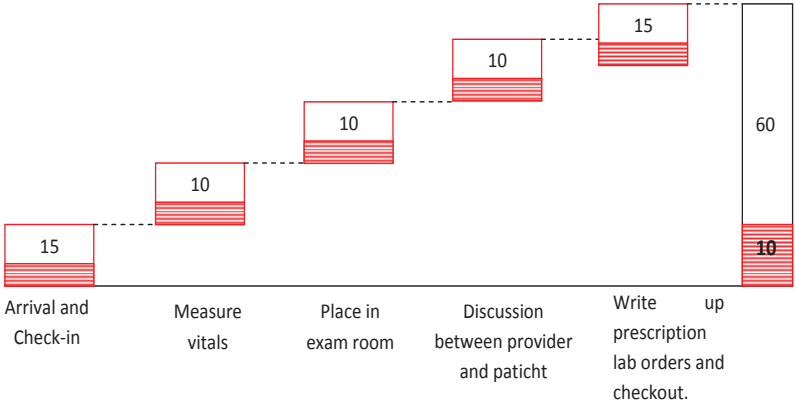
Example :

Typical clinic visit through the time lens.

☐ Non-value--added time

■ Value added time

(Typically, only 10 of the 60 minutes (~11%) of the visit is truly value-adding)

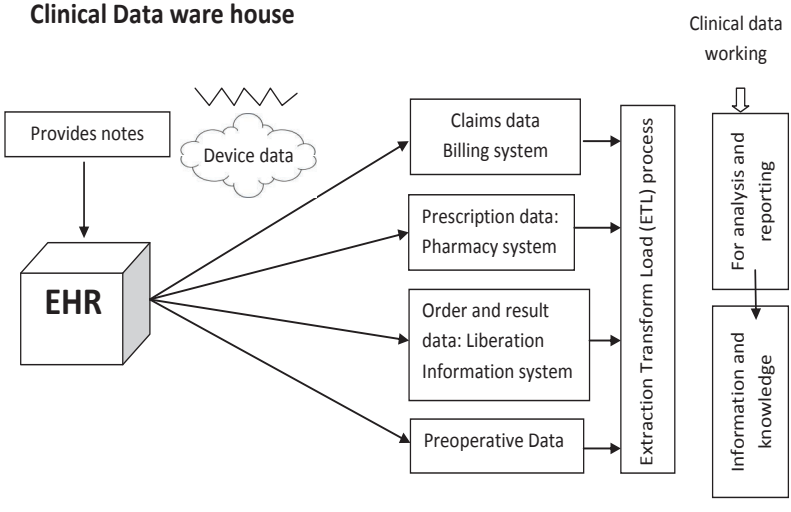


Outcomes of review and research direction :

Improvement leverage is from reducing non-value-added time NOT attempting to make value-adding steps move.

For Clinical use (patient care) :

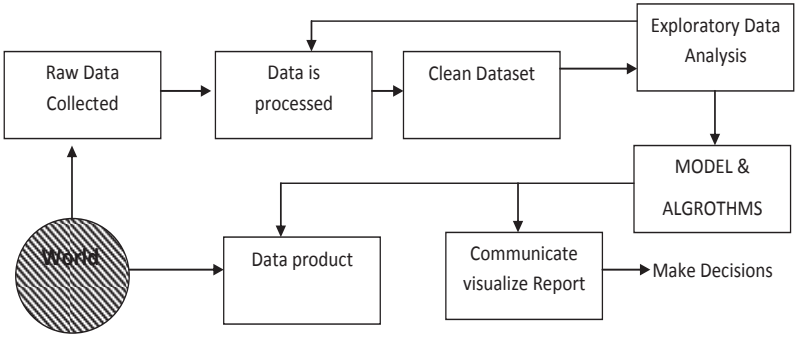
Clinical Data ware house



* Aggregates data for a patient from multiple source.
* CWD used for analysis and reporting , not clinical care.
* Requires an extraction-transform-load process

"The discovery of meaningful patterns in data , and is one of the steps in the data life cycle of collection of raw data, preparation of information analysis of patterns to synthesize knowledge and action to produce value" (NIST Big Data, 2015)

Data Science Process :



- Entire process of data collection, extraction, transformation analysis, interpretation and reporting.
- The analytics processes tee synthesis of Knowledge from information.

Improvement of diagnostic system :

- Diagnostic failures are the reasons for the death of many patients.
- In many cases early diagnosis is the key for survival.
- Image analysis of the CT scans, x-rays, etc.

Genetic Research :

Finding relationship between DNA and diseases.

* Use of Personal genome data.
* Huge data.

Computational drug discovery :

* Drug discovery is time Consuming
* Computational techniques are being used for designing compounds and analyzing chemical interactions.
* Also used for pre-clinical tests and clinical trails using machine learning algorithm.

Early warning signals :

* Colleting important health related data using Wearable.
* Continuously analyze this data to detect potential health issues.

Clinical trails :

* Predicting bioactivity and identify patients characteristics.
* Faster delivery of trial results

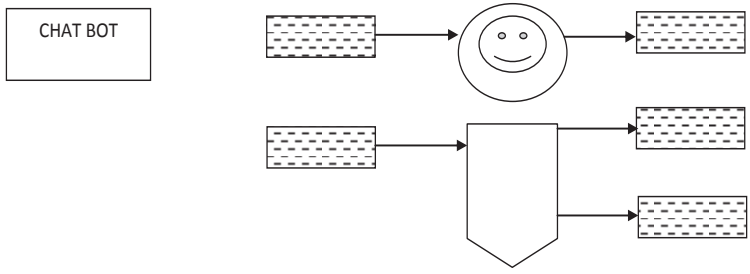
Automation of repetitive processes :

* Automating administrative task.
* Less error prone.
* Faster and more reliable.
* Low cost.

Personalized health Services :

* Collection of clinical and molecular data.
* Algorithm based treatment
* Belter insights available for the doctors.

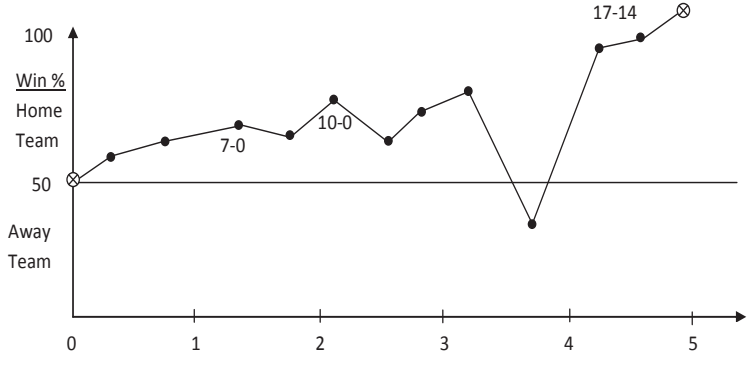
Virtual Assistance for Patients and customer Support. AI powered mobile app doing great job.

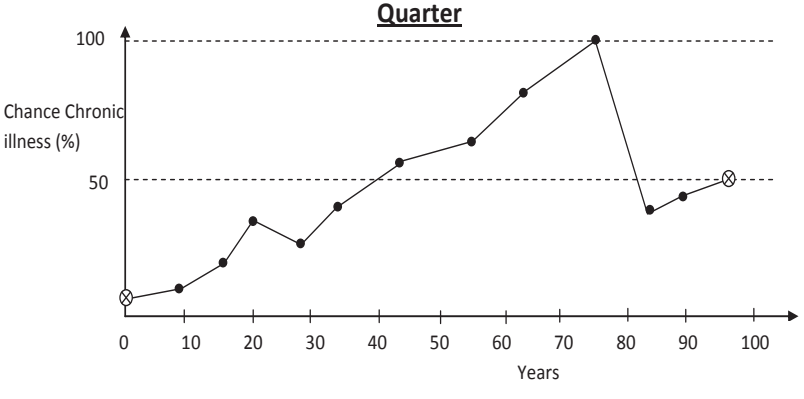


Tell your symptoms it analysis your detection and medication.

Benefits of data Science :

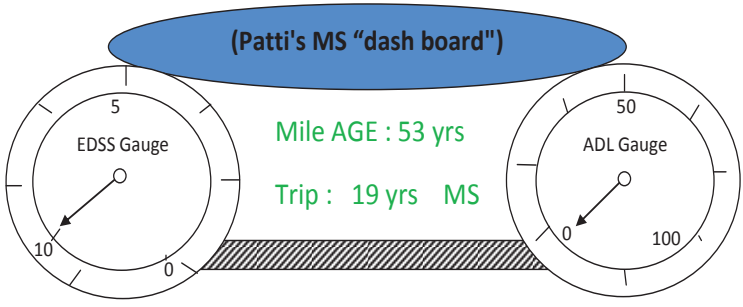
- ❖ Facilitates the easy workflow of the health care system.
- ❖ Reduces the risk of treatment wane failure.
- ❖ It helps to provide proper treatment on time.
- ❖ Early detection of symptoms.
- ❖ Remote monitoring of op symptoms by clinicians.
- ❖ Avoid unnecessary emergency due to the unavailability of doctors.
- ❖ Reduce the waiting time of patients.

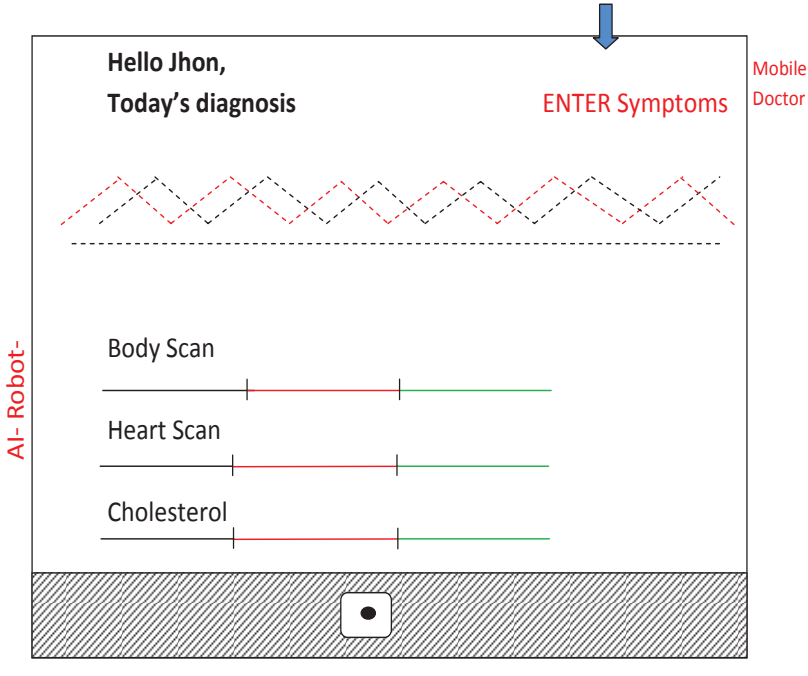




PREDICTALYTICS

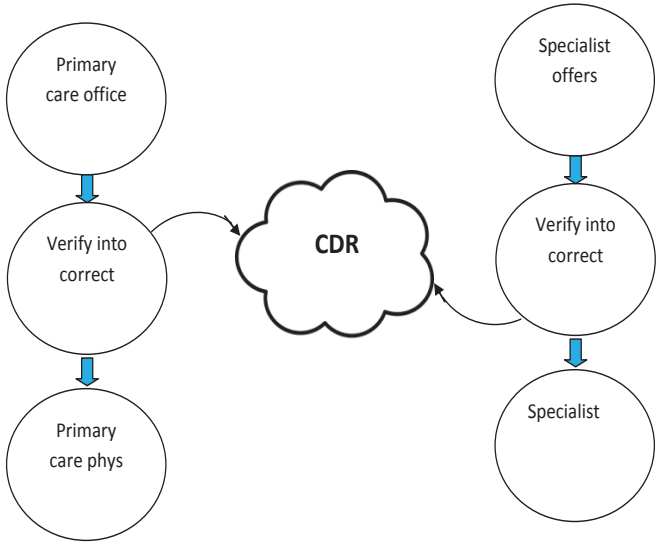
Personal Dashboard for Disease Prediction & Management.





Patients only using this apps and get instant a treatment by own. MR Guided Focused Ultrasound for Image Guided Robotic Acoustic Surgery.

THE SOLUTION :



Building blocks (information components) are transmitted electronically for use in many formats-when assembled, they provide the overall health picture of an individual at a point in time.

Privacy and Security :

- The CDR complies with state and federal security and privacy requirement.
- The CDR has been externally audited for HIPAA and SOC_2 (Service operation Centre) national security standers.
- The level of staff CDR access is based on their role.
- CDR data is classified as normal restricted or very restricted.

Velocity Matters :

VISIBLE

HIDDEN

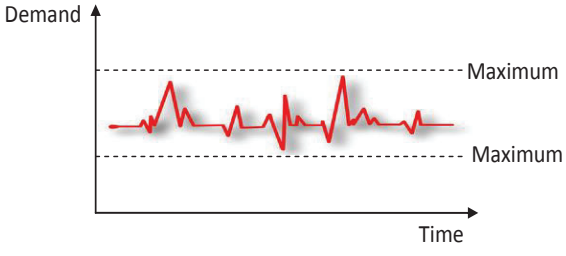
Manufacturing ○ **Inventor**
○ Fore cast accuracy ○ Supplier quality ○ Schedule compliance ○ Production quality ○ Equipment utilization

VISIBLE

HIDDEN

Service Process ○ Cycle Time
○ Staff availability ○ Pre-work accuracy ○ Incomplete orders ○ Equipment availability ○ On-time performance of prior steps

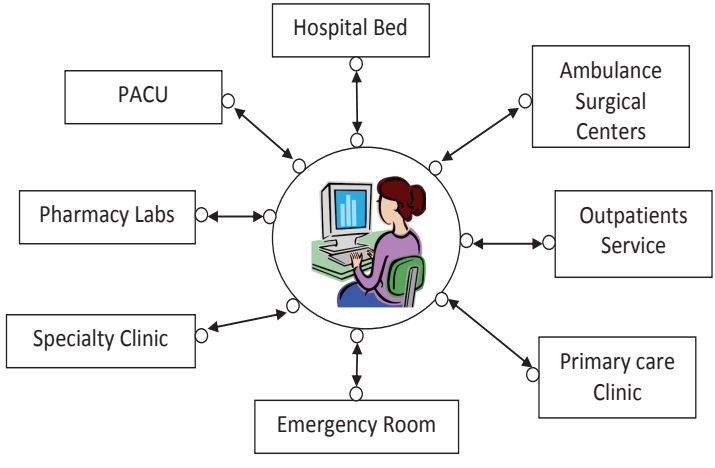
Demand Profile can be shaped :



Forecast the daily demand volume, mix and timing based on historical demand data

Fatten demand profile the Using the lean principle of Heijunka.

Being with individual departments :



Conclusion :

Data Science plays a pivotal role in monitoring patient's health notifying necessary steps to be taken in order to prevent potential diseases from taking place. Data Scientists are using powerful predictive analytical tools to detect chronic diseases at an early level. In many extreme cases, there are instances where due to negligibility, diseases are not caught at an early stage.

This proves to be highly mo detrimental to not only the patient's health but also the economic carts as the disease grows, the cost of curing it also increases. Therefore, data science plays a huge role in optimizing the economic Spending in health care. The emergence of smart phones, mobile apps, ubiquitous, high speed internet and remote monitoring devices (e.g. Sensors) coupled with health System's

implementation My study have recognized some limitation. The future work could be help to improvise the ability of researchers in the field of Science, epidemiological studies, personalized me medicine etc. Data science provides aid to process manage, analyze and assimilate the large quantities of fragmented, structured and unstructured data created by healthcare Systems.

Reference :

1. S, Chansler R (2010) The hadoop distributed file system. In 2010 IEEE 26th symposium on mass storage systems and technologies (MSST) (pp. 1-10). Ieee. https://doi.org/10.1109/MSST. 2010.5496972

2. IBM Corporation (2013) Data. driven healthcare organizations use big data analytics for big gains. https://silo.tips/download/ibm-software-white-paper-datadriven-healthcareorganizations-use-big-dataanaly.

3. Skourletopoulos G et al (2017) Big Data and Cloud Computing: A Survey of the State-of the-Art and Research Challenges. In: Mavromoustakis C, Mastorakis G, Dobre C (eds) Advances in Mobile Cloud Computing and Big Data in the 5G Era. Studies in Big Data, vol 22. Springer, Cham. https://doi.org/10.1007/978-3319-45145-9 2

4. Bashan A, Bartsch RP, Kantelhardt JW, Havlin S, Ivanov PC. Network physiology reveals relations between network topology and physiological function. Nat Commun 2012 Feb 28;3:702 [FREE Full text] [Cross Ref] [Medline]

5. Isard M, Budiu M, Yu Y, Birrell A, Fetterly D. Dryad: distributed data-parallel programs from sequential building blocks. 2007 Presented at: 2nd ACM SIGOPS/EuroSys European Conference on Computer Systems; Mar 21-23, 2007; Lisbon, Portugal.
6. Zaharia M, Chowdhury M, Franklin MJ, Shenker S, Stoica I. Spark: cluster computing with working sets. 2010 Presented at: Hot Cloud '10. 2nd USENIX conference on Hot topics in cloud computing; Jun 22-25, 2010; Boston, MA, USA.

7. Zaharia M, Chowdhury M, Das T, Dave A, Ma J, McCauley M, et al. Resilient distributed datasets: a fault-tolerant abstraction for in-memory cluster computing. 2012 Presented at: 9th USENIX Symposium on Networked Systems Design and Implementation; Apr 25-27, 2012; San Jose, CA, USA.

8. Bonini P, Plebani M, Ceriotti F, Rubboli F. Errors in laboratory medicine. Clin Chem 2002 May;48(5):691-698. [Medline]

9. Schulz W. Nucleus. San Francisco, CA: GitHub, Inc; 2018 Aug 13. URL: https://github.com/Computational Health/nucleus [accessed 2019-02-05] [WebCite Cache]

10. Greaves F, Ramirez-Cano D, Millett C, Darzi A, Donaldson L (2013) Use of sentiment analysis for capturing patient experience from free-text comments posted online. J Med Int Res 15(11):e239. https://doi.org/10.2196/jmir.2 721

11. Kostkova P, Fowler D, Wiseman S, Weinberg JR (2013) Major infection events over 5 years: how is media coverage influencing online information needs of health care professionals and the public?. J Med Int Research 15(7):e107. https://doi.org/10.2196/jmir.2 146

12. Jiang J, Cameron AF, Yang M (2020) Analysis of massive online medical consultation service data to understand physicians' economic return: observational data mining study. JMIR medical informatics 8(2):e16765. https://doi.org/10.2196/16765

13. Harpaz R, Chase HS, Friedman C (2010) Mining multi-item drug adverse effect associations in spontaneous reporting systems. In BMC bioinformatics (Vol. 11, No. S9, p. S7). BioMed Centra. https://doi.org/10.1186/14712105-11-S9-S7

Pattern Recognition

1st Author : Smita Ghosh. e-mail : smitaghosh04@gmail.com

ABSTRACT: "Patter recognition" is the Scientific discipline of machine learning (or Artificial Intelligence) that aims at classifying data (Patterns) into a number of categories of classes." Now what is "Pattern"

1) A "Pattern" is an object, process or event that can be given a name.

2) A Pattern is a set of patterns sharing common attributes and usually originating from the same source. So, Pattern Recognition may be characterized as an information reduction information mapping, or information labeling process. The objective of this paper is a to "Automatic speech and speaker recognition." This research directions will emerge and new techniques will be developed to solve some of the new challenging problems. Pattern Recognition is identifying patterns in data. These Patterns tell the data stories through ebbs and flows , spikes, and flat lines.

The data itself can be anything :

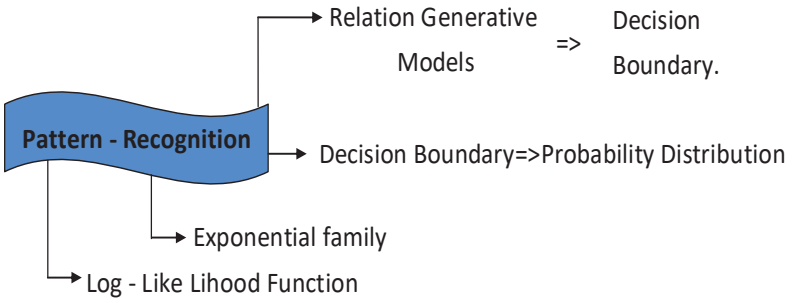
- Text
- Images
- Sounds
- Sentiments and others.

Key words:

Postulates of PR, Evaluation of classifiers, PR Process Acoustic Model output.

Introduction :

We can explain Pattern. Recognition in picture as follows:

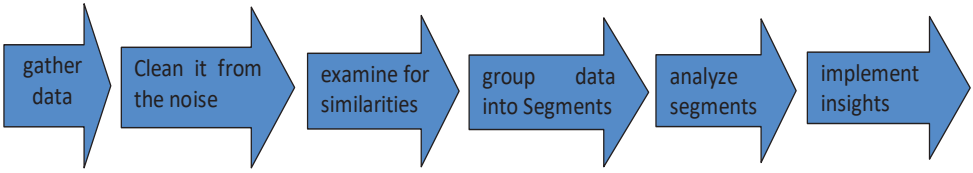


Pattern Recognition is a single blind poor reviewed academic journal published by "Elsevier Science". It was first published in 1968 by "Pergamon Press". The founding editor - in-chief was Robert Ledley, who was succeeded from 2009 until 2016 by Ching Suen of Concordia University, Pattern is everything around in this digital world, A pattern can either be seen physically or it can be observed mathematically by applying algorithms. Pattern recognition can be defined as the classification of data based on knowledge already gained as on statistical information extracted from patterns and / or their representation.

Pattern recognition possesses the following features:

- Pattern recognition System should recognize familiar pattern quickly and accurate.
- Recognize and classify unfamiliar objects.
- Accurately recognize shapes and objects from different angles.
- Identify patterns and objects even. when partly hidden.
- Recognize patterns quickly with ease, and with automaticity. Pattern Recognition is efficient enough to give machines human recognition intelligence. This is used for image processing Segmentation and analysis. For example: Computer can detect different types of insects better than humans. "Christopher Bishop" in his seminal work “Pattern Recognition and Machine Learning” describes the concept like pattern recognition deals with the automatic discovery of regularities in data through the use of computer algorithms and with the use of these regularities to take actions such as classifying the data into different categories.

Pattern Recognition Process



Fundamental of Pattern recognition :

The classic of Pattern recognition we have 6 postulates :

Postulates 1 : Availability of a representative sample W of patterns $^{i}f(x)$ for the given field of problems Ω

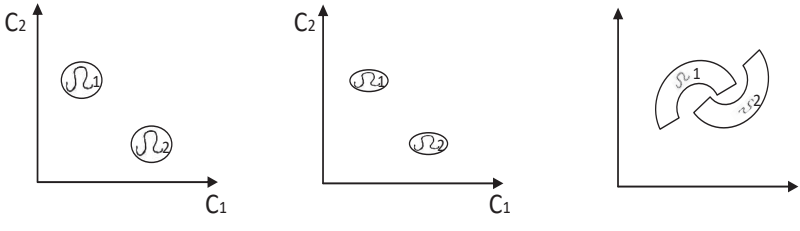
$w = \{^{1}f(x), ..., ^{n}f(x)\} \subset \Omega$

Postulates 2 : A (simple) pattern has features which characterize its membership in a certain class Ω_k.

Postulates 3 : Compact domain in the feature space of features of the same class: domains of different classes are (reasonably) separable.

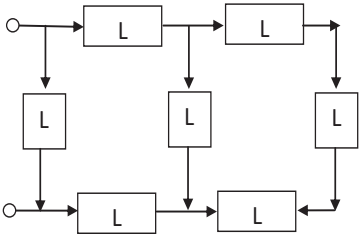
- Small intra - class distance.
- High inter - class distance.

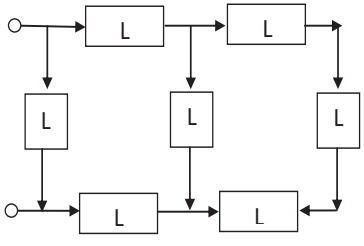
Example of an increasingly less compact domain in the feature space:



Postulates 4 : A (complex) pattern may be decomposed into these constituents.

Postulates 5 : A (complex) pattern f(x) € ℘ has o certain structure. Not any arrangement of simple constituents is a valid pattern. Many patterns may be represents with relatively few constituents.

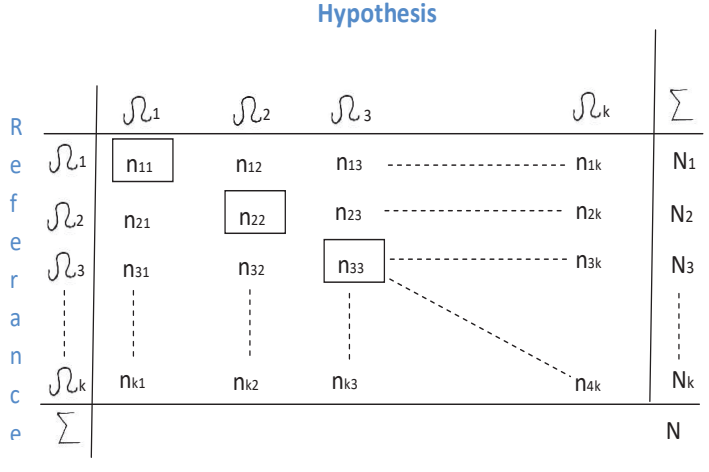




Postulates 6 : Two patterns are similar if their features or simpler constituents differ only lightly.

Performance Evaluation :

- Feature vectors are used as input for the classifier.
- Classification results in a discrete class index.
- Confusion matrix.



confusion matrix with absolute frequencies for a K-class problem.

Evaluation of Classifiers :

- A currency / Recognition Rate - RR $\frac{1}{N} \sum_{K=1}^{K} n_{kk}$ 100%
- Recall and Precision

$$\text{Recall}_k = \frac{n_{kk}}{\sum_{i=1}^{K} n_{ki}} = \frac{n_{kk}}{N_k}$$

$$\text{Precision} = \frac{n_{kk}}{\sum_{i=1}^{K} n_{ik}}$$

- Average Recall

$$\text{UAR} = \frac{1}{K} \sum_{K=1}^{K} \frac{n_{kk}}{N_k} \quad 100\%$$

Special Case : Only 2 classes

	Positive	Negative
Positive	True positive	False positive
Negative	False Negative	True Negative

Various performance measures:

- True positive rate (hit rate, recall, Sensuality): $\frac{\#TP}{\#TP + FN}$
- False positive rate (false alarm rate, fall out): $\frac{\#FP}{\#FP + \#TN}$
- Positive predictive wale (precision) : $\frac{\#TP}{\#TP + \#FP}$

- Negative predictive value : $\frac{\#TN}{\#TN + \#FN}$
- True negative rate (specify): $\frac{\#TN}{\#FP + \#TN}$

  = 1- false positive rate
- Accuracy: ACC = $\frac{\#TP + \#TN}{\#TP + \#FP + \#FN + \#TN}$
- F- measure: Harmonic mean of recall. and precision :

$$F = \frac{2.\ recall.\ precision}{recall + precision}$$

An obvious representation of a pattern will be a vector. Each element of the vector can represent one attribute of the pattern. The first element of the vector will contain the value of the first attribute for the pattern being considered.

Overall, there are two major parts of pattern recognition algorithms:

- explorative - used to recognize commonalities in the data.
- descriptive - used to categorize the commonalities in a certain manner.

There are three main models of Pattern Recognition:

To identify where the specific.

- Statistical: piece belongs. This model uses supervised machine learning.
- Syntactic/Structural: To define a more complex relationship between elements. This model uses same - Supervised machine learning.

- Template matching : To match the object's features with the predefined template and identify the object by proxy. One of the uses of such a model is plagiarism checking.

Pattern Recognition Application :

Speech Recognition :

The greatest success in speech recognition has been obtained using pattern recognition paradigms. It is used in various algorithms of speech recognition which tries to avoid the problems of using a phoneme level of description and treats Larger units such as words as pattern.

Speech recognition has already proven useful for certain application, such as telephone voice- response systems for certain applications, such as telephone voice-response systems for selecting services or information digit recognition for cellular phones and data entry while walking around a railway yard or clambering over a jet engine during an inspection.

So at and first what is “Automatic Speech Recognition?”

Automatic Speech Recognition (ASR) systems accurately translate utterances spoken into text (Words, Syllabus etc). Examples are: You Tube closed captioning, voicemail , transcription, Dictation Systems, Siri front and etc.



Speech Signal Text

With the rise of natural language processing that all changes. But what gives the computer the power to actually understand the exact sounds of the person and make sense out of it all? This is the powerful subfield of Al called Speech Recognition.

What can you infer from speech?

- what can you infer from speech ?
- what is being said?
- what language is being
- spoken?
- Who is speaking ?
- Gender of the speaker
- Age of the speaker
- Emotion

- Stress level
- Cognitive load level
- Depression level
- Is the person sleepy
- Is the person inebriated.

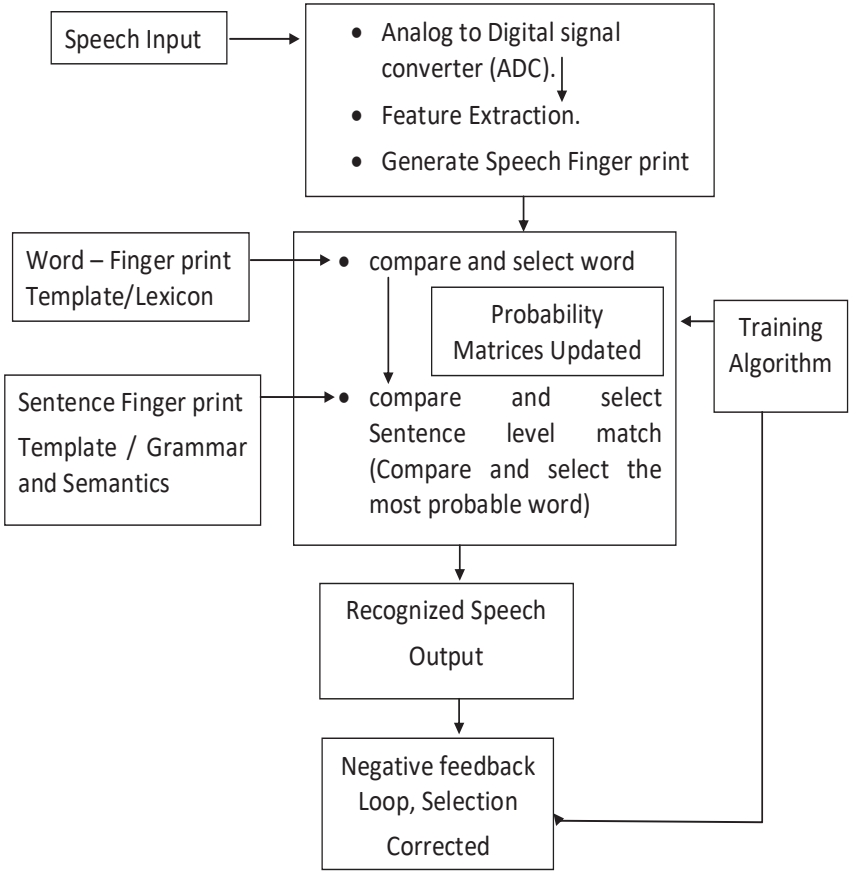
Speech conveys several types of information

- linguistic : message and language information

- Para linguistic : emotional and physiological Characteristics.

Speech Recognition Algorithms :

Almost all SR systems follow some basic structure :

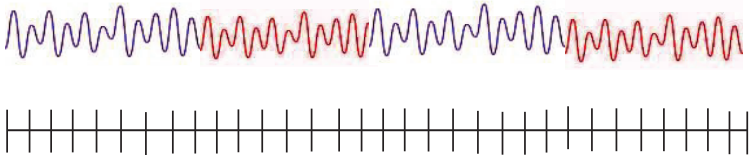


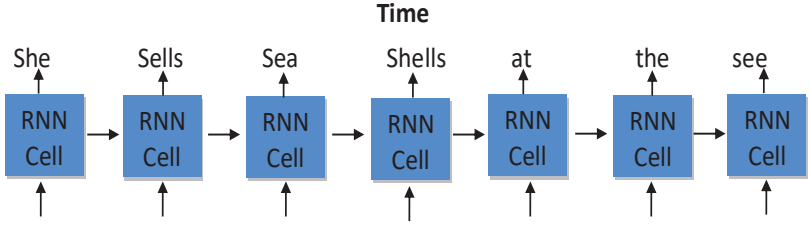
Out comes of review and research direction :

How to Deal with all physical Aspects of speech ?

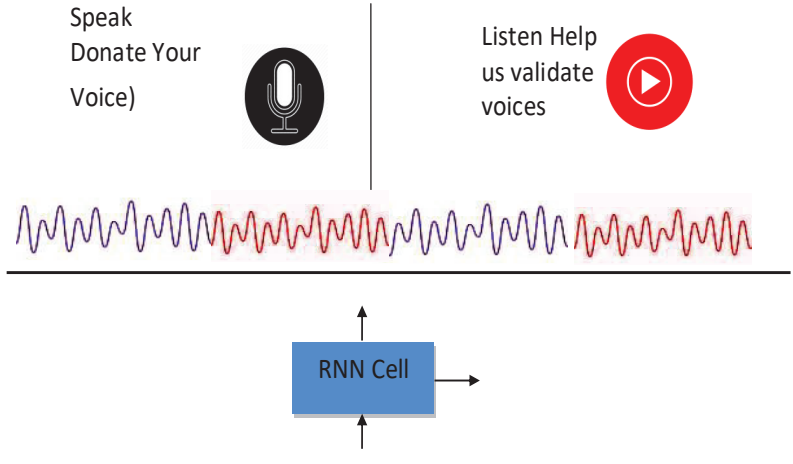
In a Neural Net Requirements:

- process sequential data.
- Low compute
- real time capability



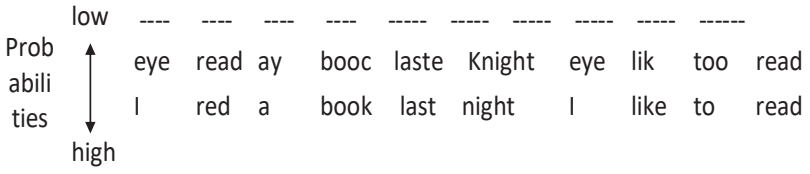


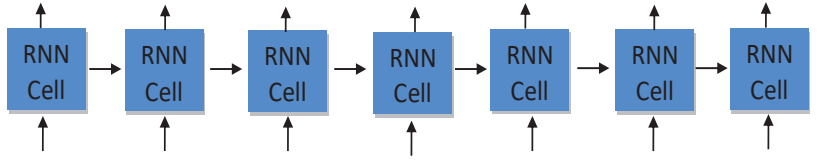
Acoustic Model Approach :



So, now How to deal with Linguistic Aspect?

So, it is Language Model + Rescoring Algorithm



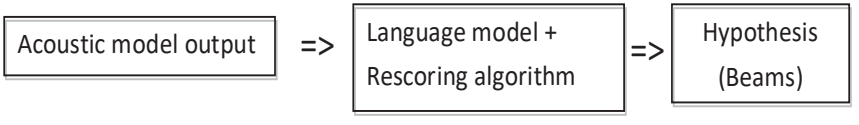




What a more likely Sentence?

Probability (I read a book) = .95

Probability (I red a book) = .25



Therefore hypothesis (beams) outcomes :

Probability (i read a book last night i like to read) = .95

Probability (i red a book last night i like to read) = .35

Probability (i red a book last night i like to reed) = .15

Data Processing Pipeline → It transforming audio waves in mel spectrograms as features to feed it into the neural network. Now transforms our labels into integer indexes. Our network will characters instead of words.

" I read a book "

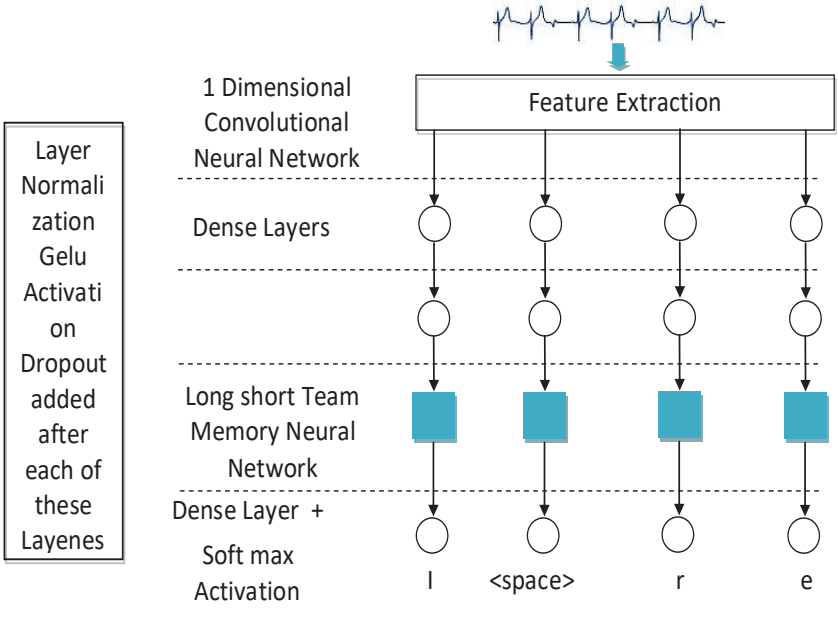
[101 19 65 12 13 16 1612]

Now augment our data to effectively have a bigger dataset



“Spectrogram augmentation " is a the technique randomly cuts out features in time and frequency domain.

Neural Network Model



Most of the memory required for training deep recurrent network is used to store activations through each Layer for use by back propagation, not to store the parameters of the network.

For example : Storing the weights for La **70M parameter network** with a layers requires approximately 280MB of memory, but storing the activations for a batch of 64, seven - Second Utterances requires 1.5 GB of memory. Such as Titan X GPUs include 12 GB of GDDR5 RAM.

But **"Acoustic Model”** storing the weights for a **4M parameter network**.

Conclusion :

Our study has recognized some limitations, PR may be characterized as an information reduction , information mapping or information labeling process. As no single technology is always the optimal solution for a given PR problem. Pattern provide a means to capture successful solutions to common Software problems in a formal written manner so that they can be successfully passed on to and understood by Software development. In this paper we approaching our "Acoustic Model". Getting to this information is simply a matter of establishing the parameters of the search so that the qualifying and symbols can be for delivered to the network. So that it can save time by not Id bothering someone and so shed "Speech Recognition has a long history with my several waves of major innovations.

Reference :

Richard O. Duda, Peter E. Hart, David G. Stock : Pattern Classification, 2nd edition, John Wiley and Sons, New York 2001, EUR 114.46

Tervor Hastie, Robert Tobshirani Jerome Friedman : The Elements of Statistical Learning – Data Mining, Inference and Prediction, 2nd edition, Springer, New York, 2009, FUR 71:05

http: www- Stat. Stanford., edu/vtibs/Elem Stat Leann

Christopher M. Bishop :

Pattern Recognition and Machine learning, Springer, New York, 2006, EUR 75.05.

T.H. Bullock, The problem of recognition in an analyzer made of neurons, in Sensory Communications, W.A. Rose nblith , Ed (MIT Press, Cambridge, MA, 1961) P.P.717-712

The Journal of the Acoustical Society o America 122,881 (2007); http://doi.org) 10.1121/1-2750160

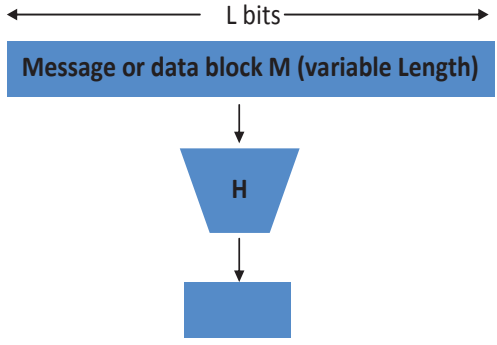
Mathematical model of Hash Function : A Review

1st Author : Smita Ghosh. (MSc. Mathematics. M.S. University) West Bengal School Dept. e-mail : smitaghosh04@gmail.com

Abstract: The term hash function has been used in computer science from quite some times. It refers to a function that compresses a string of arbitrary input to a string of a fixed length. This paper will present the detailed study of Hash Functions using some mathematical models. Discusses the basic as well as currently used iterative structures of Hash functions. Various design techniques of underlying compression functions have been explained. So that we throws light on the current scenario in Hash Functions. Verifying the integrity and authenticity of information les à prime necessity in computer systems and networks. So our mathematical model techniques make a some progressive recent development in this field. Finally various applications of hash functions are discussed showing their importance and every a day use.

Key words: Features Of Hash Function, Hash table, Collisions, Separate Chaining method, Double Hashing, Password Hashing, Performance of Hashing.

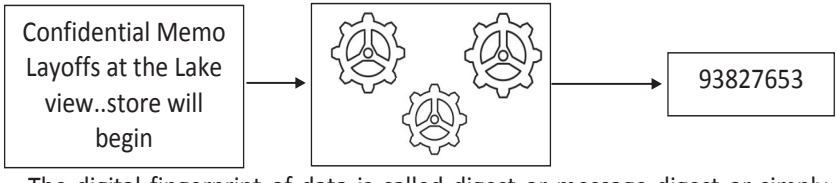
Introduction: Hashing is an algorithm that calculates a fixed size bit storing value from a file. A file basically contains blocks of data. Hash functions take data as an input and returns an integer in the range of possible values into a hash table. So a hash function is a mathematical function that converts a numerical Input value into another compressed numerical value.



The above diagram is the Block diagram of hash Function.

In hash function H accepts a variable length block of input data called as 'M' and produces the fixed size hash value can be represented as h=H(M)

So, Hash function or hash algorithm creates a unique digital fingerprint of data



The digital fingerprint of data is called digest or message digest or simply hash. Hash algorithm is. Primarily used for comparison purpose, not for encryption. Many secure Hash Algorithms have three basic Characterize:

1. Secure ⟶ Non a reversible function
2. Fixed size ⟶ Short or long data will produce the fixed – size digest

Example - Hash Algorithm : MDS

Original Data	Digest	Digest size
a	Occ175b9cof1b6a831c399e269t12661	128 bit
ab	187ef4436122d1cc2f40dc2b92foebao	128 bit
abc	900150983cd24fb0d6963f7d8e17f72	128 bit
abc 123	e99a18c428cb38d5f260853678922e03	128 bit

Hash function /algorithm is commonly used for passwords.

Keep in mind all passwords in twitter or any secure database should be stored in the from of digests. All passwords should be never stored in plaintext in any database.

Every time you login your password is hashed into a digest which is then against compared the one store in the database. That's why we say hash algorithm is mainly used for comparison purpose, not for encryption Hash functions are related to Checksums, check digits, fingerprints, Lossy compression, randomization functions, error-correcting codes and ciphers.

Although the concepts overlap to some extent, each one has its own uses and requirements and is designed I and optimized differently. The hash functions differ from the concepts numbered mainly in term of data integrity.

Features of hash functions are:

1. fixed length output.
2. compression function
3. Digest (smaller repn of larger data)

Properties:

M→H (Easy) H→M (very Hard)

M→H
⋮
n--->H

} same hash value for same message every time

M1→H1
M2→H2

} H1=H2

→ Should not happen.

Fundamental of Hash Function:

A Hash Function h maps keys of a given type to integers in a fixed interval [0,..., N-1] . We call h(x) hash value of x .

Examples :

→ h(x) = x mod N

is a hash function for integers keys. → h(x,y) = (5.X +7.y) mod N is a hash function for pairs of integers.

h(x)=x mod 5

	key	element
0		
1	6	tea
2	2	Coffee
3		
4	14	Chocolate

A hash table consists of

→ hash function h

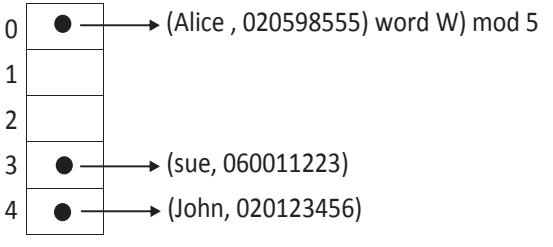
→ an array (called table) of size N The idea is to store item (k, e) at index h(k).

Hash Tables:

Example (1):

Phone book with table size N = 5

→hash function h(w) = (length of the



→ **Ideal Case :** one access for find (K)

(that is, o(1))

→ **Problem:** Collisions

→ Where to store Joe (collides with Sue)?

→ **This is an example of a bad hash function :**

→ Lots of collisions even if we make the table size N Larger.

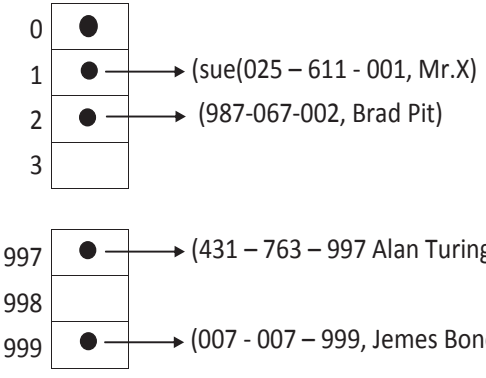
Example (2):

A dictionary based on a hash table for

→ Items (social security number, name)

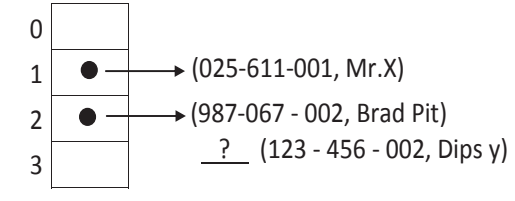
→ 700 persons in the database.

We choose a hash table of size N=1000 with : → hash function of h(x) = last three digits Of X.



Collisions: Occur when different elements are mapped to the same cell:

→ Keys K, K2 with h(k1) = h(K2) are said to collide.



Different possibilities of hashing

Collisions : → Chaining

→ linear probing

→ double hashing ---

Collisions continues:

Usual setting :

→ The set of keys is much larger than the available memory.

→ Hence collisions are unavoidable.

How probable are collisions :

→ We have a party with P persons. What is the probability that at least 2 persons have birthday the same day (N=365).

→ Probability for no collision:

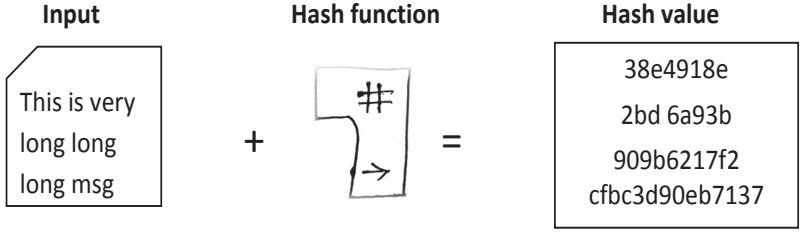
$$q(P, N) - N = \frac{N}{N} \cdot \frac{N-1}{N} \cdots\cdots \frac{N-P+1}{N}$$

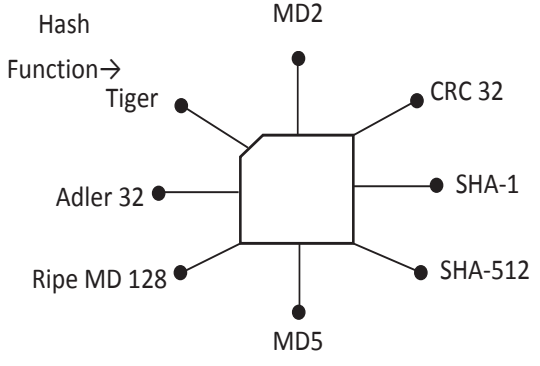
$$= \frac{(N-1)\ (N-2)\ \ldots\ldots\ (N-P+1)}{N}$$

→ Already for $P \geq 23$ the probability for collision is > 0.5

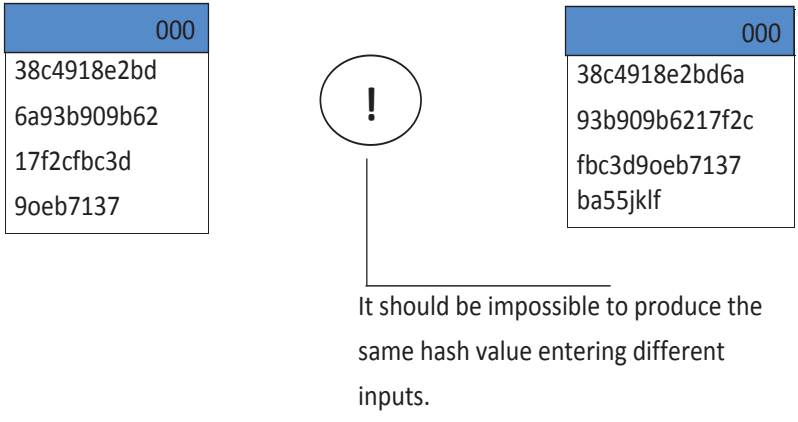
What is Hashing ?

Hashing is the process of converting an input of any length in to a fixed size string of text, using an mathematical function. This means that and text , no matter how long it is can be converted into an array of numbers and letters through an algorithm.



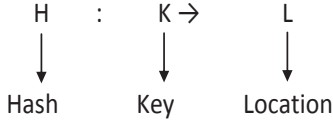


Quality → Unique hash value



Hashing is a searching technique which is inpendent of no. of element => O(1) [Complexity]

Now what is Hash function ?



Property of hash function :

1.easy to compute.

2.(L) that should be uniformly distributed in hash table.

Type of Hash Function:

1) **Division Method** → H(K) = k mod m.

= largest prime no.

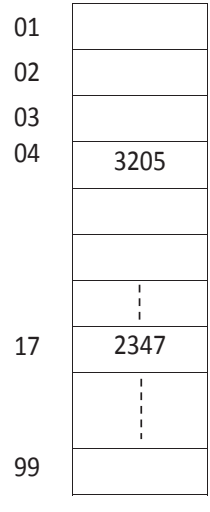
let k= 3205 ; m=97

H (3205) = 3205 mod 97

= 4

K = 2345 mod 97

= 17



2) Folding method :

H (K) = K1+ K2+--- + Kn

H (3205) = 32 +05 = 37 (location)

H (7148) = 71+4=1)1(9=19 (location)

3) Mid square method :

$H(K) = k^2 \rightarrow \ell$

H (3205) = $(3205)_2$ = 10272025

These as requirements, of a hash function H(X).

1. Hash functions are deterministic. For any o two identical data items X, H(x) will always yield the same result.
2. The outputs of hash functions from a fixed set: If d = H(x), then d is an element in a fixed set of outputs. Usually d is an n-bit integer in the range from o to 2^n-1; sometimes (in modular arithmetic) d ranges from O to P-1; for some prime p.
3. (Statistically useful hash functions only) statically property : Distribution patterns in the hash function input do not show up as distribution patterns in the hash function outputs.
4. (Cryptographically useful hash functions: only) Cryptographic property: Information about the hash function outputs does not give any information about the hash e function inputs.

If there is an unknown data item x where you are told d = H(X), you are no better off predicting item x than if you did not know the hash value d. It is impractical for you to find some data , item y such that

H (Y) = H(x) = d.

Outcomes of review and research Direction :

Now we have to learn what is "Hashing Algorithm"?

Calculation applied to a key to transform it into an address. For numeric keys, divide the key, divide the key by the member of available addresses, n, and take the remainder

address = key Mod n

- For alphanumeric keys, divide the sums of ASCII codes in a key by the number of available addresses , n, and take the remainder.

- Folding method divides key into equal parts then adds the parts together- The telephone number 01452 8345654 becomes

  Ol + 45 +28 + 34 +56 +54 = 218

Depending on Size of table, may then divide by some constant and take remainder.

"But when more than one keys (hash Functions) map to the same location of hashes. In this situation, two or more data elements qualify to be mapped to the same location in hash table, this is the situation when collision occur.

Collision Resolution. : open addressing

- Linear probing
- Plus 3 rehash
- Quadratic probing

(failed attempts)^2

- Double hashing

Closed addressing

So objectives of Hash function is :

- Minimize collisions
- Uniform distribution of hash values
- Easy to calculate
- Resolve any collisions

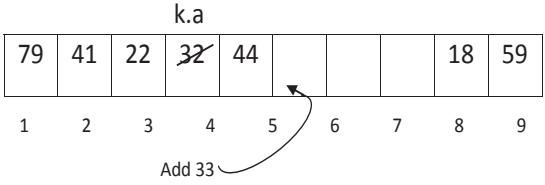
So, we say that hash table is used to index large amount of data. It address to each key calculated using the key itself. Collisions resolved with open or closed addressing. Hashing is widely used in database indexing, compilers , caching, password authentication and more and finally Insertion, deletion and retrieval occur in constant time.

Hashing collision Resolve :

We know h (x) = x mod 10

Keys = (18, 41, 22,32, 44, 59, 79)

Hash= (8,1,2,2,4,9,9)



insert (key)

h=hash (key)

int i=O ;

Deletion : Replace element with MARKET say, k.a

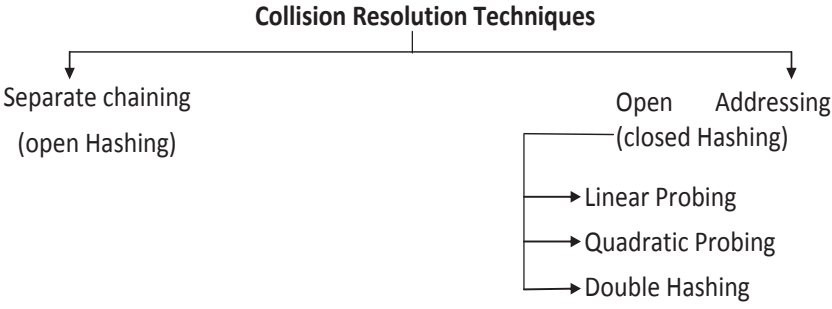
{ While (h+i mod N) not empty
Index And i<N
} i+t ;
If (Full) { return ; }
else
{ Add key to A [(h+i) mod N];
}

Now, I want to search (key)

{ h = hash (key) ;
i = o

While (h+i) mod N / index Is not empty
AND i<n)
{ if (A [h+i) mod N] = = key)
{return true ; // FOUND
i+ +;
} // NOT FOUND
} return false;

So finally this is the chart of Collision Resolution Techniques -



Separate chaining Method:

To handle the collision,

- This technique create a linked list to the slot for which collision occurs.
- The new key is then inserted in the linked list.
- These linked lists to the slots appear like chains.
- That is why this technique is called as separate chairing.

Example: Using the hash function "key mod 7", insert the following sequence of key in the hash table 50, 700, 76, 85, 92, 73 and 101

Use separate chaining technique for Collision resolution.

50 % 7 = 1

700 % 7=0

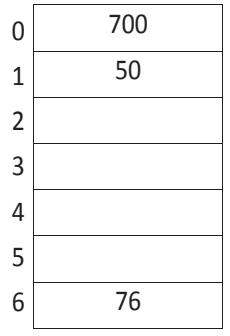
0	
1	
2	
3	
4	
5	
6	

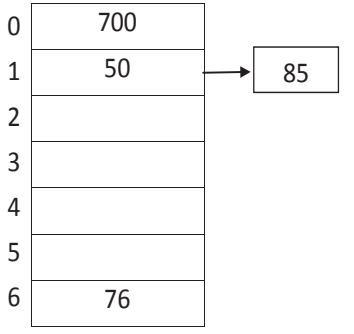
0	
1	50
2	
3	
4	
5	
6	

0	700
1	50
2	
3	
4	
5	
6	

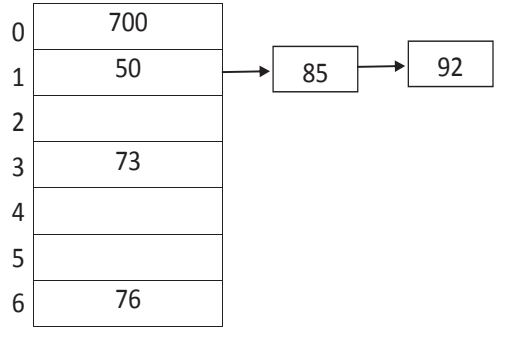
76 % 7 = 6

85 % 7 = 1

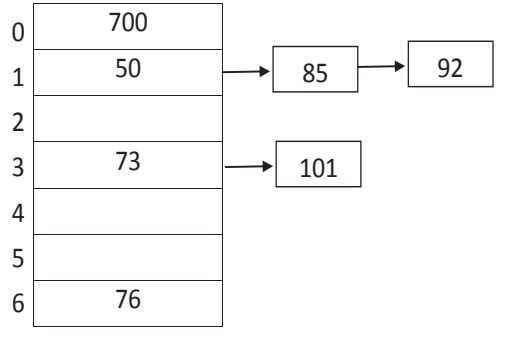

0
700
1
50
2
3
4
5
6
76


0
700
1
50
85
2
3
4
5
6
76

92 % 7 = 1


0
700
1
50
85
92
2
3
73
4
5
6
76

101 % 7 = 3


0
700
1
50
85
92
2
3
73
101
4
5
6
76

Time complexity for searching/Deletion :

- In such a case, all the keys will be present in a single linked list.
- Sequential search will have to be performed on the linked list, to perform the search.
- So, time taken for searching in worst case sin O(n).

Double Hashing: Double hashing uses a secondary Bash function d (k);

→ Handles collisions by placing items in the first available cell

h(k) + j. d(K) ; for j = O, 1, ..., N-1

→ The function d(k) always be>0 and <N

→ The size of the table N should be a prime.

Example : We use double hashing with:

→ N=13

→ h(k) = k mod 13

→ d(K)= 7-(k mod7)

K	h(k)	d(k)	Probes
18	5	3	5
41	2	1	2
22	9	6	9
44	5	5	5,10
59	7	4	7
32	6	3	6
31	5	4	5,9,0
73	8	4	8

31		41			18	32	59	73	22	44		
0	1	2	3	4	5	6	7	8	9	10	11	12

Designing a hash function →

For a hash table to work well, we want the hash function to have two properties :

- **Injection :** for two keys $k_1 \neq k_2$, the has function should give different results.

  $h(K_1) \neq h(K_2)$, with probability $\frac{m-1}{m}$

- **Diffusion (Stronger than injection):** If $K_1 \neq k_2$ knowing h (k_1) gives no information about h (K_2). For example if k_2 is exactly the same as k_1, except for one bit, then every bit in h (k_2) should change with 1/2 probability compared to h(k_1). knowing the bits of h(k_1) does not give any information about the bits of h (k_2).

As a hash table designer, you need to figure out which of the client, hash function and the implementation hash function is going to provide diffusion. For example, Java hash table provide (some what weak) information diffusion, allowing the client hash code computation to just aim for the injection property. The hash table specification should say whether the client is on to provide a hash code with good diffusion.

A hash function may be premage resistant consider h (X) = X^2 (mod n) where n = pq and P,q are large primes. Since computing a square root is equivalent to factoring n in this case, this function is pre image resistant However, since h(x) = h (-x) this function is not collision resistance or Second pre image resistant.

Hashing Technique - I :

Suppose we are storing employee records, the primary key for which is employee's telephone number

Telephone	Name	City	Dept	--------
9864567654	Sam	NYC	HR	
9854354543	Tom	DC	IT	

Here each row is uniquely identified through the telephone number of the employees.

Now for this was define three operations

- Insert Employee record
- Search for an employee
- Delete employee record

Now the question is how to implement this problem such that all the 3 given operations are done in most efficient manner.

Let consider few solutions:

1. Use an Array -.

   Search takes linear time.

   We can store them in an array out then searching a record will require linear time as we have, to go through all the records until the required one is found.

   An improvement in search can be made if we store them in a sorted manner.

   - If stored in sorted order, search can be done in O(Log n). Using binary search but then insertion and deletion becomes costly, as we need to maintain the sorted order.

2. Next method is to use a Linked List here also we require a linear time to search for a particular record as we need to go through all the records until the required one is found.
3. The next approach is using balanced binary search trees (BTS) to store records

   Insertion takes 0 (Logn)

   Search takes 0 (logn)

   Deletion takes 0 (logn)

The use of balanced binary search tree makes sure that we achieve a complexity of O(logn) for all three operations.

4. Next method is to use, Create a Direct access table.

- Insertion takes 0(1)
- Search takes (0)1
- Deletion takes 0(1)

This method provides an efficient complexity of o(1) for all three operations. Lets see how it looks like.

Directed Access Table

Telephone	Add

986456 7654	OX1
98 54354543	OX2

Name	City	Dept.	--------
Tom	DC	IT	--------

Name	City	Dept.	--------
Sam	NYC	HR	--------

Here telephone number act as a key and the value stores the address of the record. These are the records. This method looks good but it also suffers certain limitations.

Limitations :

1. Size of table

(m * 10 ^ n)

The first limitation is the size of table. The extra space required is o(m*10^n); where m is the size of pointer to the record and n are the digits is the telephone number.

2. Integer may not hold the size of n digits.

The other limitation is that digits in the telephone number can be more than what our integer variable can store. We'll try to improve the method and simultaneously introduce you to the concept of hashing.

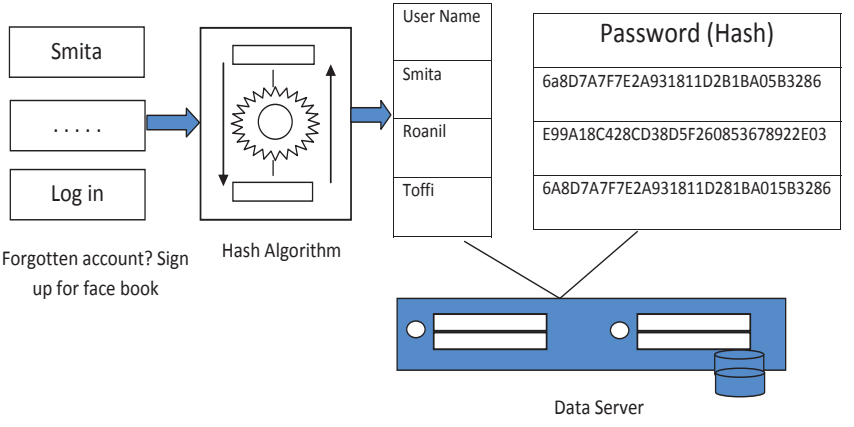
Hash Algorithm Qualities :

1. Input data from arbitrary size to return fixed size value.
2. Output digest has unique value.

Text	Digest	MD5
a	OCC17589COF1B6A831C399F269772661	128 bits
abc 123	E99A18C428CB38D5F260853678922E03	128 bits
Please subscribe my channel	6A8D7A7E7E2A931811D2B1BA015B3286	128 bits
Complete file	606FCC5F15300BE196EE775312F8A9019	128 bits

Password Hashing :

Log in to Facebook



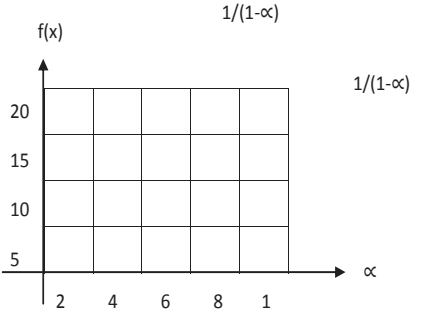
Performance of Hashing : In worst case insertion, Lookup and removal take o(n) time: →Occurs when all keys collide

(end up in one cell)

→ The load faetor ∝= n/N affects

The performance :

→ Assuming that the hash values are like random numbers, it can be shown that the expected number of probes is :



If worst case insertion, look up and I removal take o(n) times :

→ Occurs when all keys collide (end up in are cell)

The load factor x= $\frac{n}{N}$ affects the performance

→ Assuming that the hash values are like random numbers,

It can be shown that the expected 7 number of probes is: $\frac{1}{(1-\propto)}$

In practice hashing is very fast as long as x < 0.85

→ O(1) expected running time for all Dictionary ADT methods

No hash function is a good in general:

→ There always exist keys that are mapped to the Same value. Hence no single hash junction h can be proven to be good.

However, we can consider a set of hash functions H (assume that keys are from the interval [o, M-1]).

We say that it is universal (good) if for all keys o< i = ȷ <M:

probability (h(i) = h(j)) $\leq \frac{1}{N}$

for h randomly selected from H.

Double Hashing → This method is the efficient method of collision resolution technique because it was double hash function to calculate the address of any key.

Hash functions should be such that the hash address generated by the two hash functions are distinct

Hash (K,P) = [H_2 (k) + P H_2 (k)]

H_1 (k) and H_2 (k) are two different hash functions.

p is the probe no. 0, 1, 2, ..., n-1 m is the size of hash table.

Insert some records with key 19, 15, 7, 39, 55, 29, 45,67 in hash table of size 12

Key	Location	Probe
19	19 % 11 =8	1
15	15 % 11 =4	1
7	7 % 11 =7	1
39	39 % 11 =6	1
55	55 % 11 =0	1
29	29 % 11 =7	2
45	45 % 11 =1	1
67	67 % 11	3

Hash (K, P) = [H1(K)+PH2 (K)

H1 (K) = K%11

H2 (K) (K%7)+1

Hash (29,1)=[7+1 * {(29%7)+1}

= [7+2] =9

Hash (67,1)=[1+1 * [67%7+1]]

= [1+5] =6

Hash (67,2)=[1+2 * [67%7+1]]

= [1+10] =11

55	0
45	1
	2
	3
15	4
	5
39	6
7	7
19	8
29	9
	10
67	11

Conclusion :

The work ends with a conclusion that complexity theory has long studied problems like:

Mathematicians have classified the hard problems. There are Direct Access Table, Double Hashing and also to authentication by password hashing. As we have been seen hash functions from a wide family of functions. Mathematicians have showed us that we can rely. On functions with properties, like the properties involving collision resistance and Weak collision resistance. For the future, maybe many of the algorithms which we use should be re-structured simply because with quantum machines, there already exist algorithms that can solve hard problem. The main aim of this paper is the development of recent techniques applicable to Crypt Analysis Hash function. According to the efficiency analysis and security authentication, this proposed structure improves Security· We have made all attempts to give a complete pictures of Hash mathematical model and its a design. This paper would really help budding researches who would take up research in this particular field.

References :

1. An overview of Cryptographic Hash Functions and their uses, John Edward Silva 2003, GIAC Security Essential Practical Version.

2.William Stallings, The Whirlpool Secure Hash Function, Taylor and Francis Group 2006.

3. Soren S Thomsen : An improve pre image attack on MD2.

4. RSA Laboratories: Risa Laboratories

“Frequently asked questions about today's cryptography, version 4.1. 2000.

http://www. ressecurity.com/r salabs/faq/2- 3-1.html

5.Johnson Brad and Goessels Jonathan. The ssl hand shake 2001.

http:// www System experts . com / tutors / The- SSL - Hand shake-VI. 5f. pdf

6.SHA-1 hash function under pressure heise Securityist.

7.http://csrc.nist.gov/publicalions/fibs/180-4/fips-180-4.pdf

8. "cryptanalysis of MD5 & SHA-1" (PDF)

9.W.E. Burr, u coy cryptographic Hash Standards: Where Do We Go From Here", IEEE Security and Privacy . Vol. 4, NO. 2, 2006, PP. 89-91

10. M. Naor, and M. Yung, "Universal One-Way Hash Functions and their Cryptographic Applications", in STOC, 1989, pp.33-43.

11. P. Rogaway, and T. Shrimpton, "Cryptographic HashFunction Basics: Definitions, implications and separations for preimage resistance, second preimage resistance, and collision resistance", inFSE, 2004, pp.371-388.

12. B. Schneier, Applied Cryptography, John Wiley & Sons, 1996.

DYNAMICAL SYSTEM IN NEUROSCIENCE

ABSTRACT: Rhythmic brain processes might also explain how we can stay focused while multitasking- like when trying to remember an address while driving a car. Rather than simultaneously focusing on these tasks, we might be alternating between them on a sub second time scale.

In the healthy brain, a change in wave intensity has been observed in the context of a wide range of cognitive activities such as memory and learning. My research focused on brain regions which is characterized by strong brain wave intensity. In my study I will show how some transmission and processing of information in the brain may be the reason why we actually see cognitive impairment in human. The brain has been thought of as a biological computer that processes information through traditional circuits. Where data zips straight from one cell to another. The brain parses information through the interactions of waves of neural activity. So, we have to understand how the computational machinery of brain is working

In this paper I will show you how different "Mathematical Models" helps to explain the brain's understanding state can change, affecting people's attention, focus or ability to process information.

KEYWORDS: Cognitive Revolution, Mind Reading Bubbles, Nonlinear Brain Dynamics, Biomarker Discovery, Computational Psychiatry, Info-Theoretic Hashing Model, Stochastic Synapse Model.

INTRODUCTION: The brain is the control center of the body, and it's responsible for everything from your thoughts and emotions, to your movement and sense.

A neural network learns when we feed it with a large amount of data and each connection is linked with a weight. Magnetic resonances measures activity in the brain by detecting changes in the blood flow. Just like a computer. The brain has been reacting for different functions. The brain has an inbuilt backup system where the functioning pathways replace the damaged pathways. Backup system, on the other hand, are created manually on a computer. The cerebellum, it's responsible for movement and balance. Brain is constantly changing and adapting based on our experiences and environment.

HUMAN BRAIN

HIPPOCAMPUS Spatial Memory fast learning.

NEO-CORTEX (75%) What's so significant that overcome costs-sensory motor model of the world.

MID BRAIN Emotion basic learned behavior.

BRAIN STEM Autonomous behaviors.

SPINAL CORD Relax behaviors.

Detecting emotional and cognitive changes to predict response to different types are of input, e.g. music, video,

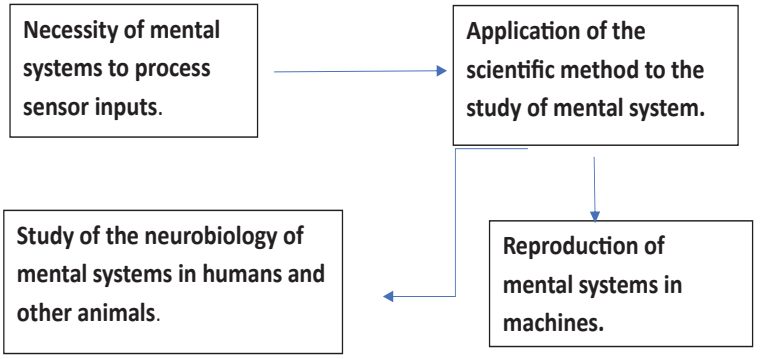
news, ads, mails. One of the most fascinating aspects of neuroscience is the so-called neural-codes the underlying patterns in neurons and brain cells that are responsible for human behavior, mood swings and other abstract mental phenomena.

NEURO FOR AI

- Successful examples: Reinforcement learning, deep learning.
- Still, artificial brains are why behind the natural ones:
- Brains develop from a single cell via neurogenesis and plasticity, while artificial NNs (ANNs) are manually constructed.
- Brain can easily adapt to very different environments and new tasks over lifetime, ANNs are still highly specialized and inflexible.
- Attention, memory, learning mechanism(backprop) in ANNs can be improved by more biologically plausible implementations.
- Brain is a dynamical system changing even without the input, in resting-state, while machine-learning models are mainly static.

The study and development of computer systems able to perform tasks normally believe to require human intelligence.

COGNATIVE REVOLUTION



TEMPLATES: Internal representation of shapes or objects: properties of elements, spatial relationship;

- ❖ **SIMPLE SHAPE TEMPLATE:** Neighboring contours surrounding a simple shape.
- ❖ **DIRECTION OF BORDER PIXELS:** Pointing inside, useful figure-ground separation.

SUPPORTING EVIDENCE FROM NEUROSCIENCE:

- ➢ Neurons responsive to complex patterns, such as corner, junction and curvature.
- ➢ In the low-level visual cortex, there are neurons selective for convex or concave or conjunction of 2-3 adjacent curvature events.
- ➢ Border ownership cell signals a boundary owned by the focus.

The study and development of computer systems able to perform tasks normally believed to require human intelligence.

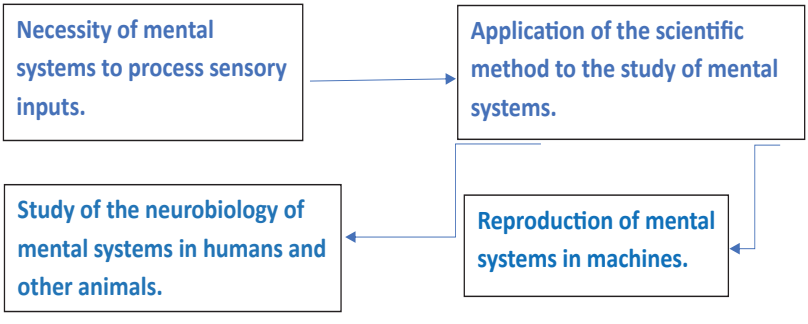
RUDIMENTARY PROCESS OF NEUROSCIENCE: Social responsibility of science is developing increasingly safe performative and reliable AI-powered neurotechnology and neuro-inspired AI systems. Mathematically, the base model for an irregular spike train is the

probability of spiking within a time interval (t, t+δt) for a small change in time-

P (spike in (t, t+δt) ~λδt

However, this model is insufficient neurons have refectory periods following a spike.

COGNATIVE REVOLUTION: Reducing the global impact of neuroscience and psychiatric disorder.



A cyber-biological system involving the two-way exchange of information between biological brain and an AI, and in which there are processes of mutual adaptation between the human user and the artificial system.

THE INTERPLAY BETWEEN NEUROSCIENCE AND AI:

1. **THE DIGITAL MIND:** More and more activities of the human mind have become inferentially analyzable using data from digital devices and intelligent algorithms.
2. **THE ARTIFICIAL MIND:** Neuromorphic approaches to computer are increasingly able to mimic the functioning of the human brain in data processing and use this ability for cognitive tasks such as detecting objects, recognizing or translating language and making decisions.

3. **THE HYBRID MIND:** Closed-loop brain computer interfaces (BCIs) and other neurotechnology's established a greater degree of integration and mutual influence between the cognitive and affective processes of the human mind and AI system.

Modern AI supported research hold many promises for basic and applied science. Data sharing and relief to the problem.

But only if the data are provided in a usable way. The brain is an immensely complex organ which regulates many of the behaviors that animals need to survive. Determine under what conditions it is ethical to develop and deploy AI powered neurotechnology and neuro inspired AI systems.

The brain is a very effective computation machine and the aim of AI is to build machines that are really good at all the tasks a brain can do.

DEFLATION OF THE MIND READING BUBBLE: Artificial neural networks algorithms inspired by connections in the brain, have learned to perform a verity of tasks from pedestrian detection in self-driving cars to analyzing medical images, to translating languages. Studied shows that research teams regularly failed to report their analysis pathways in their publications, making an exact replication nearly impossible.

The artificial intelligence research community doesn't necessarily have a complete understanding of what neural networks are doing, they give us good result but we do not know how or why?

Due to interpersonal variability, fMRI can demonstrate correlations between brain activity and behavior on a group level but it's ability to identify a single mental state in one person may never meet a tolerable level of accuracy.

SENSORY INPUT	PREVIOUS EXPERINCES
p(u/x)	p(x)
	✓ Childhood
	✓ First love
	✓ Journey anywhere

Learning= Integration. p(x/u)

If human brain was like a lattice, it would take so much path length to reach from one ROI to another ROI which would slow down the functionality of the brain.

If human brain was totally random, it would be functional fast but there would be very low clustering which would result in few connection formations in the case ROIs.

So, the small-word network is the perfect balance for the human brain which works at the optimal pace and has enough clustering co-efficient.

ASSOCIASTIVE LEARNING: Choose path that is the most similar to the one which was rewarded Learning that lets one thing predict another thing.

Let y= g(x); z= f(x)

x ⟶ y ⟶ z

Now from the Chain Rule, $\frac{dz}{dx} = \frac{dz}{dy} \times \frac{dy}{dx}$

x ⟶ y ⟶ z ⟶ ω

$$\frac{d\omega}{dx} = \frac{d\omega}{dz} \times \frac{dz}{dy} \times \frac{dy}{dx}$$

OUTCOMES AND RESEARCH DIRECTIONS: The human brain consists of about 100 billion neurons. Each of those neurons makes about 10000 connections. A single neuron is an amazingly complex little, basically nano-machine doing incredible things. The brain is an

amazing device; it's the most complex thing we know in the universe. We have to do things like create artificial neural networks. The brain is very different from a computer, the way it's structured. A computer basically has the CPU is separated from the memory, we get a thing, that is called memory bus. The memory bus is working the full time, continuously when a computer is turned on.

$\frac{Predictive\ Model + Healthy}{Mental\ Disorder}$ = Mental State

MENTAL STATE IN VIDEOGAMES**:** Sparse regression - 75 to 95 %

PAIN PERCEPTION: Sparse regression – 70 to 80 % accuracy, "holographic "patterns.

COCAINE ADDICTION: Sparse Markov net biomarkers; MPH effects analysis ("stimulant 4 stimulant")

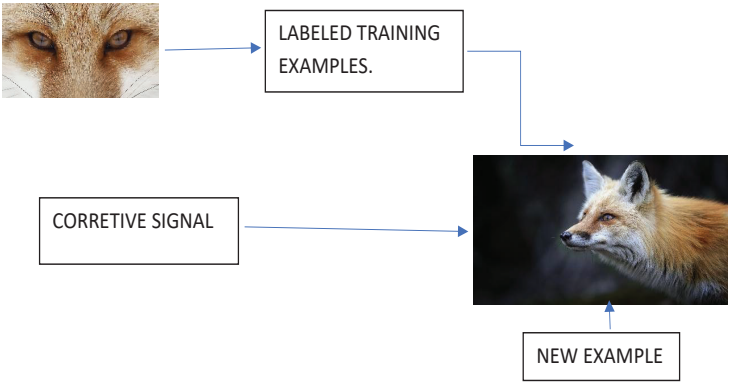
COGNITIVE LOAD PREDICTION: 91% WI recurrent conversion Nets.

Schizophrenia Classification: 74% to 93% accuracy symptom severity prediction. Nonlinear dynamical models of calculation and fMRI.

AI is meant to replicate the workings of the human brain to make machines and digital applications as initiative and efficient as possible. To achieve this, engineer in the field of AI build neural networks that mimic the structure and processes of the human nervous system. At the same time, neuroscientists can benefit from deep learning and other AI components to find cures and better solutions for complex illness such as Alzheimer's and Amyotrophic Lateral Sclerosis. Speaking to unknown, big data can help health experts with understanding the abstract.

First exposure ⟶ Correct response

We could potentially collect more data for an independent cohort to test our model, but this would be highly time consuming and expensive. In neuroimaging studies, one can select a set of regions of interest which are believed to be implicated in a particular disorder or cognitive task.



MODELING NONLINEAR BRAIN DYNAMICS:

1. High temporal (0.8 Hz) and spatial (few voxels/neuron) resolution (unlike fMRI / EEG).
2. Oscillatory behavior.
3. Very high dimensionality: ~ 10000 time series (neurons), even in a collapsed 2D version (average) of the original 3D data.

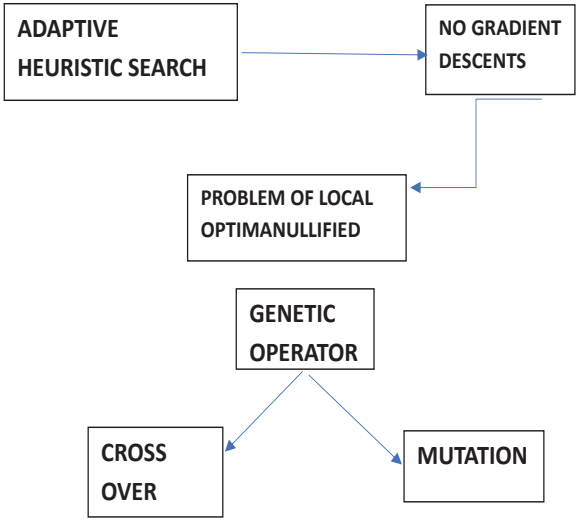
AI models can be used to accurately simulate the various neuron to neuron connections in the body.

PREDICTING TREATMENT RESPONSE IN DEPRESSION:

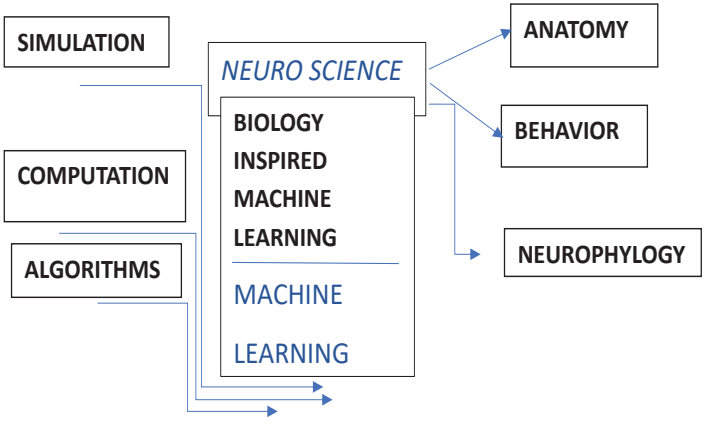
- Most depressed patients do not respond to their first antidepressant respond to their first antidepressant treatment.
- 1949 STAR*D patients labelled as “responders” or “non-responders” to citalopram (QIDS≤5)

- Cross-validation and external verification of model built from demographic/ symptom data.

THE EVALUATOION MECHANISM: Evolution has played a big part in development of human species, algorithm for heuristic search optimization based on the same fundamentals can have a far-reaching effect.



MENTAL STATE RECOGNITION AND BIOMARKER DISCOVERY: In this review I will discuss different multimodal neuroimaging setups, the advances achieved in basic research and clinical application and the methods used.



NEUROGENISIS SIMULATION: Here I will provide a comprehensive overview of mathematical tolls reoccurring in multimodal neuroimaging setups, the advances achieved in basic research and clinical application and the methods used.

Function magnetic resonance imaging is a popular tool for studying brain activity. It can non-invasively image the human brain without any ionizing radiation. The method can detect brain activity in correlation to tasks performed by the subject during the scan and is used in neurology and psychology research.

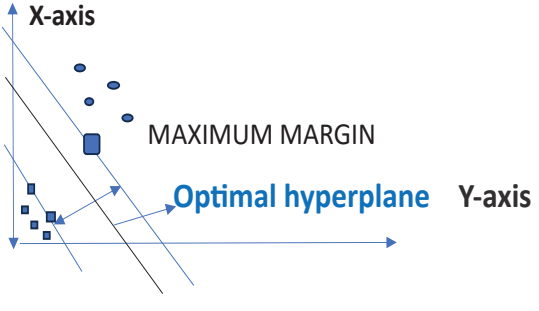
> **AI FOR NEURO: COMPUTATIONAL PSYCHIATRY-** "Psychiatric research is in crisis" – Wiecki, Poland, Frank, 2015.

Computational psychiatry is the use of Mathematical and Computational approaches to address questions relating to mental illness.

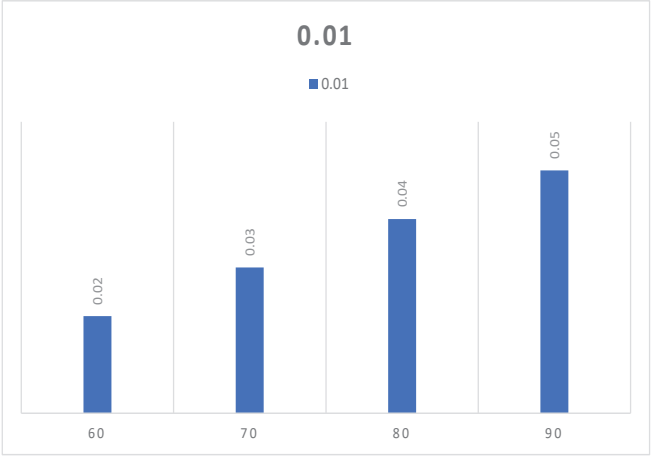
A new approach to mental illness:

DATA-DRIVEN COMPUTATIONAL PSYCHIATRY: Use machine learning techniques (supervised and unsupervised) to discover hidden structure, often in high-dimensional data.

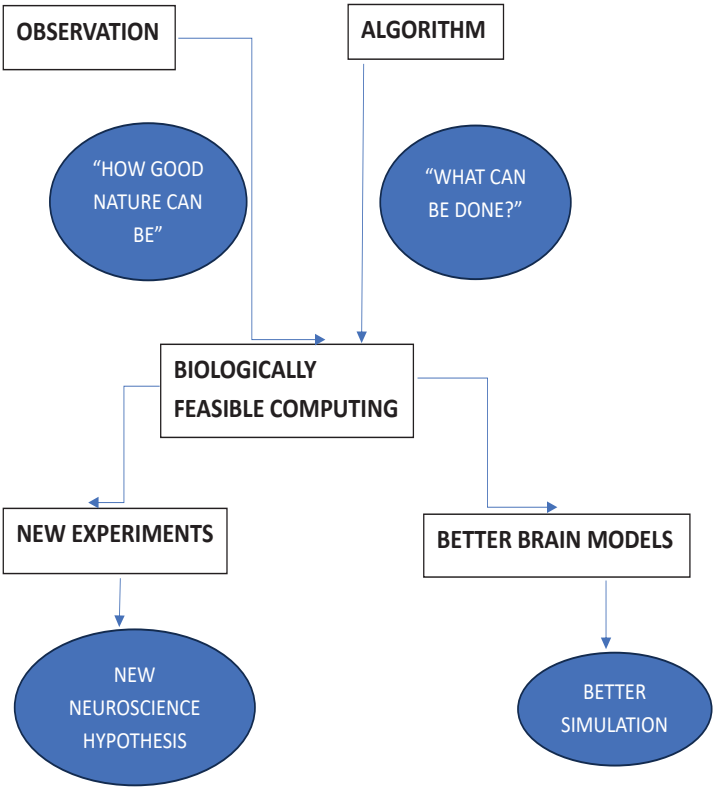
SUPERVISED LEARNING	UNSUPERVISED LEARNING
Labels provided train a classifier to predict categories e.g. support vector machine (SVM)	No labels find clusters in the data e.g. Gaussian Mixture Modelling.



DIVERCITY CURVE



Human brain has an incredible capacity to store information. The average noggin can store an estimated 2500 terabytes, according to the paper.



The researchers envision complex 3D cell structures that would be connected to AI and machine learning systems.

MRI itself creates a variation of electronic noise. If you move your head, it affects the magnetic field and that effect lingers for a while and does not only disturb the image in that moment but also the following images, says Associated Professor Anders Eklund.

DYNAMICAL MODEL: Van Dar Pol oscillator effect is,

$$X_{1i}(t) = \alpha_{1i} x_{1i}(t) (1- x_{1i}^2(t)) + x_{2i}(t) (\alpha_{2i}+\sum_{j=1}^{N} W_{ij} x_{1j}(t)$$

Here $x_{1i}(t)$ is i-th observed variable

and $x_{2i}(t)$ is i-th hidden variable.

W – interaction "network"; α_{1i}, α_{2i} , α_{3i}, W_{ij} parameters.

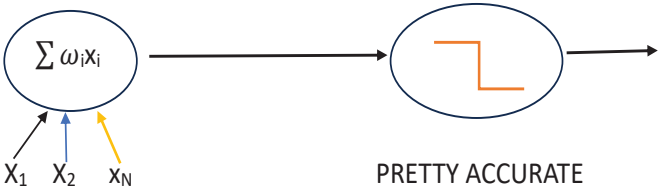
alphas- determine the bifurcation diagram of the system.

I. Oscillatory behavior is common in all neural systems; Van Der Pol is simplest nonlinear oscillator with rich enough behavior.
II. Voltage- like X1 (activity); and recovery – like X2 (excitability), similarly to neuroliterature.

Computational psychiatry leverages multi-level data collection to produce mechanistic models connecting low level biology and high-level behavior. Recently, new advances have Recently, new advances have emerged at different levels of psychiatric research. Therefore, these well-characterized, multilevel data provide a new opportunity for a strong alliance between the traditional model-based approaches and the new data- driven approaches in a new age of computational psychiatry.

WHY BIOLOGICAL NEURONS ARE DEEP NEURAL NETWORKS?

PERCEPTRON: Perceptron as a logic gate. ax+by ≥ threshold



NOT SO ACCURATE

SUM

COMPARE

INPUT= $x_1 \omega_1 + x_2\omega_2 + \text{-------} + x_N\omega_N$

OUTPUT = $\{$**1** if IN ≥ threshold

0 if IN < threshold

To train the network is to adjust the input weights. We still refer to the nodes as “neurons”. Key property of a neurons are electrically excitable cells control membrane voltage.

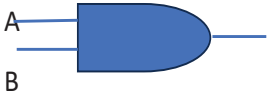
Voltage-gated channels, can open and close denuding on membrane voltage. Dendritic function is reduced to summing inputs.

Coincidence detector requires:

1. Depolarization (voltage – gated)
2. Neurotransmitter.

NMDA channels allow for non-linear integration of incoming information. Single neurons can process spatiotemporal sequences of inputs. Store information in bits units with two possible states 1 0

Here now arise “Logic gates”, these individual gates perform Boolean Operations (And, Or, etc.)



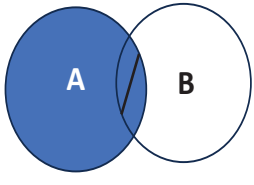
XAND(Gate)



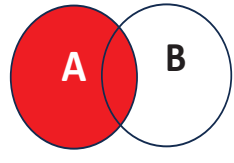
XOR(Exclusive) (Gate)

A	B	X
0	0	0
0	1	0
1	0	0
1	1	1

A	B	X
0	0	0
0	1	1
1	0	1
1	1	0



VAN-DIAGRAM OF AND(GATE)



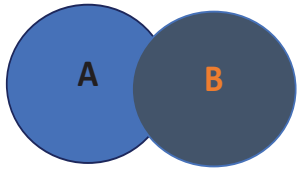
XOR (exclusive)



GATE

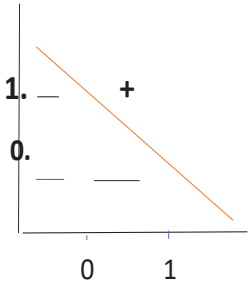
OR (inclusive)

GATE



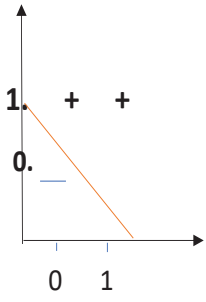
Van-diagram of OR GATE.

AND



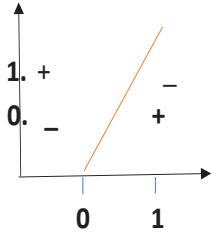
LINEARLY SEPARABLE

OR



LINEARLY SEPARABLE

XOR



LINEARLY NON-SEPARABLE

To perform XOR a multi-layered network is required.

WHY A DEEP ARTIFICIAL NEURAL NETWORK PREDICT ACTIVITY OF SINGLE BIOLOGICAL NEURONS? Artificial neuron first detects the function of single neuron then it passes the accurate signal to network for decode them.

Biophysical model contains some following differential equations:

$D/4R_a\,\delta^2v/\delta x^2 = C_m\,\delta v/\delta t + \bar{g}\,N_a m^3 h\,(v - EN_a) + \bar{g}\,Kn^4 h\,(v - E_K) + g_l\,(v - E_l) + I_{other.}$

$\delta m/\delta t = -\alpha_m\, m + \beta_m(1- m);$

$\alpha_m = -\frac{.1(V+40)}{1-\exp(-.1(V+40))}$, $\beta_m = 4\exp(-(\frac{V+65}{18}))$

$\frac{dh}{dt} = -\alpha_h h+\beta_h(1-h)$; $\alpha_h = .07\exp(-.05(v+65))$, $\beta_h = \frac{1}{1+\exp(-.1(v+35))}$

$\frac{dn}{dt} = -\alpha_n n+\beta_n(1-n)$; $\alpha_n = \frac{.01(v+55)}{1-\exp(-.1(v+55))}$, $\beta_n = .125\exp(\frac{-(v+65)}{80})$

Network required 5-8 layers to accurately predict single neuron activity. Dendritic and non-linearities equip neurons with vast computational capabilities.

INFO-THEORETIC HASHING MODEL:

- Patient's responses can be very long.
- Therapist's responses are much shorter, high level, 'label'- like summarizing and confirming patient's response.
- What constitutes a "good" response?
  Difficult to measure output of a therapy session. It can take many sessions to see an "improvement", in patient's condition.
- Some notion of relevance/coherence (mutual information) may help describe "successful" dialogue.

PATIENT **THERAPIST**

argmax (C_p: Ct; M_h)=H (C_i;M_h)-H (C_i|C_p:M_h)

Construct hash codes of responses.

⬇

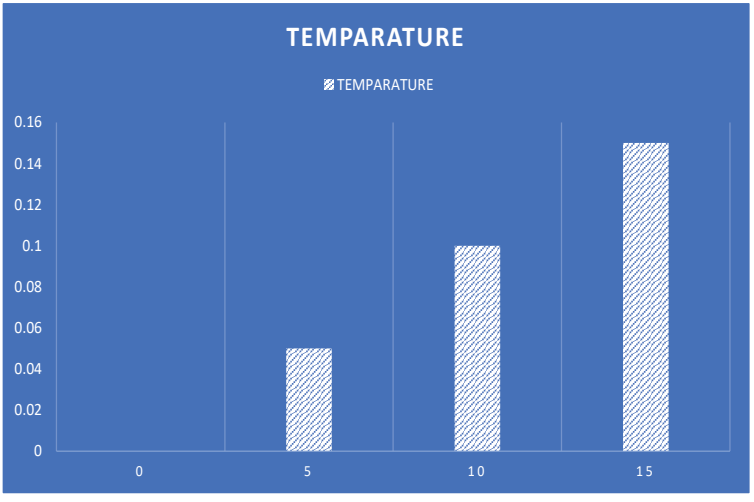
Optimize hashing model to maximize mutual information between patient and therapist.

⬇

Learn a predictive model to maximize mutual information between patient and therapist.

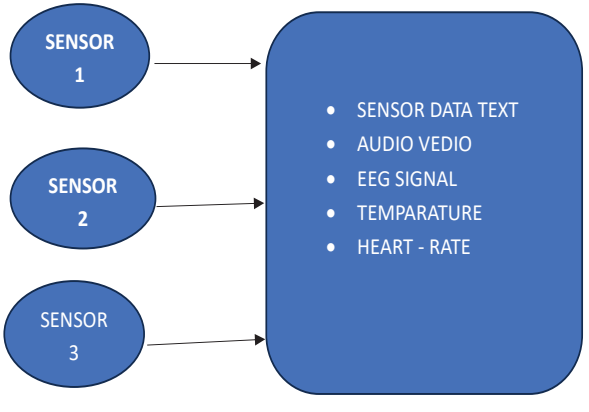
Let's see how Dynamic co-relation decrease with distance when transmission occur in every signaling process between patients and therapist. The following graph shows that how distance effect to transition of temperature and patient become hot, cold and critical.

Distance	TEMPARATURE
5 unit	.00 ^{0}c
10 unit	.05^{0}c
15 unit	.10^{0}c
20 unit	.15^{0}c



FUTURE VIRTUAL THERAPIST: A virtual AI assistant on a smartphone which implements the following four main steps:

A. Data collection.
B. Mental state recognition
C. Talking action to improve the mental state
D. Receiving feedback from a person to improve future actions

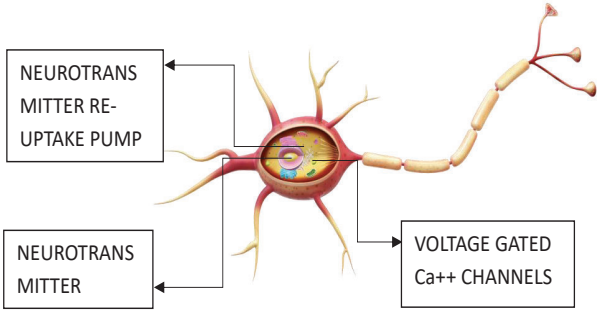


DISTINCT BUT RELATED PRIVACY PROBLEMS: Neuro privacy concerns the protection of brain data (or neural data). Mental privacy concerns the protection of mental information. Manipulation of a specific psychological function to identify localized effects of that manipulation on brain activity. The brain connection that we make when we explore and navigate our environment help us better connect to the World around while brain is connecting mental privacy.

STOCHASTIC SYNAPSE MODEL:

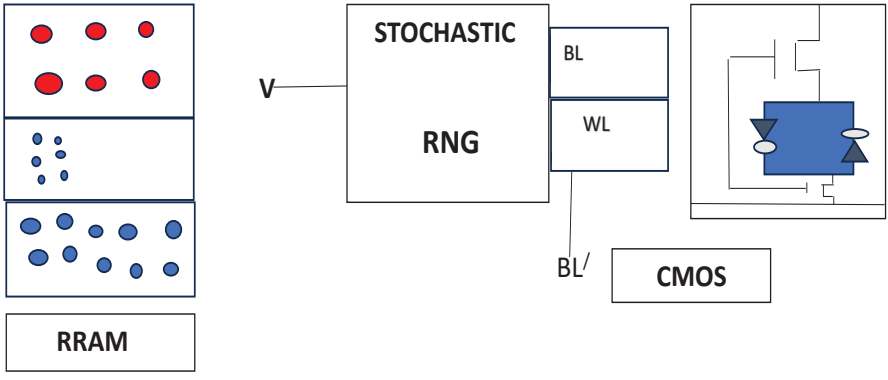
- Two different Neuron-types: Inhibitory(I) or Excitatory(E).
  Strength of the synapse: J
  Number of presynaptic neurons: C.
- Spiking times: t_j^i = t of the j th spike coming from the ith presynaptic neuron.
- Stochastic Assumption: Neurons spike according to a Poisson process with constant probability of emitting a spike per unit time v.

Therefore, $I(t) = J_E \sum_{i=1}^{CE} \sum_j \delta(t - t_{Ej}^i) - J_I \sum_{i=1}^{CI} \sum_j \delta(t - t_{Ij}^2)$



- Stochasticity in memristors can be exploited for learning a neural interference.

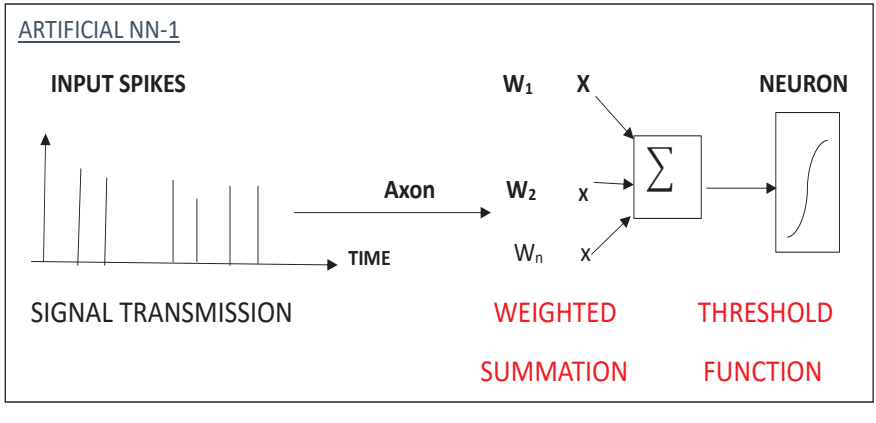
- CMOS implementations require hardware expensive random number generator circuits.



STOCHASTIC BITS IN OTHER TECHNOLOGIES:

Number of synapses about 10000 times the Humber of neurons, need for memory compression. Artificial neural networks have a wide range of uses in machine learning. Easy type of artificial neural network model has different strengths and use cases. Recurrent neural networks are often utilized for analysis sentiment or translating text too. The death and scale of the neural architecture mean a non-linear decision-making process can be achieved.

ARTIFICIAL NEURAL NETWORK: SIMPLE MODEL



Computing paradigms have shown the capability to perform complex computations at lower area and power costs. Stochastic computing is one such paradigm, which represents each data point in the form of a bit stream, where the probability of having "1" s corresponds to the value of the data. Weight is nothing an integer number that controls the signal between the two neurons. If the network generates a "good or desired" output, there is no need to adjust the weights. However, if the network generates a "poor or undesired" output or an error, then the system updates the weights in order to improve subsequent results.

Combination= bias + weights*input ($F=W_1*X_1+ W_2*X_2+ W_3*X_3$)

Finally, activation function is applied output

= activation(combination) in the pic-1.

Activation is sigmoid represented by = $1/1+e^x$

Based on both the language model and fMRI data, trained a system that could predict how the brain would respond when it hears each word in a new story for first time.

SHORTEST PATH LENGTH: Shortest path length between two vertices in an un weighted graph is the minimum number of edges we need to go across in order to go from the first vertex to another.

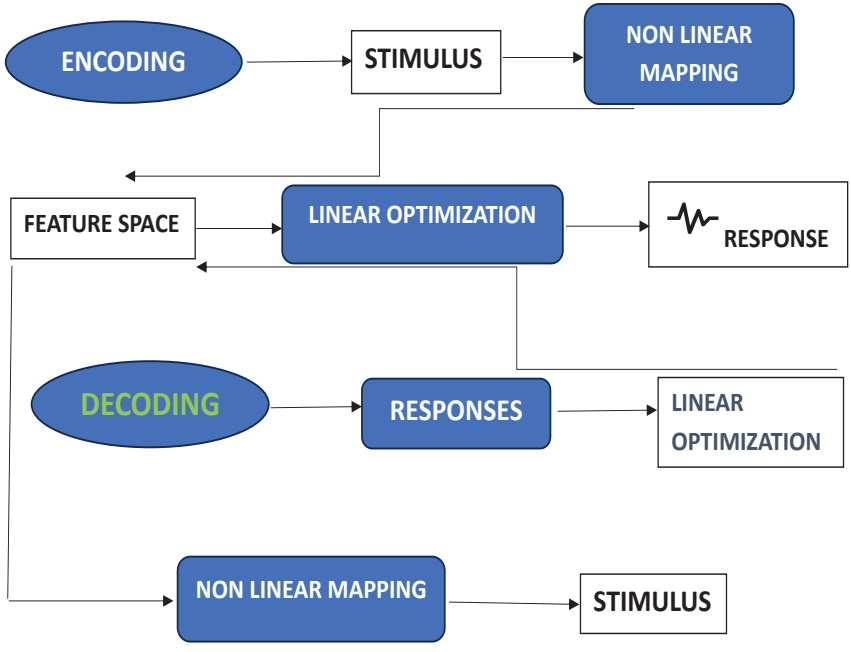
$$L= 1/N\sum Iij$$

Communication is central to the operation of brain networks, as it is necessary for information integration and for distributed neural computation.

HOW MAPPING IMPACT IN SHORT TERM MEROMY?

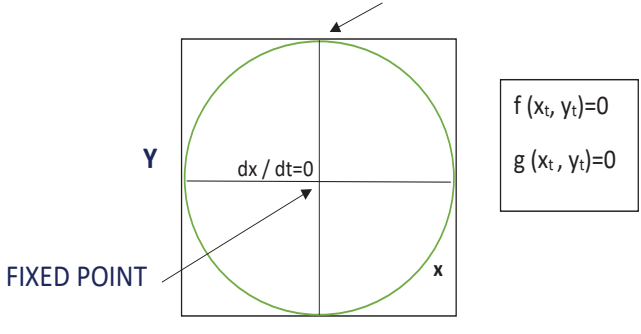
In the human the frontal lobe plays an important role in processing short-term memories. Short-term memory has a low capacity to

retain, information.



The researchers are currently extending these studies to explore of how multiple brain regions interact with each other with the objective of transferring and processing different types of information.

PHASE PLANE OF THE SYSTEM: It is assumed that f, g are continuous, differentiable in some region D in the XY-plane. This assumption makes f continuously differentiable in D. dy/dt=0



Each case (x_t, y_t) in D is a trajectory whose graphic in the phase plane is a single point, called an equilibrium point.

$\frac{dx}{dy}$= ax(t)+by(t); $\frac{dy}{dt}$= cx(t)+dy(t)

At, X Region	At, Y Region
x= 0, y= -1	x= -1, y= 0
$\frac{dx}{dt}$= .1	$\frac{dx}{dt}$= 0
$\frac{dy}{dt}$= 0	$\frac{dy}{dt}$= - .1

Points in space where the value of a variable does not change with time. Solutions of linear differential equations: $\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$

$v^{/}$= Mv, this is the generalizes differential equations to arbitrary number of dimensions.

The nullclines [null means '0' and cline means slope] of the system

$x^{/}$= f (x, y); $y^{/}$= f (x, y)

Occur when f (x, y) =0 or g (x, y) =0

You have found Stochastic differential equations:

$\frac{dv}{dt}$= f (v, t) +g (v, t) η(t)

η(t) ~ N (0, Δt) where η(t) ⟶

Random fluctuation.

v ⟶ membrane potential of a neuron.

Therefore, $\frac{dv}{dt}$= - av(t) + bη(t)

So, the Standard Recurrent Neural Network (RNN) is x(t+1) =f(x(t),I(t), t; θ)

Therefore, The Neural Ordinary Differential Equation is

$$\frac{dx(t)}{dt} = f(x(t), I(t), t; \theta)$$

Continuous time in RNN

$$\frac{dx(t)}{dt} = -\frac{x(t)}{\zeta} + f(x(t), I(t), t; \theta)$$

CONCLUSION: We know that our brain is a spatial organ. The hippocampus in particular is responsible for mapping, navigation and memory storage. These functions are linked to additional mechanisms such as episodic and long-term memories. Research has shown that when we exercise these functions, we see an increase in brain activity. These active neurons not only create new connections but preserve and organize existing ones. Research use machine learning tools to reveal how memories are coded in the brain. However, my work shows that, working function of brain not inactive anymore. If some part of brain is not working properly, then we storing it single to specific neural network and also activated our memories by connecting it to another level of frequency.

OBJECT ORIENTED PROGRAMMING AND IMPORTING

AUTHOR: SMITA GHOSH

ABSTRACT: Object-oriented programming took the best ideas of structured programming and combined them with several new concepts. The result was a different way of organizing a program. In the most general sense, a program can be organized in one of two ways: around its code or around its data. Using only structured programming techniques, programs are typically organized around code. This approach can be thought of as code acting on data.

Object-oriented programs work the other way around. They are organized around data, with the key principle being "data controlling access to code." In an object-oriented language, you define the data and the routines that are permitted to act on that data. Thus, a data type define precisely what sort of operations can be applied to that data. Developers have criticized the object- oriented programming model for multiple reasons. Object-oriented programming is a programming paradigm that provides a means a structuring program so that properties and behaviors and bundled into individual objects.

KEYWORDS: GUI System, Internet Protocol, Ha Proxy, DNS, LAN, Remote Procedure Call, Range based Sanding, Protocol Buffer, Object Storage Data, Postal Management System, Midday Meal Management System. Kinetics motion of dropping a motionary object.

INTRODUCTION: Object Orientation is process which describe how a system should be analysis ands design, it is not a language or tool.

How a developer identifies an object behave like a proper hierarchy is the key method. Keyword transformation used to change one object to another object.

Computer programming has been around for some decennium now. Now a days one one of the most intersecting areas of software development is the fusion base manipulation to show the behavior of an object.

Object oriented programs work the other way around. The principals of object orientation programming have three traits in common: Encapsulation, polymorphism and inheritance.

ENCAPSULATION: Encapsulation a class hides programming mechanism that binds together code and data it binds together code data it manipulates the objects is the device that supports encapsulations. Encapsulation protects data from accidental modification, enhance code organization. Encapsulation used for hiding data and data function. Abstraction focus the unpredictable behavior of an object. Encapsulation focus on the implementation. Here code generated any interface to design and accessing the function to make task completely. A group of databases can access the system and draw their computer resources hardware.

POLYMORPHISM: Polymorphism is one of the basic components of object orientation programming. Polymorphism can be help in scaling large projects by making the code. Polymorphism allows time changes behavior of an objects. This can significantly improve the flexibility, reducibility and maintainability of a code. Large and complex system are using this kind of code. A simple example of polymorphism is found in the steering wheel of an automobile. It simple develop the games and allowing objects to simplify these games and allowing objects to simplify these games, and shared this

oriented behavior. This can be using data writing flexibility, reuseable and maintain code. Polymorphism is often used in conjunction with design pattern like the Entity Component System. Practical example of polymorphism is as follows:

Polymorphism ➡ plane class

Class Plane. drive ()

Class chartered plane. drive ()

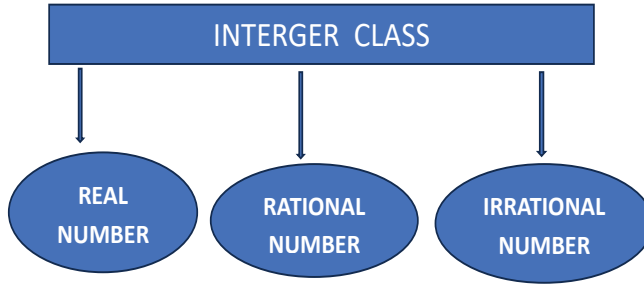
(int spd, string des)

GUI SYSTEM: A graphical user interface comprises visual components like cursor, icons and buttons, enriched with sound and visual effects.

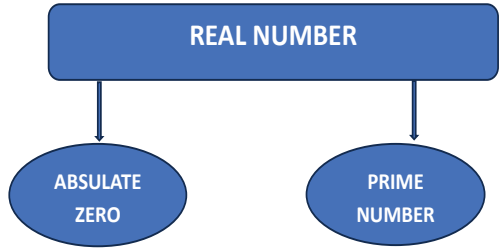
Explaining these principles helps understand makes user interface easy to use. That is why design matter in large interface.

INHERITANCE: Inheritance is the noun word which means something inherited. From parental we get the property which is called inherited. Reuse are applying for better functionality of the system. Protected means user friendly for anyone but not harming interface. Visible information differs by its classes. Implementation is a base class of inheritance which differ into different keywords. In object orientation the Inheritance means parental object by it's system, and doing the real works. Inheritance is the other class of mechanism which differ by its acute hierarchy. Inharitance is the core of object orientation method and it is manipulated by the mechanism of its classes. Here the classes we presented into some different subclass.

CLASS:



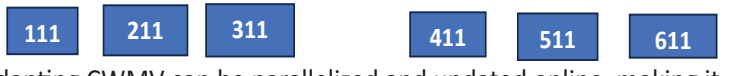
SUBCLASS:



It can inherit its general attributed from there parents. It is the process by which one can achieve a powerful concept. Inheritance not only protected the public class or subclasses. Hiding details of television except TV screen and control panel is called absorption. I n a specific exam a special niech is used for the accurate location of data simulation, that is called light absobtion.

INTERNET PROTOCOL: IP is the structural data transmitter which transfer data to the exact points following no barriers. TCP Header control porting and controlling data packages and delivered to the exact IP. IP plays a vital role to data flow and data transmission. Internet Protocol is mainly used in IT sphere. Internet Protocol maintaining the most traffic rules in digital world. Just as the house have exact address all digital gadgets have an exact IP address. TCP/IP balance the speed of the server. The dynamic assigning the network management so that any device can join with the shameless network anytime. An IP address transform within computer, router, IP address.

10 + 20 + 30 40 + 50 + 60

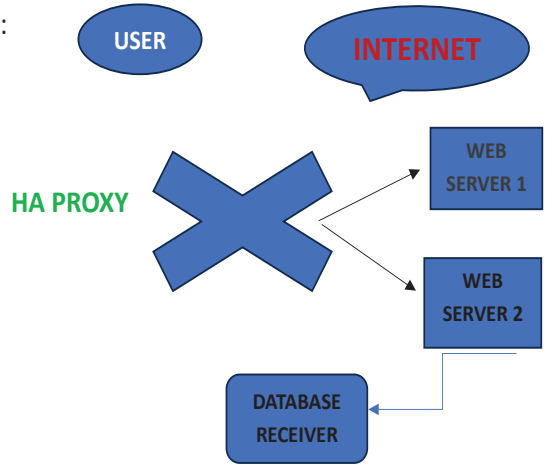


Adapting CWMV can be parallelized and updated online, making it suitable for streaming, real time or large scale of ensemble task

C (log |A|+ m); where m=mistake, C= constant

mod A implies an operator of 'A'

Loading Balance:



HA Proxy inspects traffic and monitor – client behavior when we send a request to server.

FUNDAMENTAL: Function of IP-address is that how a computer work with different server.

How to trace the bug is reacting?

Bug is relationized in to basic traces. That is serverity and priority.

SERVERITY: Serverity tells that how much bug plays a functionality of a function.

PRIORITY: How much bug getting impact to priotism a particular network to fix relation of the task. Effective bug report can ensuring to exact tunning between work flow and QA Report. Bug plays a key impact of a network to trace actual volatility.

Wien's Law of the distribution of energy the dependence of the energy the dependence of the energy U of the resonator upon the temperature is given by a relation of the form:

$$U = a.e^{-b/t}$$

Since, $\frac{1}{T} = \frac{ds}{dU}$; where 's' is the entropy of the resonator, we have for R as used in the text:

R = 1: $d^2s/dU^2 = - bU$

According to Wines's displacement law, energy U transformed to natural vibration period 'v' is explaining as,

$U = v.\ f\left(\frac{T}{V}\right)$; when temperature become high U

became, U = CT; R = 1: $d^2s/dU^2 = - U^2/C'$

putting R = 1: $d^2s/dU^2 = - bU - U^2/C'$

Integrating we get,

$\frac{1}{T} = \frac{ds}{dU} = \frac{ds}{dU} = \frac{1}{b} \log \{1 + \frac{bc}{U}\}$

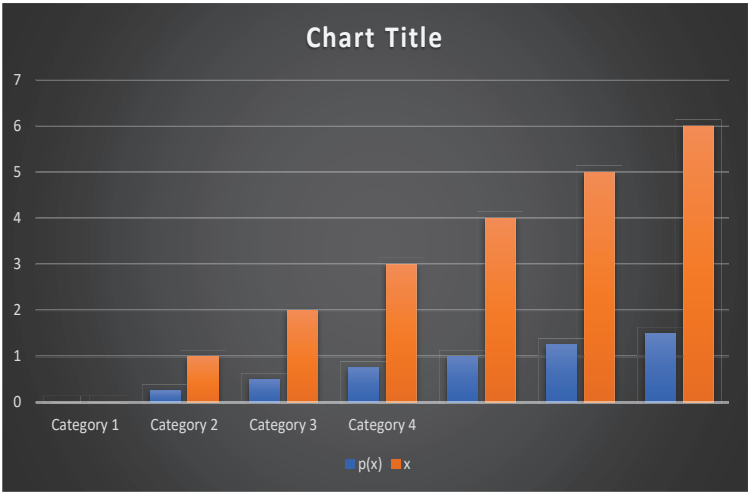
Radiation formula now becomes

$U = bc: (e^{-b/T} - 1)$

Now we explaining statical mechanics and mathematics that probability distribution gives the probability that any system which belongs to a system will be a certain state where state's energy and temperature of the system is distributed in the form $Pi \propto \exp (- €i/k_BT)$;

Where, $p_i \propto \exp (- €_i/ K_BT)$; where p_i is the system in state i, K_B = Boltzmann Constant. Thermodynamics temperature = T

CHAOS THEORY: Initial condition of a system defining in a theory that is called Chaos Theory. Application of Chaos Theory related to biology, physics, chemistry, economics, mathematics.



The above chart diagram symbolized probability distribution of p(x) vs x …

EFFECT OF GEOCENTRIC PARALLAX: Let 'O' be the observer and C be the center of the earth (supposed spherical), then $< CMO$ is the geocentric parallax p, of the body M,

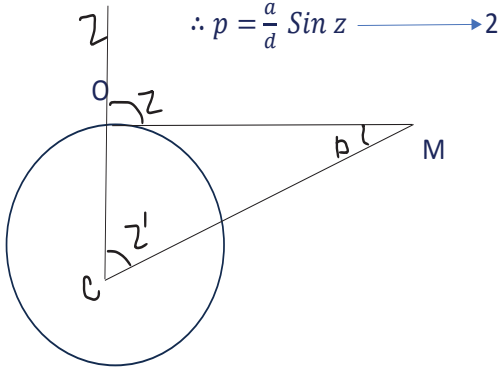
Earth's radius CO produced gives the direction of the zenith of the observer. $< ZOM$ is called the observed (or apparent) zenith distance and $< ZCM$ is called the geocentric (or real) zenith distance of M.

Let 'a' be the radius of the earth and 'd' the distance of the body from the center of the earth. From the triangle ΔOCM,

$$\frac{Sin\ p}{Sin(180°-z)} = \frac{a}{d}$$

$$\therefore Sin\ p = \frac{a}{d} \text{ Sin z} \longrightarrow 1$$

Since p is small, in circular measure Sin p = p



$$\therefore p = \frac{a}{d} Sin\ z \longrightarrow 2$$

When the body is on the horizon z = 90°

If P is the horizontal parallax,

Then P = $\frac{a}{d}$ Sin 90°

= $\frac{a}{d}$

P = P Sin z

Thus, the parallax of a heavenly body varies as the Sine of its observed zenith distance.

If z' is the real zenith distance and z the observed zenith distance of a heavenly body, then from the figure,

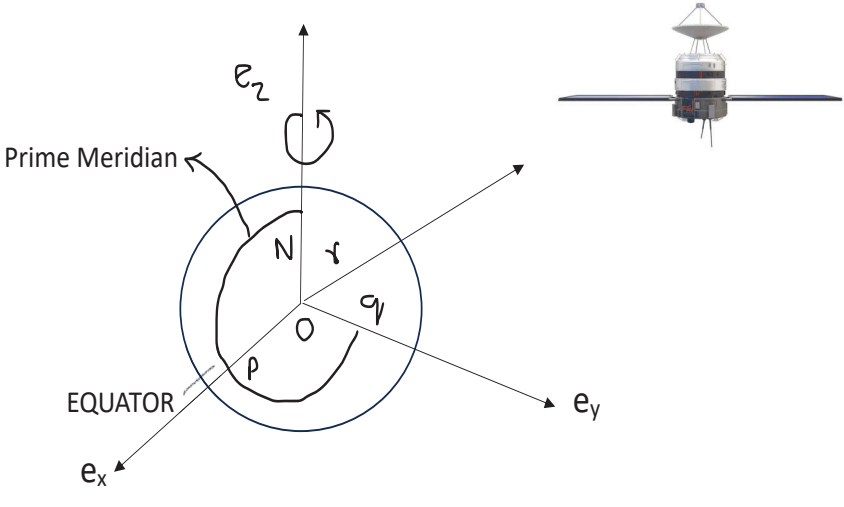
Z' = Z – p = Z – P SinZ

In a geostationary satellite, a 12 GHz radio wave with a transmission power of 160W is transmitted using a 39 dBi gain transmission antenna. The signal is received on the ground below 40000 km. Using a reception antenna, with a gain of 29 dBi. The transmission antenna gain is calculated as (20) times. The receiving antenna is likely not

working at specific points (i, j,l) due to a combination of factors related to signal propagation, the antenna's radiation pattern and potential physical obstruction. The size of average Poynting vector reaching from the receiving antenna is (22)w.20.a.4.b.8.c 40d.80e.400f.800g.4000h.8000k.40000m.8000 21.a.(2.5)*10Λ – 9b.(6.4)*10Λ – 9c.(2.5)*10Λ–10d.(6.4)*10Λ – 10e.(2.5)*10Λ – 11f. (6.4)*10Λ – 11g.(2.5)*10Λ – 12h.(6.4)*10Λ – 12k.(2.5)*10Λ – 13m.(6.4)*10Λ – 13h

Due to polarization mismatch receiving antenna rejecting i,j,l frequency.

KINEMATICS MOTION OF DROPPING A MOTIONARY OBJECT: The earth is modeled as a sphere of radius R that rotates with constant angular velocity Ω in a direction $e_{z,}$ where e_z lies along a radial line that lies in the Earth at point 'O' to the North Pole of the Earth at point N. Furthermore, the center of the Earth is assumed to be an absolutely fixed point.



The position of the satellite is known in terms of an Earth-centered Earth-fixed Cartesian co-ordinate system whose right-handed basis (e_x, e_y, e_z) is defined as follows:

- The direction e_x lies orthogonal to e_z in the equatorial plane of the Earth along the from 0 to P, where P- lies at the at the intersection of the equator with the great circle called the prime meridian.
- The direction e_y lies orthogonal to both e_x and e_z in equatorial plane of the Earth such that $e_y = e_z \times e_x$

Using the basis (e_x, e_y, e_z) to express all quantities, determine the velocity and acceleration of the spacecraft

- As viewed by an observer fixed to the Earth and
- As viewed by an observer in a fixed inertial reference frame. That is how a data spread in the longitude and latitude wise.

Basic projectile motion always depends on gravitational acceleration (primary force). The payload is dropped in the atmosphere of earth, the secondary force that impact its range of accuracy is air resistance.

Air resistance, also known as aerodynamic drag, which create a fictional force and this force minimize the speed of air molecules. Air molecules take a curved parabolic path and motion create a not exactly parabolic path.

Quadratic Drag (Air resistance)

$F_d = \frac{1}{2} C_d \rho A v^2$; F_d = Drag Force(N)

C_d = Drag Coefficient, ρ = Air density

(equals 1.225Kg/m^3) (unitless, ~ 1.05 for a cube)

A= Cross- sectional area of the object(m^2)

v= speed of the object(m/s)

DOMAIN NAME SYSTEM: DNS server sending one msg. to any IP address and computer allowing to load the exact website or page. It mappes the exact domain to the accurate IP address. DNS records are using for identifying exact configure service. Primary categories of DNS systems are:

Generic Domains: Generic Domains are org, net, com and edu. It is widely used in the general system, throughout the world.

Country Code Domain: This domain represents the specific region such as 'in' for India, 'us' for United States, 'uk' for United Kingdom, 'jp' for Japan.

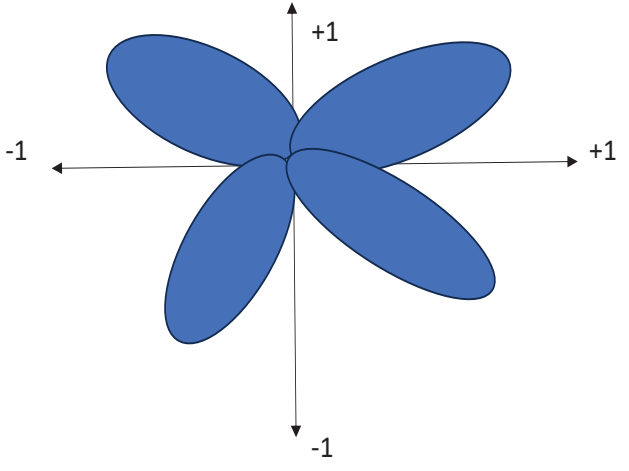
Inverse Domain: These domain helps IP address back to domain name. DNS can map IP address to find the exact website.

API Para diagrams: API is responsible for query language. Where decision flows to another way of "REST" (Para diagram). There are many reasons to select 'SOAP' for security and transaction and 'ACID' for web scenarios. The way "API" circulate data in simulation 'GET','POST','PUT','DELET'. SOAP carries API for durability and own benefit of computer parts. Then we may "Query Language", "SOAP "and "ACID" make a proper triangle for web scenario. For Industry development APIs have play a vital role overall rating 5/10 to generate AI system. Software is complex if the system is complex. Object oriented is the mind of a developer. Developer hoe thinks and judging with an object-oriented paradigm. Object oriented software system connects with a major individual computing model.

PAPER OVER VIEW IN MY EYES (LEARNING OUTCOMES):

HOW IMPLICIT FUNCTION ORIENTED An OBJECT IN COMPLEX SYSTEM? If a fn. Is defined as, $f_i (x_1,\ldots\ldots,x_n,y_1,\ldots\ldots,y_n)= 0$

Where i=1,2, 3……, n then F (xi, y_i) = 0



Now this fn.is diff. at the pt. (x_i, y_i) and m is a variable which is differ a specific section of point.

As object-oriented analysis and design is a complex system. Now we are explaining this as follows. Implicit value does not get any result, then bug reply is none value.

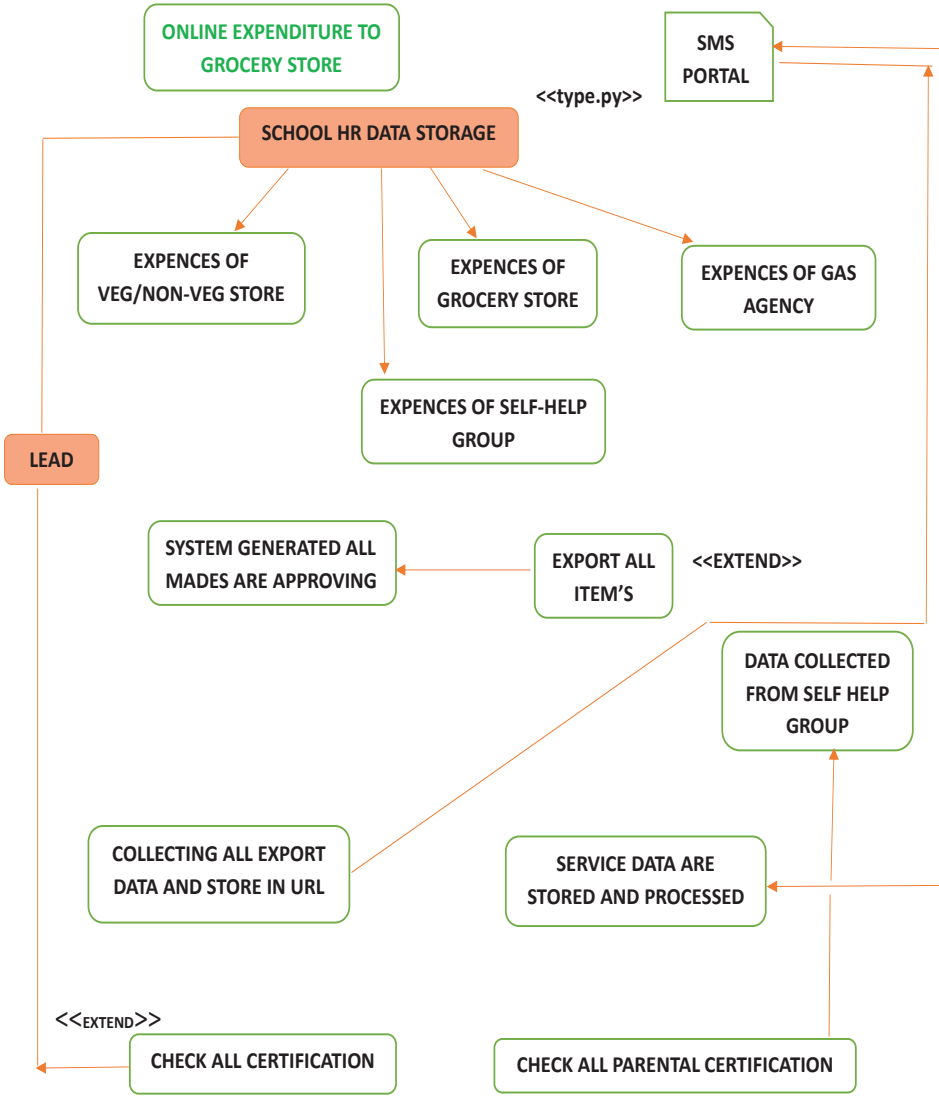
def meow (n:int)→str: return “meow\n*n.

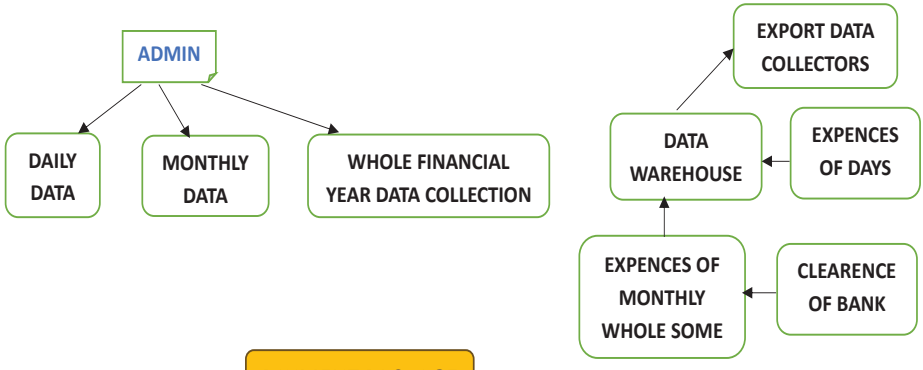
MIDDAY MEAL MANAGEMENT SYSTEM: State machine diagram shows the accurate picture of dynamical system. Life cycle of the class of objects depends on trigger, post condition and past conditions. Time bounding plays a vital role to give accurate msg. to the responding URL. Components are connecting with different ports, which belong in the same interface.

Here I am showing all cases how Midday Meal Management System.

State machine diagram shows the accurate picture of dynamical system. Time bounding plays a vital role to give accurate msg. to the responding URL. Life Cycle of the class of objects depend on trigger, post condition and past conditions. Components are connecting with different ports which belongs in the same interface.

MIDDAY DAY MEAL MANAGEMENT SYSTEM:





PAYMENT PACKAGE

Bank Balance = int ++

def main ()

print ("Balance"; balance)

Deposite (12000)

Withdraw (10000)

Print ("Balance", balance)

def deposite ++ = credit

def deposite -- = devide

Therefore, objects of masses communicated by receiving and sending massages. Diagram shows all the possible core object which we leveling in the data output. That is how the controlled object receiving the exact code of a diagram, which we put in the binary number.

The Java Code of the made for internal interface of stores as follows:

```
Class Ladder {
 public static void main
  (string args []) {int x;
    for (x=0; x<5; x++) {
```

```
    int x;
if(x==1)
system.out.print ln (“expenses of veg/non-veg food item”)
else if (x==2)
system. Out. print ln (“expenses of grocery item”)
else if (x==3)
system.out.print ln (“expenses of gas agency”)
else if (x==4)
system.out.print ln (“expenses of self-help group”)
```

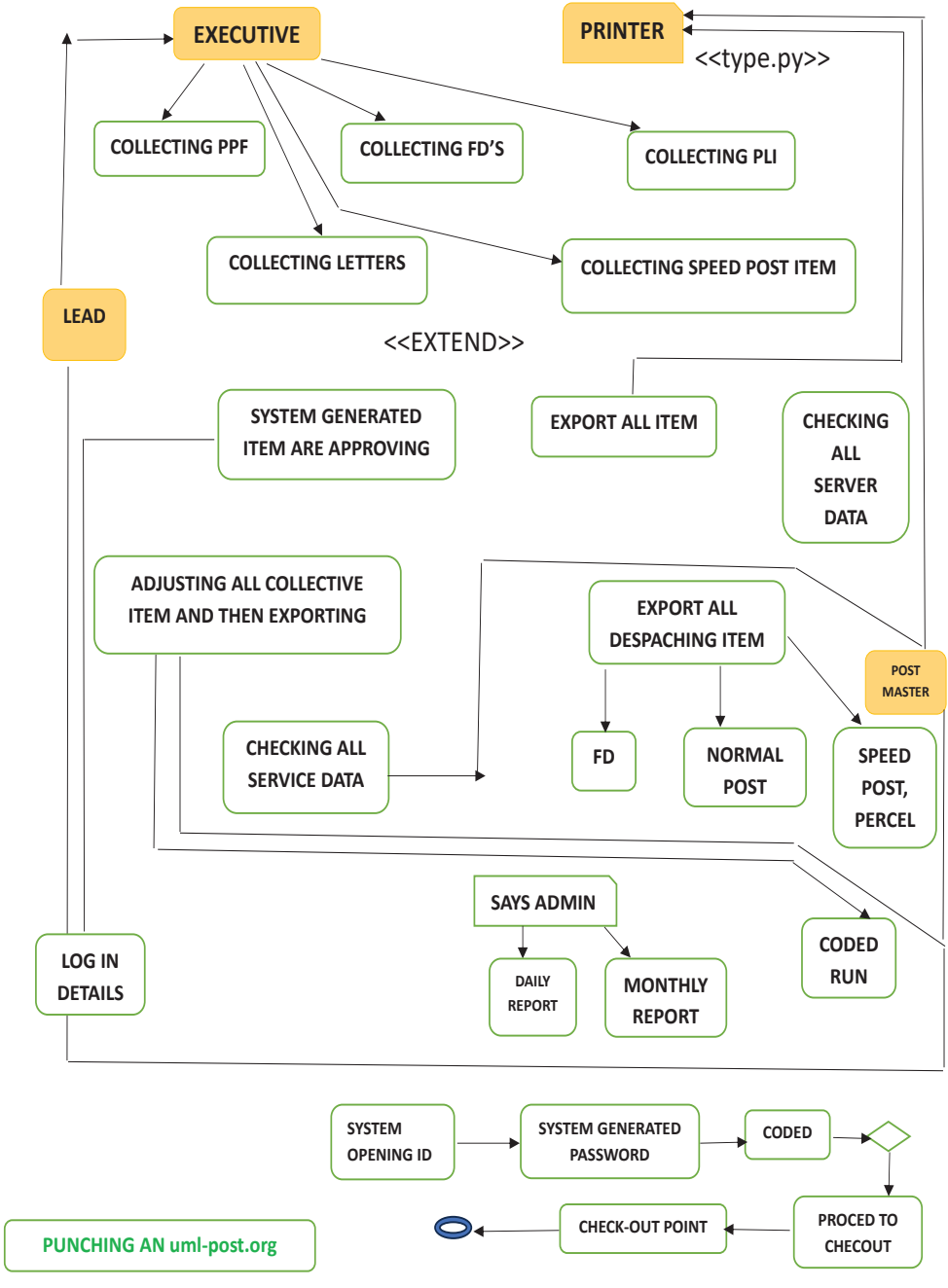
Use of such code old software may convert to new software so that developer may convert communication gap between user and creator.

```
int data storage=4;
switch (data storage) {
case-1: system.out.print ln (“Data collected from self-help group”);
break;
case-2: system.out.print ln (“sms portal”); break;
case-3: system.out.print ln (“export data and store in URL); break;
case-4: system.out.print ln (“service data are stored and processed”);
        }
```

“POSTAL MANAGEMENT SYSTEM”:

Now I am showing a Nested Management system under Postal Management. Here discussing all the possible case how “Postal Management System” moving toward a proper orientation in a

Nested Interface. This model diagram shows how Postal Management System software regulate data in object orientation process.



1.def main ():

……. executive= get – executive ()

…….if executive [0] ==” ppf”:

……..executive [1] =” PLI”

…….. print (f” {executive [0]} from {executive [1]}”)

…….. print (f” {executive[‘ppf’]} from {executive [“PLI”]})

2. def get_Despatched Item ():

……Item = input (“Item:”)

……FD’s = input (“FD’s: “)

……Speed Post = input (“speed post: “)

Setter

3. def main ()

Admin = get_Admin ()

Admin.report =” Daily Report, Monthly Report”

Print (Admin)

Class Dispatching Item:

Despatching ITEM= ITEM ()

Self. Despatching item = [“FD’s”,” Normal Post”, “speed post parcel”]

Print (FD’s, Normal Post, Speed post percel)

4. def get (cls):

post master = input (“post master: “)

Lead = input (“Lead: “)

Printer = input (“printer: “)

return cls (post master, Lead, printer)

TRANSMISSION OF PROJECTILE ION THROUGH O.R.M: In this process energy, ion and charged particle will transfer one body to another matter by the simulation, which is called projectile electron occupation. Each 5^0c increasing of temperature a celestial objected through 10-100 Kvolt energy transmission one heavier matter. Sun-comet-star, planet all of the cosmic particle was oriented through ionization of mechanism of classical physics. Every jump of electron to higher state emission of energy is +ve ly increasing. Generally, we are seen that 1st three jump energy emission is natural level. But the fifth jump is emission become so high, and create a hugh energy.

So, emission of energy follows the rules:

$d \propto \frac{1}{I}$; d = Distance of each shell.

I = Intensity of the charged particle per **spin** use each shell. Here each jump maintains 3.3 Å interconnected force (Radius Value).

The size of the average pointing vector S can be calculated using the Friss Transmission Equation’s pow density part for a directional antenna:

$S = P_{tx} \times G_{tx} / 4\pi R^2$

Given, Transmission Power: P_{tx} =180ω

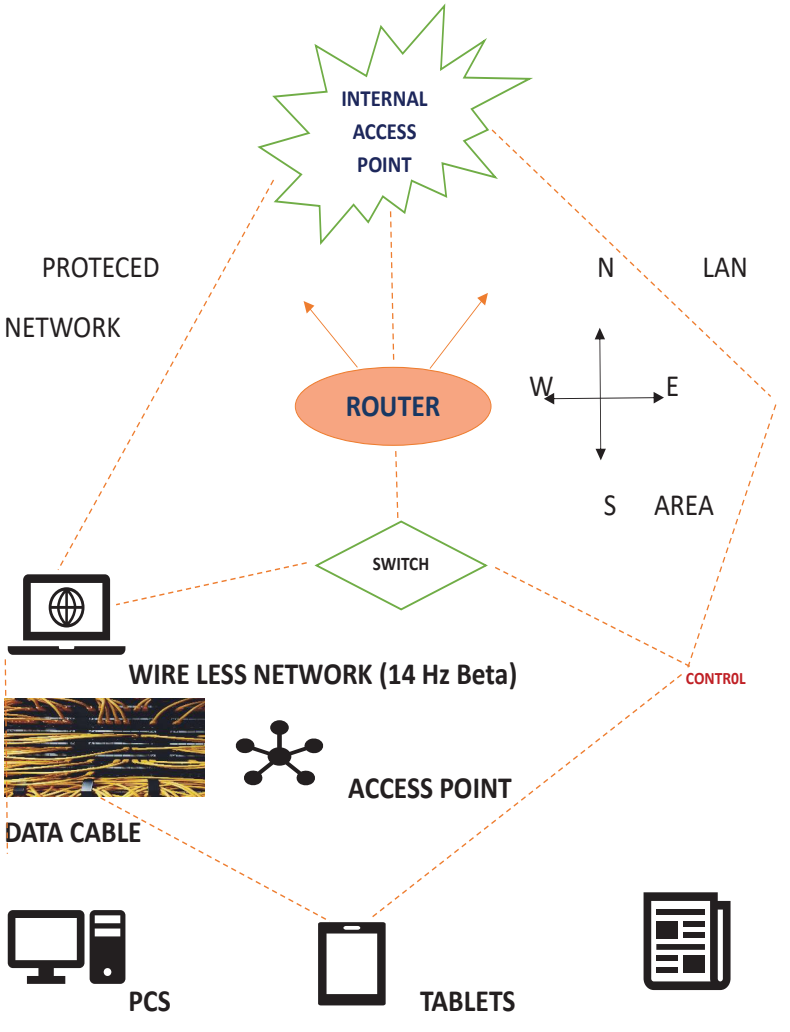
Transmission antenna gains G_{tx} = 7943 (from previous step)

Distance R = 40000 km. = 4×10^7 m.

HOW NATURAL LANGUAGE PROCESSING WORK THROUGH OBJECT?

The coding of natural language processing based on complexity of the text. NLP is not same as human language development process but is developed by some arbitrary object or symbolic orientation. NLP enable AI to convert data in text further more it is applied in different type of ChatBots. Sometimes it sounds like some science fiction but it cores origin of massive data collection which interpreted as Natural Languages. Python interpreted the languages as a text format which we later hypertext as symbolic language transformation that is how non-verbal form.

LAN working field and network: Local area network connected with a wireless communication, here server and network connected through IP address and longitude and latitude effect the Networking speed. LAN user using data by sharing effortless and shameless collaboration. LAN user using peer to peer device which was controlled by one IP address and connected with so many wired networks. LAN is depending on some security issues such that networking permission, access control, end to end connection, where we can easily identity if any unauthorized device connected with the specific network by JEOPARDIZE virus and malware may harm LAN. So, some protected software is monitoring the network so the user gets a protected and safe network connection.



This is how I explain protected network control LAN Area Control.

DATABASE RAPELICATION: If a database crashes by any effect, then the replica will recover the database so that replication save the stored data and, in this process, we save database. Here I am showing that how in 'C'. I convert a database, to replica. We use cloneing to save all objects in one file or server.

```
/*Calculate Database*/
  main ()
    {
Char Name [] = “ENGINE”;
     while (i<=6)
{
print f (“%c”, name[i]);
  i++;
}
} i < = 7, Loop is terminated
```

And here is the output ….

```
  ENGINE
 main ()
 {
char name [] = “NAME”;
    int i= 0
 while (i< = 4)
print f (“% c”, name [i]);
 i++;
   }
      }
```

And here is the output …

```
    NAME
```

```
   main ()
     {
  char name [] = “HOST”;
    int i= 0
while (i<=4)
 printf (“%c”, name[i]);
i++;
 }
   } where (i<=5) loop is terminated
```

And here is the output….

```
    HOST
  main ()
 {
char name [] = “USER”;
    int i = 0
  while (i<=4)
  print f (“%c”, name [i]);
   i++;
 }
   } where i<=5, loop is terminated
```

And here is the output….

```
    USER
  main ()
```

```
{
  char name [] = “PASSWORD”
    int t= 0
while (i<=8);
printf (“%c”, name[i]);
  i++;
}
   } where i<=9, loop is terminated
```

And here is the output

```
   PASSWORD
```

Now using **Kepler’s Third Law** I discuss how a planet’s mass is negligible in comparison to the Sun, so now we understand how a small particle moving around anywhere in planet in a particular Networking Jone.

The force of attraction between Sun and the planet, when a planet is ‘m’ and Sun’s mass is ‘M’ and distance between Sun and the planet is ‘r’ is = $\lambda Mm/r^2$, where λ is the Gravitational Constant.

Also, we say that the planet is attracted toward the Sun with the force $\lambda Mm/r^2$

Here acceleration is $\lambda M/r^2$ toward the Sun.

And toward the planet it is $\lambda m/r^2$

Now relative acceleration of the planet toward the Sun is $\lambda M+m/r^2$.

The time period of the planet in its elliptic orbit of semi-major axis ‘a’ is $T= 2\pi/\sqrt{\lambda(M+m)}\ a^{3/2}$ ⟶ 1

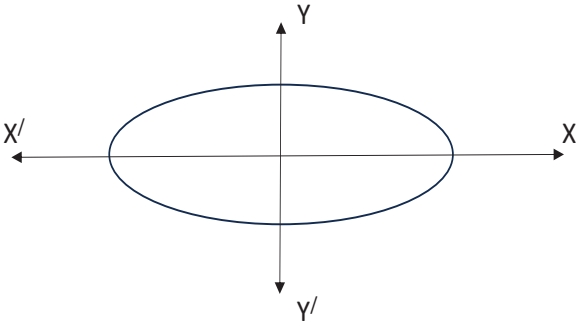
Similarly, the periodic time of a second planet having a mass ‘m’ is given by $T^{/} = 2\pi/\sqrt{\lambda(M + m^{/})}\ a^{3/2}$ ⟶ 2

Squaring and dividing 1 and 2 we get,

$T^2 / T^{/2} = 4\pi^2 \times a^3 / \lambda(M+m) \times \lambda (M+m^{/}) / 4\pi^2\ a^{/3}$

$= (M+m^{/} / M+m^{/})\ a^3/a^{/3}$

$T = 2\pi/\sqrt{\lambda(M + m)}\ a^{3/2}$ and $T^{/} = 2\pi/\sqrt{\lambda(M + m^{/})}\ a^{3/2}$



Newton’s Law of universal gravitation from

How NATURAL LANGUAGE PROCESSING Works through object?

The codeing of natural language processing based on complexity of the text. NLP is not same as human language development process but is developed by some arbitrary object or symbolic orientation object or symbolic orientation. NLP enable AI to convert data in text further more it is applied in different type of Chatbots. Sometimes it sounds like some science fiction but it cores origin of massive data collection which interpreted as natural languages. Python interpreted

The languages as a text format which we later hypertext as symbolic language transformation that is how non-verbal text covert into verbal form. Here I am trying the analysis one voice interpretation range in audio waves.

In Fast Fourier Transformation we convert signal w.r.t frequency and distance. Now we measuring the duration of sampling rate 'BL' stands for Measuring Duration, 'fs' stand for frequency and 'D' stands for Duration…

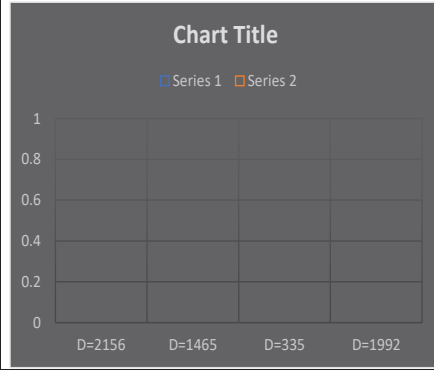
$$\mathbf{BL} = \frac{D}{fs}$$

$$\therefore \mathbf{D} = \frac{BL}{fs}$$

$$= \frac{2156}{15 \times 1000}\ \mathbf{s}$$ (Distance between Malda to Mumbai

$$= \mathbf{.143}$$ = 2156)

MUMBAI	DELHI	KOLKATA	CHENNAI
D=2156 Km	D= 1465 Km	D= 335 Km.	D= 1992 Km.
fs = 15 Khz	fs= 15Khz	fs=15Khz	fs=15Khz

BL=.143	BL=.097	BL=.022	BL=.132 

Now I create a program that display the frequency, timing and distance relation.

```
Import win sound
 f = 4000    # frequency
 d= 4000    # timing
  win sound (f, d)
          (f, d)
```

COLCLUSION: The world is viewed by collection of objects. Different objects are oriented with different problems. It also oriented with different behavior, different attributed or need deep testing states.

When a class become real, it oriented physical to another world. When a class seemed to be logical, it oriented logical-world. Object oriented programming has several limitations; it needs appropriate planning to construct a proper program. You can use to solve so many different problems. It also needs deep testing. It also jumps one program to another maintaining the accuracy to create a perfect

program. Its implementation modified both parent and child class. In this paper I try to established some practical exercise of interface as well as implementation. The object-oriented programming makes method of beneficial collaboration to build a developmental in code sustainability, and efficiency. However Object Oriented Programming is not focused in making computer algorithm or actual program.

DATABASE PRIVACY AND SECURITY IN CRYPTOGRAPHY FOR SMART CITY

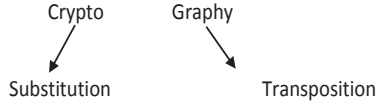
Author 1
Smita Ghosh, Msc. Mathematics M.S. University.

CONTENTS

X. L. ABSTRACT……2
X. 2. INTRODUCTION……3
X.3. FUNDAMENTAL OF DATABASE-PRIVACY AND SECURITY IN CRYPTOGRAPHY……4
X. 3.1.1. HOW DO WE KNOW IF A CRYPTOGRAPHIC TECHNIQUE IS "SECURE" ?.....5
X. 3.1.2. SIMPLE CIPHERS……5
X. 3.1.3. CAESAR CIPHER……5
X. 3.1.4 SHIFT CIPHER……6
X. 3.2. SUBSTITUTION CIPHER: CRYPTANALYSIS……7
X. 3.2.1. FREQUENCY ANALYSIS……7
X. 3.2.2. CRYPTO QUIP……8
X. 4. CRYPTO GRAPHIC HASH FUNCTION……8
X. 4.1. APPLICATION OF HASH FUNCTION ……9
X. 5. #DIGITAL SIGNATURE……11
X. 5.1. SHA-256 HASH FUNCTION ……14
X.5.2. FILE CHECKSUM ON DIGITAL SIGNATURE……15
X. 6. AES / ADVANCED ENCRYPTION STANDARD ……16
X: 6.1. AES - 128 SP CORE ……16
X. 6.2. DATA - AT – REST ENCRYPTION AND DECRYPTION……17
REFERENCES……18

X. 1. ABSTRACT:

"Cryptography " the word Is the combination of two words.



"To solve an encrypted message... find a different plaintext of the same language long enough to fill one Sheet or so, and then count the occurrences of each letter. Call the most frequently occurring letter the first, the next most occurring the second ... and so on. Then look at Cipher text ... and also classify its symbols. Find the most occurring symbol and change it to the first letter.... the next most common symbol is changed to the form of the second letter... and so on, until we account for all symbols of the cryptogram we want to solve." – A1–Kindi.

Data security is an imperative aspect of any database system. It is of particular importance in distributed systems because of large number of users, fragmented and replicated data, multiple sites and distributed control.

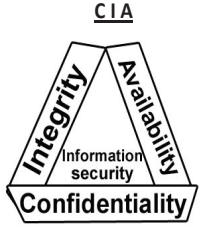
Now in Cryptography we encoding information before sending via unreliable communication paths so that only an authorized receiver can decode and use it. The coded message is called Cipher text and the original message ies called plain text. The process of converting plain text to cipher text. The process of converting plain text to a cipher text by the sender is called encoding or encryption. The process of converting cipher text to plain text by the receiver is called decoding or decryption. In this paper i focused on how a "Cryptographic hash function" maps data of arbitrary size to a fixed size and has secure some special properties. At a high level, a hash function can be thought of as a hard - to - invert random - looking function. While it may work for certain purposes. Studding cryptanalysis is difficult because there is no suitable standard text book. Therefore, the proposed research is to organize the existing literature of database encryption can use to learn first survey of the most relevant concepts of cryptography.

KEYWORDS:
Database Security, Cryptography, Cryptographic Hash Function, Hashing Password, Digital Signature.

X. 2. INTRODUCTION:

What is Database Security?

Database security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and attacks.



- Confidentiality
- Integrity
- Availability

1. Now what is the Anatomy of an Attack"?

http:// map.norsecorp.com/ #/

The above link by Norse gives us a visual representation of the real time attacks happening across the world this very second! It clearly demonstrates why we need to secure our databases. Symantec estimates than in 2015, .500 million identities were exposed.

with an estimated world population of 7.4 billion, this translates to "7% of the world population was exposed to hackers."

Security Threats: Most common attacks

- SQL Injection
- Buffer Overflow vulnerabilities
- Denial of Service (DOS) attacks

- Weak Authentications

Now explaining clearly the above topics : 1st,

SQL Injection: Attacker inserts malicious code into the database Program to exploit the vulnerabilities in the application.

Buffer overflow: exists when a program attempts to put more data in a buffer than it can hold.

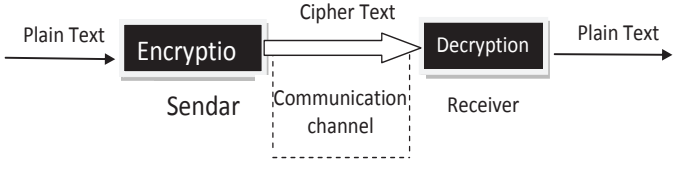
DOS attack: is a cyber-attack where the attacker makes a machine or resource unavailable to its intended users by flooding the machine with superfluous requests in an attempt to overload system.

Weak authentication: attacker can steal the identity of a legitimate user, gaining access to confidential data.

Now what is cryptography ?

Simple meaning of cryptography is confidentiality.

"Cryptography" - is the Science of encoding I information before sending via unreliable communication paths so that only an authorized I receiver can decode and use it.



X. 3. FUNDAMENTAL OF DATABASE PRIVACY AND SECURITY IN CRYPTOGRAPHY:

Cryptography, the art and Science of keeping information secure. It deals with the design of algorithms for encryption and decryption, intended to ensure the secrecy and/or authenticity of the data including: symmetric and Asymmetric Encryption.

The work Cryptography is Greek

- Crypto : secret

- Graphy : Writing

Basic goal is to send messages that no one but the expected recipient can read – We can do so much more, though!

X. 3.1.1. HOW DO WE KNOW IF A CRYPTOGRAPHIC TECHNIQUE IS "SECURE"?

- we let lots of really smart people try to break it (crypt analysis)' - If they can't, we assume it is secure.

X. 3.1.2. SIMPLE CIPHERS :

- Problem: We might be wrong.
- Originally, Cryptographs was performed by hand
- Goal was to protect messages sent by couriers

  - From people who might intercept the courier

  - From the courier himself
- War was a popular time to use them

X.3.1.3. CAESAR CIPHER:

- Ear least documented 'Cipher' was used by "Caesar".
- Each letter in a message is substituted by another that is 3 Letter's away.

  -A becomes D,

  P becomes S, etc.

Example:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

let's do one for N=10....

ATTACK	AT	DAWN
DWWDFN	DW	GDZQ

X. 3.1.4. SHIFT CIPHER:

- Generic version of Caesar Cipher
- Each letter is shifted by N

- In Caesar, N=3

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Let's do one for N=10 ---

ATTACK	AT	DAWN
KDDKMU	KD	NKG X

SHIFT CIPHER : CRYPTANALYSIS :

- How do we break this?
- Brute – force : Try all possible values for N

  - There are only 26
- Feasibility ?

  - Easy by hand

  - Trivial by Computer

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	A	W	G	N	C	X	M	B	V	L	Z	D	S	J	T	E	K	Y	F	U	I	P	O	H

- Generate a random set of substitutions for each letter.

-Always A 1 1 correspondence.

X. 3.2. SUBSTITUTION CIPHER: CRYPTANALYSIS :

- Brute force: Try all possible letter combinations – There are (26!)
- Not going to do that by hand-

  Q Y YQ A V Q Y W Q I D

- Key observation : In a Substitution cipher, basic language features are preserved …….

- You can tell how often a letter occurs in the message

- You can see when letter repeat

- Etc.

X. 3.2.1. FREQUENCY ANALYSIS :

- A cryptanalysis technique described & in the 9th century by Al-Kindi in Iraq.
- Not all letters in a language occur with the same frequency.
- Languages have certain features.
- In English ...

-E is most common.

- vowels are about 40%

- vowels tend to be separated by consonants.

-Q tends to be followed by V. etc.

Frequency Analysis:

Performing frequency analysis on substitution Ciphers is a news paper puzzle!

CRYP TOQUIP

HOITD	OF	LHOIB	FJ	ZDBH
AU	NZPJ	P	NXPTAOTPZ	
RUMD	JUL	FOBGA	HPJ	AGPAH
RLHA	PI	PX FZDHH		NXPIM

X. 3.2.2. CRYPTO QUIP:

I GUESS THE MEN WHO INTRODUCED COMMUNAL MELTED – CHEESE DISH TO ALEO AMERICA WERE FONDUING FATHERS.

All of the previous techniques have two basic components :

- Algorithm (what you do to the message)

- Key (The secret that you need in order to encrypt/decrypt properly)

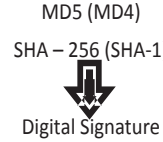
Hiding message contents is probably! the first concept you think about when you think about Cryptography. The encrypt function has the property that given the output (Cipher text), it's hard to determine the input (plaintext) without the key. The decrypt function has the obvious correctness property, that decrypt (encrypt (m, k); K) = m

The encrypt / decrypt functions have properties Similar to their analog form Symmetric cryptosystem. A message can be encrypted using the public key. Given the output (Cipher text), it's hard to determine the input (plaintext) without the private key. The decrypt function has the obvious correctness property , that decrypt (encrypt (m, public key), private key) = m.

Out comes of review and research direction

X. 4. CRYPTO GRAPHIC HASH FUNCTIONS :

This functions are basically fun damental building blocks that are used within many cryptographic algorithms and protocols and they have a number of very important applications in the context of information security as a whole. Now some of the more common algorithms in this category that are known as cryptographic hash functions include: things like MD5, and also, it has some : predecessors :



like MD4 and others, as well as algorithms like SHA-256, by other algorithms like SHA-1 and so on, and also there are some algorithms that may be you've heard of, or maybe o that are a bit lesser known but things like RIPEMD, and BLAKE and Skein and others. Now Cryptographic hash functions are basically used to blocks in many

applications, and the first the historical application of these types of hash functions was in the context of what's known as a Digital Signature, and digital Signatures are used in so many different cryptographic applications today. There're the cornerstone of may ecommerce protocols. They are used in doing things like bitcoin generation and so on. Now by Hash function I basically mean that it will take input and message can be of arbitrary Length and hash function applies digest a mathematical transformation and or maybe a set of mathematical transformations to this un put to produce a single output, and we typically call this output a digest, although, sometimes you will see the output referred to as a tag, or as a hash, or as a fingerprint but digest is sort of the most common nomenclature. The output always be the same for a given input, so if you have a given input you're going to see the exact same output.

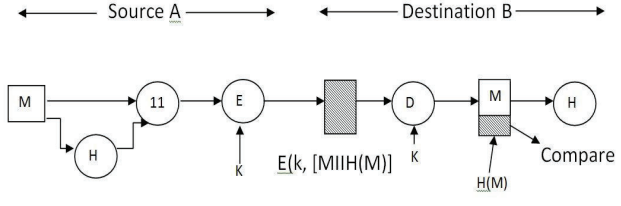


(tag, hash)

Therefore purpose of hash function is to verify the integrity of a message. Massage authentication and hash function assure that data received are exactly as sent by sender.

X. 4.1. APPLICATION OF HASH FUNCTION :

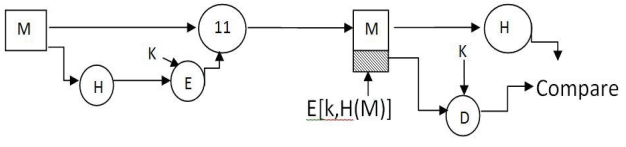
#1



- In the above figure, hash code is generated from message and then appended Ho message.
- The Message plus concatenated hash code is encrypted using symmetric encryption.

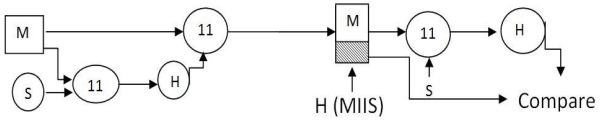
- Because only A and B share the secret key (K); the message must have come from A and has not been altered.
- The hash code provides the structure on redundancy required to achieve authentication.
- Encryption is applied to the entire massage plus hash code, confidentiality is also provided.

#2



- In above figure, hash code is generated from given message.
- After generation of hash code, it is encrypted using secret key (K).
- Them encrypted hash code is append with original message and send to the receiver.
- It reduces the processing burden for those applications that do not require confidentially.

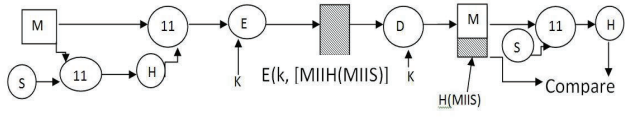
#3



- It is possible to use a hash function but 8 no encryption for message authentication.
- The technique assumes that the two communicating share a common secret value S.

- A computes the hash value over the concatenation of M and S, appends the resulting hash value to M.
- Because B possesses, it can recomputed the hash value to verify.
- Because the secret value itself is not sent, an opponent cannot modify an intercepted message and cannot generate a false message.

#4



- Confidentiality can be added to the approach a previous method by encrypting the entire message plus the hash code.
- When confidentiality is not required, method (2) has an advantage over methods (1) and (4), which encrypts the entire message, in that less computation is required.

X.4.1.A. Application of Hash function:

QR code (stands for Quick, Response code) in 2D barcode, it QR Carries data in two dimensions. It is designed by Denso wave in Japan and 1st use in 1994 for the Japanese in that they are one of the most efficient ways of encoding Japanese Character as Fig 4



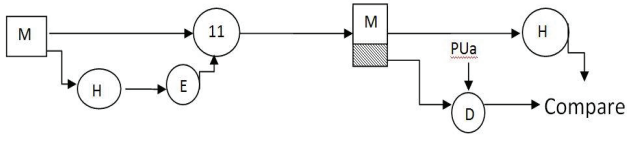
Since to QR code carries information both horizontally and vertically, QR code is capable of encoding the same amount of data in approximately one-tenth space of a tradition barcode. QR coda has error correction

capability Data can be restored even if the symbol is partially des dirty or damaged. A maximum 30% of code words *1 can be restored * 2.

*1! A code word is a unit that Constructs the data area. In the Case of QR Code, one code word is equal to 8 bits.

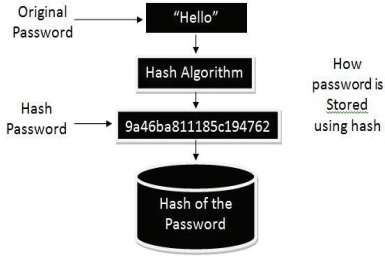
*2 : Data restoration may not be fully performed depending on the amount of dirt or damage. Readable from any direction of 360°

X. 5. # DIGITAL SIGNATURE (AUTHENTICATION ONLY) :

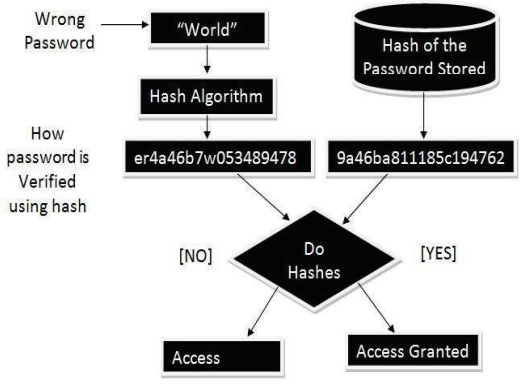


- Another important application, which is similar to the message authentication application, is the digital signature.
- Purpose of digital signature is verify sender's signature to achieve authentication.
- In this case of the digital signature, the hash value of a message is encrypted with a user's private key PRa. Anyone who knows the user's public key PUa can verify the integrity of the message. It also provides a digital signature, because only the sender could have produced the encrypted hass code.

APPLICATION : HASHING PASSWORD



- Hash functions are commonly used to create a one - way - password file.
- A hash of a password is stored by an operating system rather than the password itself.
- Thus, the actual password is not retrievable by a hacker.
- Who gains access to the password file. In simple teams, when a user enters a password, the hash of the password is compared to the stored hash value for verification.

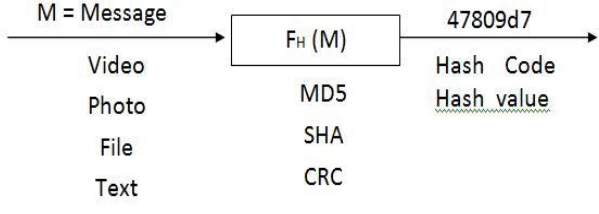


- This approach to password protection is used by most operating systems.
- Hash functions also can be used for “intrusion detection” and "virus detection". Now following table shows you how “Hash Function” Resistance Properties Required for various Data Integrity Applications.

	Preimage Resistant	Second Preimage Resistance	Collision Resistant
Hash + digital signature	yes	yes	yes
Intrusion detection and virus detection		yes	
Hash + symmetric encryption			
One – way password file	yes		
MAC	yes	yes	yes*

*Resistance required attacker is able to mount a chosen message attack.

Now the following diagram clear everybody How "Hash function actually work."

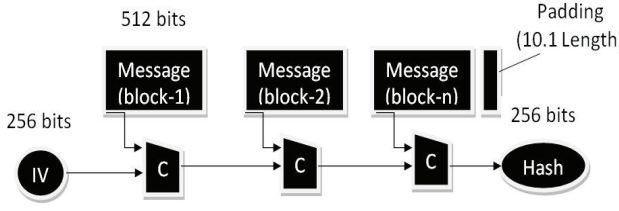


PROPERTIES

M ⇄ H (Easy / Hard) H→Fixed Length M1→H1, M2→H2

M > H ⟶ Compression Function $H_1 \neq H_2$ → Collision Free

X. 5.1. SHA –256 hash functions:



So, what is SHA - 256 ?

It is SHA-256 TP Core. The cryptographic hash function is the algorithm to map data from arbitrary size to fix size as a one-way function which is needed for information secretary application. And one of the most well known is SHA 256. SHA stand for "Secure Hash Algorithm" It is used to generate 256 bits of hash is value from any length of input message.

Complaint with FIPS 180-4 Input data length up to 261 bytes compute 512-bit data block in just 65 clock cycle.

Through put 1.575 Gbps@ 200 MHz easy to with this cores.

Each message would have its own hash values so it is impossible for two inputs to have the same hash value. Now Let see SHA – 256 IP core specification :

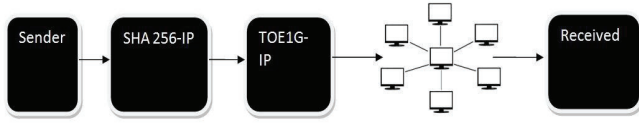
It's implemented secure Hash standard FIPS 180-4 with the maximum input message length message length is up to 2 (61) bytes. It can compute 512bit data block in just 65 clock cycles. The performance of SHA-256 is 7.875 Mbps throughput per 1 MHz or 1.575 Gbps at 200 MHz. Most importantly it's easy to and networking IP, SHA 256-IP enable more opportunity to create secure efficient and high-performance application.

Here is the example application of SHA – 256

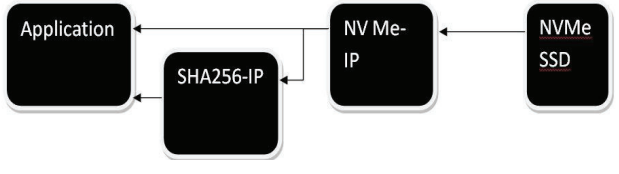


for message or best data block verification. It just give an example, then you want to ensure that the data has not changed - You can compare the hash of your file to the original one which usually provide in the website you got the data from. And if the two hashed message are matched then the data file is correct.

X. 5.2. File checksum on Digital Signature :



Now this block diagram shows you the example how to use SHA-256 together with our Networking IP. The transmitted data is hashed by SHA 256-IP in form of file checksum or digital signature, then Send through the network with TCP/IP protocol implemented by TOE1G- IP. Another example is for using this data storage IP, when user request to read data from the SSD. You can connect with our NVMe-IP and hash the read data with SHA 256-IP.



if you need to improve the performance you can multiple the & SHA256-IP like this.

X. 6. AES/ADVANCED ENCRYPTION STANDARD



- Some key is used for encryption and decryption.
- Support 3 key length ; 128, 192, 256 bits
- Brute - force attack is practically impossible.
- Specify FIPS POB 197 .

  Now I introduced to you the ASE-128 IP Core.

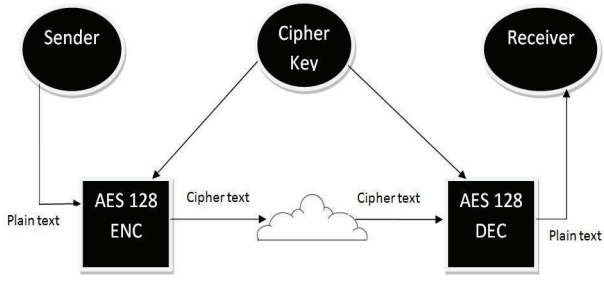
X. 6.1. AES-128 IP CORE

Specification →

- Complaint with Advanced Encryption Standard o FIPS PUB 197
- Support AES ECB mode standard for both encryption and decryption.
- Compute 128-bit data block within constant 11 clock cycles
- Performance : 11:6 Mbps through put per 1 MHz clock or 2.9 Gbps@ 250 MHz.
- Easy to use with Design Gate way's Data Storage and Networking IP cores



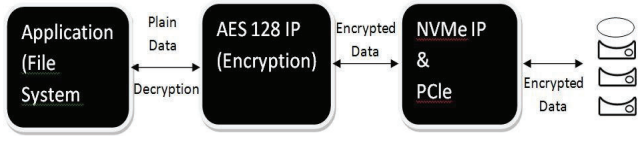
Secure Data Transfer :



AES provide you a high speed and secure data System to adapt.

X. 6.2. DATA - AT - REST ENCRYPTION AND DECRYPTION :

One of the example of A ES-128 IP encryption :



NVMe SSD

You can connect AES-128 IP · Before Storing data in NVMeIP and decrypting data when you read want to read out. Data is a valuable assets of an Organization. So, its Security is always a big challenge for an organization.

X: 7: ILLUSTRATION OF Database for privacy and Security :

To eliminate the security the threats every organization must define a security policy In recent times security of shared databases was studied through cryptographic view paint. A new framework was proposed in this paper in which different keys are used by different parties to encrypt the database, Database Privacy is a concept that is organizations have the responsibility to protect clients information,

because their clients entrust them to do so. Sensitive, confidential and critical information is often kept in database. To protect this information & being accessed by third-parties without clearance, companies and organizations have to be diligent about data protection. Some of their efforts have to center on guarding against threats to application servers, database Servers and storage systems. Privacy professionals also can secure. Storage Systems against theft involving servers hard drives, desktops and laptops Encryption methods might be employed to help protect applications and data based on their sensitivity levels. It an Organization can detect exploits or indications of database compromising before the threat becomes real and unmanageable, the database might be able to be rectified with little and reversible damage.

CONCLUSION :

To eliminate the security the threats every organization must define a Security policy. In recent times Security of shared databases was studied through cryptographic view paint. A new framework was proposed in this paper in which different keys are used by different parties to encrypt the database. Different Governmental, non-governmental and private and many other organizations have sensitive data or web servers that really need to be protected from the attackers or intruders. To make the database Secure different Security techniques were developed. One of them is encryption techniques. Though encryption improves the protection but its implementation decisions are also very important. Developing the encryption strategies arise some important questions also, like how, when and where the encryption will be performed. Using some Hash functions we reduce the performance. My study have recognized some limitation. The future work could be carried out make encryption more effective and efficient.

REFERENCES :

1) ISO/TFC en Information Security management standard 2005.
2) C.-C. Chang and C.-W. A database record encryption scheme using the RSA public key Cryptosystem and its master keys. In ICCNMC '03: Proceedings of the 2003 International conference on Computer Networks and Mobile computing, page - 345 , Washington, DC, USA, 2003, IEEE Computer Society.
3) A.O. Freier, P. Karlton and P.C. Kocher. The SSL protocol Version 3.02, 1996.
4) W.K. Wong, D.W. Chung, E. Hung, B. Kao, and N. Mamoulis. Security in Outsourcing of association rule mining. In VLDB '07: Proceeding of the 33rd and international conference on Very Large data bases, pages Ill-122 , VLDB Endowment, 2007.
5) http://searchsecurity.techtarget.com/definition/privilage-escalation-attack.
6) R. Canetti. Security and composition of multiparty cryptographic protocols. Journal of Cryptology. vol. 13, No-1, PP.143- - 202, 2000]]
7) http://www.freetechexam.com/computerstips/computertips/database - security.html.
8) Tingjian Ge, Stan Zdonik, fast, Secure Encryption for indexing in a column Oriented DBMS: 2007 IEEE, 23rd international Conference on Data Engineering (2007). Publisher : IEEE Page (S): 676-685
9) http://en.wikipedia,ong/wiki/Database-Security
10) Tanya Bacca ; Making Database security an IT security Priority a SANS Whitepaper November 2009.

THE INSANE ENGINEERING OF THE PERSEVERANCE ROVER

Author : Smita Ghosh

WEST BENGAL SCHOOL DEPARTMENT, e-mail : smitaghosh04@gmail.com

Abstract:

Human rover drives on Earth heavily rely on semantic information from rover images to plan a path. The manually planned drives by human rover drivers are able to use this semantic information about terrain types to drive over longer distances and over challenging terrain that would otherwise cause faults when using Auto Nav and en danger the rover's hardware. NASA's Mars rovers have possessed an autonomous driving capability, called Auto Nav. This paper provides a snapshot of the dataset as it currently stands. I have a plan to continue making improvements and additions to the dataset, including the images from the new Mars Rover Perseverance. Deep learning has quickly become a necessity for self-driving vehicle on Earth. In contrast, the self-driving vehicle on Mars, including NASA's latest Rover. Earth is the only planet on which a variety of public are available to humans.

Key words:

Hierarchical path planning, autonomous navigation, see back effect, Mars 2020 rover, Machine learned heuristic.

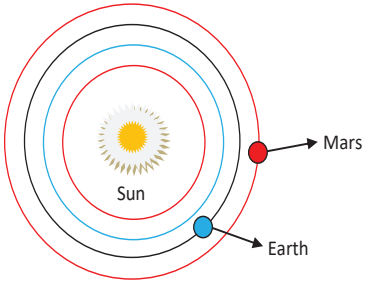
Introduction:

Uses machine-learning algorithms such as energy-aware path planning and scheduling, information-theoretic path planning. The thermal inertia algorithm works on variables like thermal conductivity of a material, its density, specific heat capacity of the surface. The thermal inertia

algorithm works on variables like thermal conductivity of a material, its density, specific heat capacity of the surface.

In order to learn more about Mars, NASA. Scientists often look at surface changes as a result of avalanches, Sand storms and meteorite strikes. One such surface change is the creation of creators. This scientists have previously discovered thousand new craters by manually inspecting images from the Mars. Reconnaissance orbiter. This space craft was orbiting Mars for around 14 years. So that's a lot of images with potential craters in them but the one problem is that it takes scientists up to 40 mints just to inspect one image for any creators, Simulation of "dust devil" from data provided by the Mars

Reconnaiss ance Orbiter.



The Robot is designed to hunt for signs of past microbial life, if it ever existed. It is the first NASA Mission to hunt directly for these “bio signatures" since the Viking mission in the 1970s.

The rover will collect Samples of rock and Soil, encase them in tube, and leave them on the planet's surface to be returned to Earth at a future data.

Perseverance will also study the Red Planet's geology and test how astronauts of future, Mars missions could produce Oxygen from co_2 in the

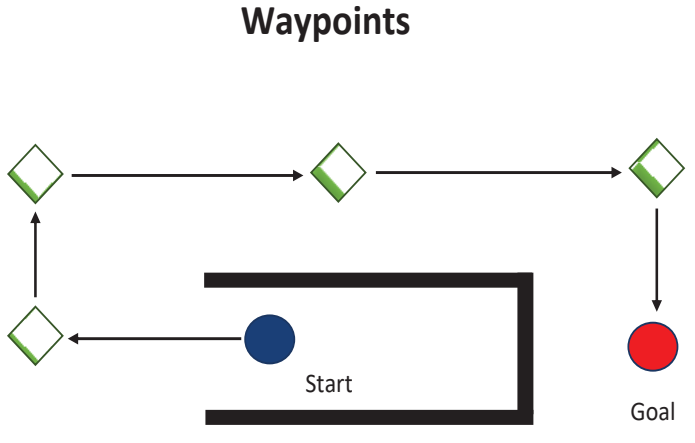
atmosphere. The Oxygen could be used for breathing and rocket propellant.

Hierarchical Path Planning: -

Long distance planning is challenging for the existing planner which mainly relies on local information.

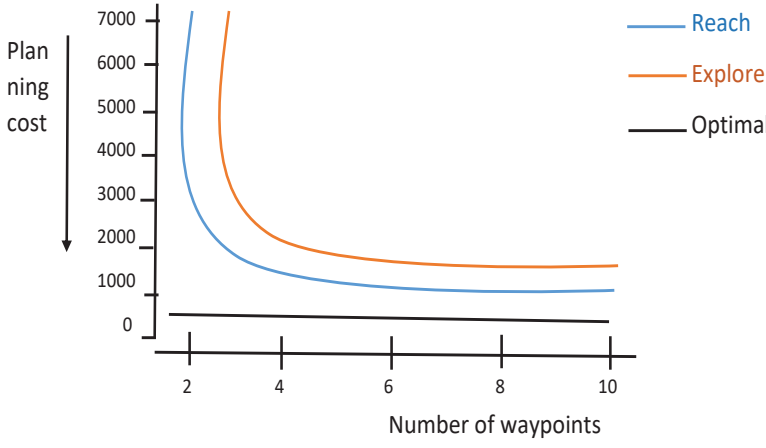
We propose to utilize hierarchy in planning tasks:

1. Use global information to define sub – problems for planning in the form of waypoints.
2. Use the existing planner to complete plans connecting waypoints.



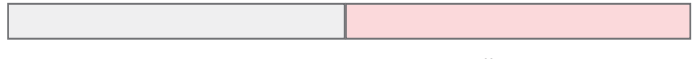
Preliminary experiments show a 10x reduction in planning cost when used with the A* algorithm if an export places the waypoints.

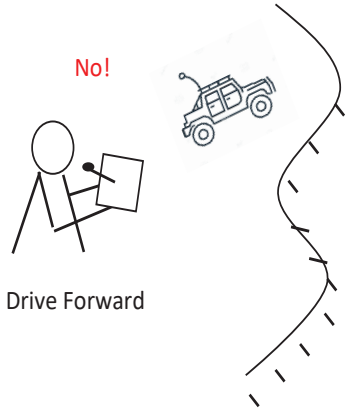
Work is underway to design machine learning models for automatic waypoint placements from global map information.



Autonomous Navigation: -

Spectrum: -





Heuristic Approach

- Practical rule or behaviours
- Not guaranteed to be optimal
- Doesn't need complete, environment information.

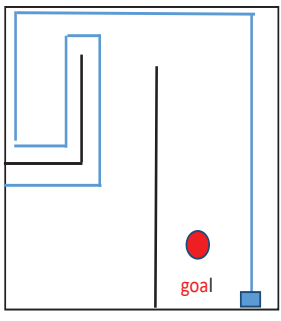
Optimal Approach

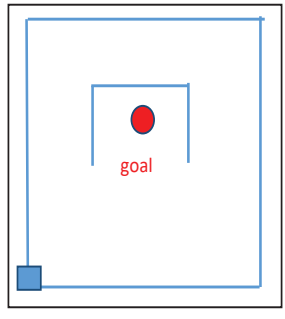
- Requires more environment information
- Planning is achieved through optimization

Heuristic Approach: -

- Practical rules or behaviour.
- Not guaranteed to be optimal.
- Doesn't need complete environment information.

Maze solving vehicle

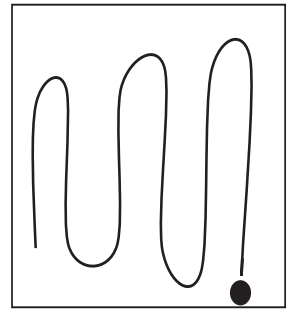




drive forward keep will on left

Optimal path

Robotic Vacuum

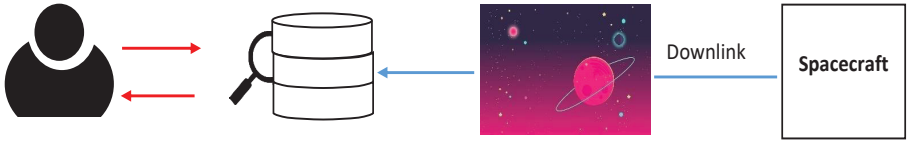


drive forward random turn at obstacle

Navigation is the ability to determine your location within an environment and to be able to figure out a path that will take you to a goal. This is an overview of how we get a robotic vehicle to do this automatically.

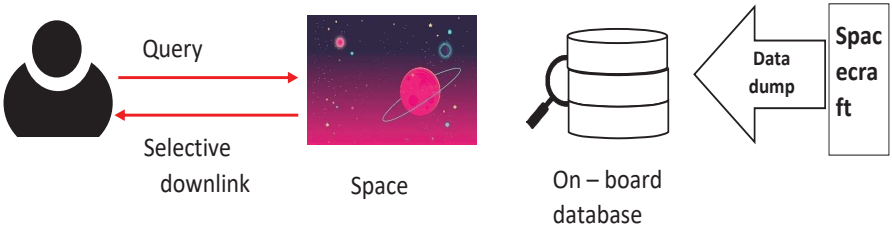
Drive – by Science: -

Current – paradigm: -



Space

Drive – by Science



The rover's goals include looking for past Martian environments capable of supporting life, seeking out possible microbial life in those environments, collecting rock and soil samples to store on the Martian surface, and testing oxygen production from the Martian atmosphere to prepare for future manned missions.

Literature Review :

Fundamental:

Many scientists believe that millions of years ago, Mars had an atmosphere and liquid water, conditions where life could thrive. Humans have looked for signs of life on Mars science telescopes could first scan its surface. In 1877, Giovanni Schinaparelli mistakenly thinks he sees irrigation or transport canals crisscrossing the Martian landscape. In 1976, the Viking probe sends back low resolution photos wrongly identifying pyramids and a giant Sphinx-like face. But in 2016, Mars Reconnaissance orbiter beams back higher quality images of what some have interpreted as the ruins of Bronze age-styled walled cities. Obviously, a civilization in that state wouldn't have had the capability to blow themselves up with nuclear weapons, which means that somehow some other predatory alien race must have intervened. Imagine the inhabitants of this Martian civilization. All of a sudden there's huge flashes of light and heat, destruction that reigns everywhere and everything you've ever know was destroyed in an instant. It literally would have been hell on Mars. The weapons not only wiped out the civilization, but basically destroyed the biosphere of Mars so it could never recover.

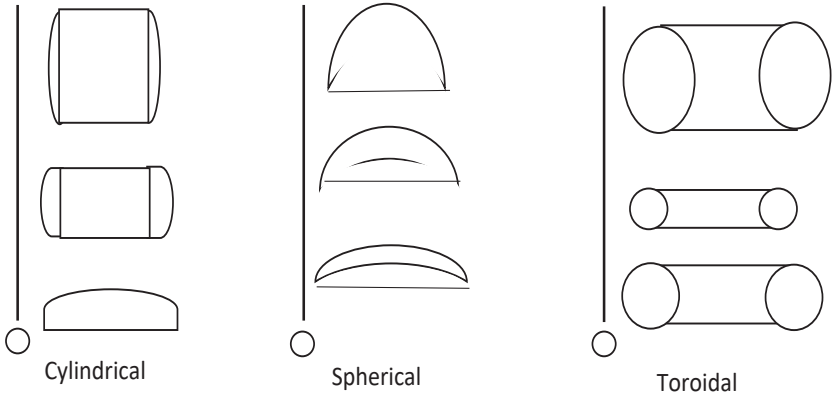
Ground – based Energy – Aware & Time – Optimal Planning: -

- Problem originally posed as a MDP and solved using dynamic programming;
- 5-D state – space:
    - x,y: x – y location on orbital map
    - ξ: rover status (sleeping or driving)
    - b: battery level
    - t: time of day
- State – space size: ~ 6.5 GB per Km.

The team's major objective for the MAARS project was to improve "safety, productivity and cost – efficiency of the future Mars rovers by fully exploiting the computation power of HPSC and modern SoCs such as snapdragon", where SoCs – systems on a chip, HPSC – High Performance Spaceflight Computing. These developed algorithms are aimed at improving responses based on the queries given by scientists that are needed for their research to make those responses closer to what scientists wish to get from the rover databases and provide them with more diverse images based on a set query.

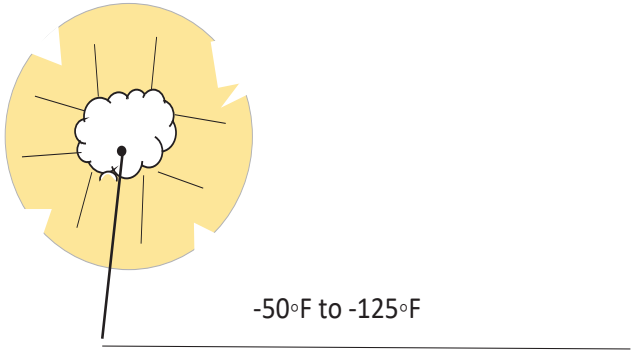
Artificial Intelligence is revolutionizing the space industry. NASA's frontier development lab is working with companies like Google, IBM and Microsoft to develop industry changing AI systems, including machine learning neural networks. Some say we've got the tech to right the planet within decades, but what if we can't cool our climate, or feed a population that's projected to be 10 billion by the year 2050? These topics makes me anxious. Thankfully, there's folks out there using A.I. to tackle some of our most pressing problems, like innovating agriculture and redefining how we think about food. If things really do go south, building a new home, on another planet. How can A.I. help humanity

adapt to a new way of life? Mars is the next great frontier. NASA has been sending probes since the 1970s, and, more recently, they even sent a space SUV to explore the red planet. By 2033 they plan to send humans to Mars. To go to Maars it is about six months to get there, and then you have to wait about a year and a half on the surface, for the planets to realign for a very short trip back. The Apollo 11 astronauts were in a tiny capsule. Stand by for T-1. It had the volume on the lunar module the equivalent of a c – block cell at Alcatraz. If it was only five foot high, but you can't expect someone but you can't expect someone to live in a habitat like that over any period of time.The rub is it'll have to be built by A.I. before they arrive.



A.I. allows you to study millions of options, comparing iterations against each other and find the optimal one. This process is sometimes known as "generative design", a fancy way of saying machines learn to do what architects do. Here A.I. algorithms compare and predict how different designs and forms function in a virtual Martian environment. The function could be structured strength, it could be thermal insulation. Life on Maars is not as simple as Bowie made it sound. The air is a toxic cocktail of mostly carbon dioxide.

There's basically no gravity, no water. Dust storm can last for months, temperature ranges from – 50 to -200 degrees Fahrenheit.



There is no Home Depot on Mars, so A.I – powered robots will also need to find, create and process all the raw materials themselves. So the idea of harvesting a building, the material that we selected to build on Mars, it's renewable, fully recyclable, and it's biodegradable, and as it turns out, that material is super strong. The material is a mixture of basalt a common rock on Mars, and plastic polymer made from corn. The problem is you can't find corn on Mars. It's got to be grown by robots. It's going to take a while before we can grow enough corn to print building on Mars, but we do envision a Mars agriculture. It is a climate problem but we also figure out the automation part.

It is extremely expensive to launch anything into space, and so rather than bringing up all the food and so on, and so we need to have some kind of A>I. being able to make those immediate decisions. This is look like science fiction but it's also right on that tipping point of innovation where it's becoming reality. In earth robotics is already starting to transform farming. Scientist want to utilize machine learning in things, so the system adapts to different circumstances.

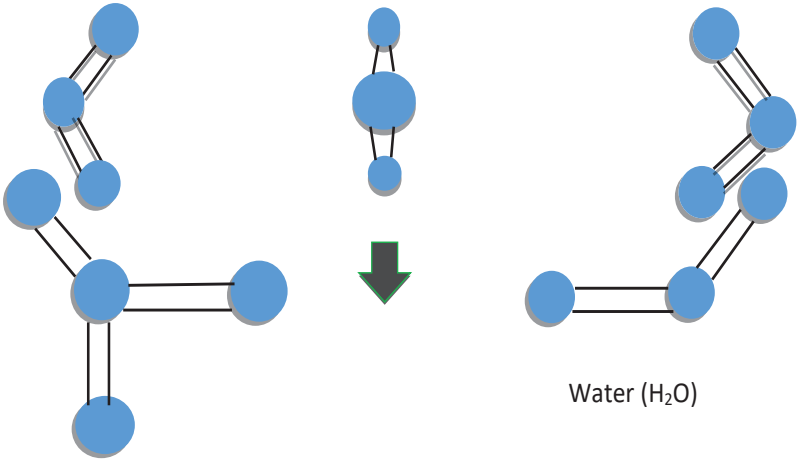
Methodology :

Research outcomes and review: -

The idea of a Martian civilization destroyed in this way seems incredible, and scientists have looked for other explanations for the presence of Xenon 129 on Mars. After all, it is possible for nuclear activity of sorts to take place in nature. Under very unique conditions, water flowing through the uranium deposit can cause fission, the same process used inside an atom bomb. But this thing did what it did at 1.7 billion years ago. Not only were there no humans around then, there wasn't even multicellular life on Earth. Nature has illustrated that it can create its own nuclear reacts. The question is could this same event have occurred naturally on Mars? Former NASA physicist Dr. John Brandenburg says the material found on Mars cannot have been produced by any natural nuclear process. A natural nuclear reactor, if it had gone unstable on Mars, not only would produce the wrong Xenon spectrum, but it would have created two massive creators. The ground is absolutely smooth. Brandenburg believes the evidence point in one direction. 300 million years ago intelligent life on Mars was of the worlds. We've now discovered that humanity is not the most evil species in an aberration on nature. We're a part of the fabric of the universe, and not everything in the universe is friendly. It is happened that Mars was attacked by aliens, it happened when there was virtually no intelligent life on Earth, so they wouldn't have noticed us. But the question remains, now that we're here, are they coming back?

The International Space Station does not really recycle oxygen. Oxygen is created on the International Space Station through the electrolysis of water. This produces hydrogen and oxygen. The hydrogen is then reacted with carbon dioxide to form water and methane. The methane is then simply exhausted into space while the water is fed back into the system.

$$3H_2 + CO_2 \longrightarrow H_2O + CH_4 + O$$



Water (H_2O)

Methane (CH_4)

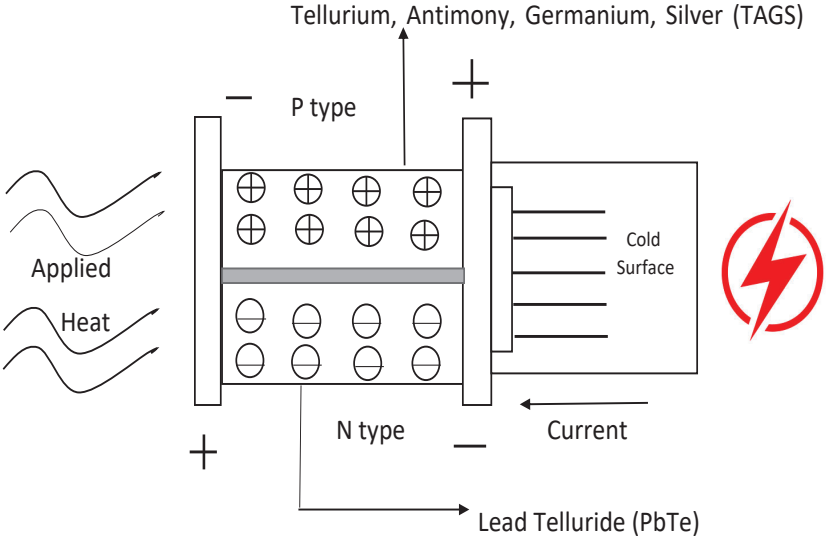
The International Space Station requires regular resupply of water as we are losing 2 hydrogen atoms for every oxygen molecule we create.

The MAARS task seeks to bring together JPL's developing HPSC capabilities, innovative on-board autonomy, and novel mission concepts. In particular, two novel capabilities for future Mars rovers are being developed. Drive-By Science (DBS) and Energy- Optimal Auto Nav (EOA). The Machine Learning- based analytics for Autonomous Rover System (MAARS) program encompasses a range of areas where artificial intelligence could be useful.

See back Effect:

The thermoelectric effect is the direct conversion of temperature differences to electric voltage and vice versa via thermocouple. A thermoelectric device creates a voltage when there is a different temperature on each side.

See back Effect in Action:



Pic- I

Findings :

MAARS : Task Overview

- FY 18-20 strategic R & TD (6x/4x)
- Task Goals
- Develop i) drive-by-science and
  ii) Risk/resource-aware path planning capabilities
  iii) Deploy/benchmark on HPSC emulator/analogue processor
  iv) Field test/demo with Athena Rover.

Particular emphasis on on-board deployment of deep learning. According to NASA only 40% of missions sent to Mars have been successful.

AI in Data Collection:

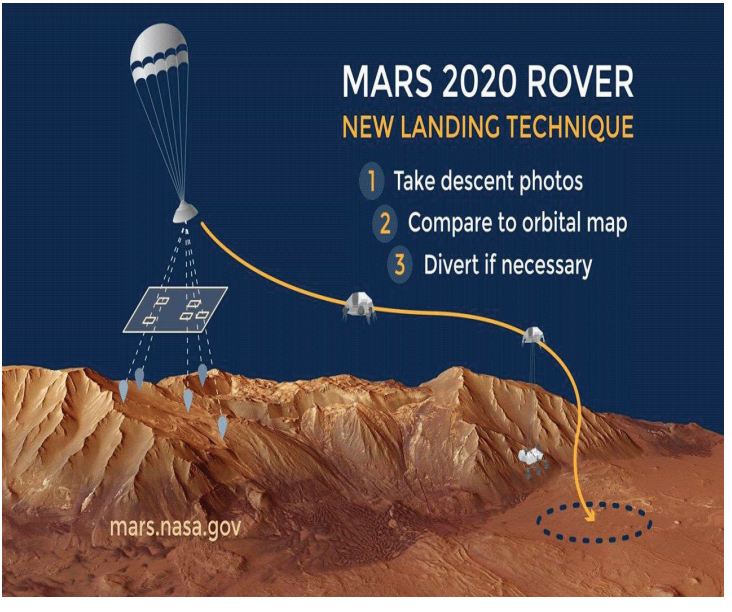
- NASA's perseverance Mars rover is getting critical help from the multiple on-board AI systems that are designed to guide its two-year exploratory mission on the red planet.
- The perseverance Rover relies on AI for Multiple Processes such as,
  - AI for Landing
  - AI for Targeting Instruments
  - AI for improved Autonomous Navigation.

  Never thought about optimizing paths by accounting for recharging solar panels up on a hill/going around obstacles. Sounds like a couple of exciting computational problems to tackle here.

MARS 2020 ROVER: -

Terrain Relative Navigation

1. Take decent photos
2. Compare to orbital map
3. Divert if necessary



Pic- II

AI in the Landing Process: -

The perseverance rover RTG uses 4.8 kilograms of plutonium dioxide as it's heat as this form of radiation is most efficiently converted to heat in a compact space.

Maars final demo, FY21 Demonstrated Capabilities: -

- Autonomous driving over ~500m
- Terrain-aware navigation
- On-board resource-aware strategic planning
- Drive-by science
- Real-time execution on HPSC-analogue processors

Above Capabilities are enabled by :

Terrain Classifier

SP OC

Resource-aware planning

RA ND

Image Captioning

SCOTI

UHURA

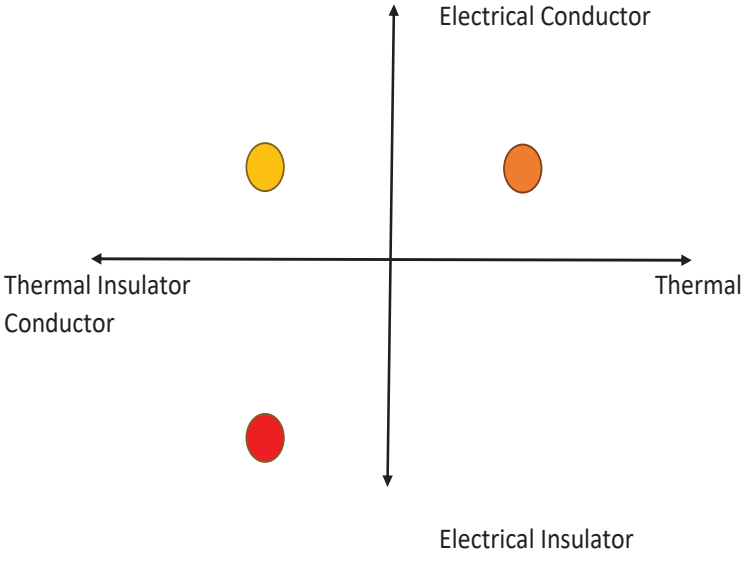
Image Understanding

SULU

Traversability Evaluation

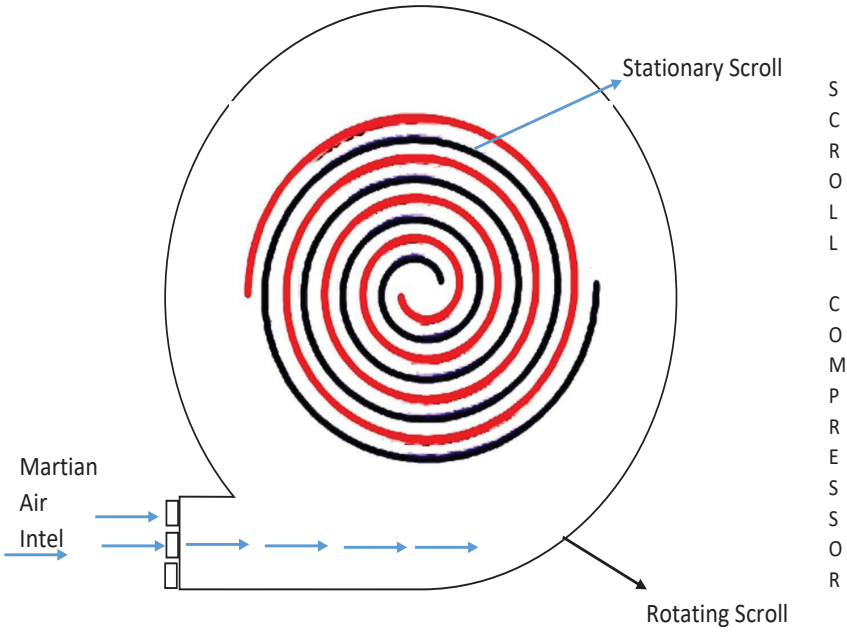
VEEGER

The only reason why the rover released by the crane safety landed exactly where it was supposed to, among dangerous rocks, near menacing terrain features, but in a place that scientists believe in rife with potential sources of mind-bending evidence of ancient alien life.



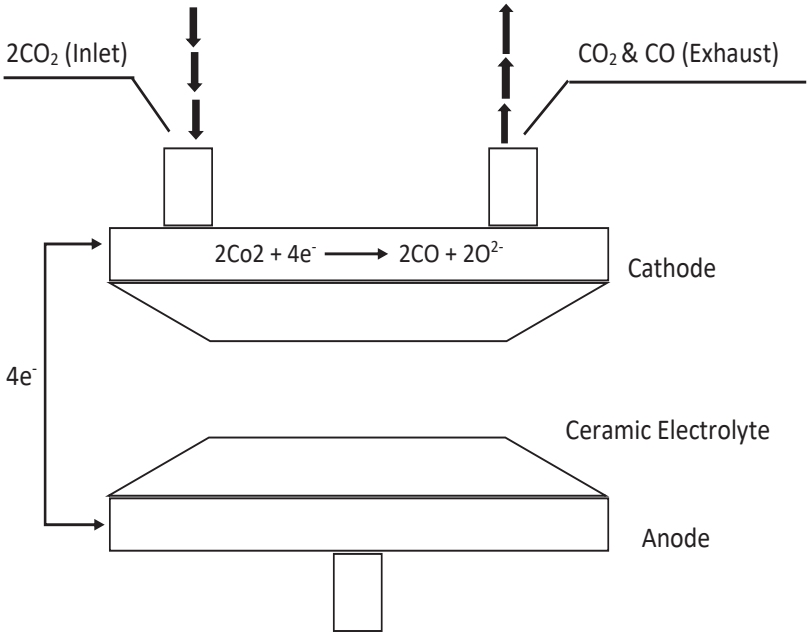
Pic-III

These two semiconductors need to be both thermally insulating, to ensure this heat gradient properties are typically linked. Copper is both a great electric and heat conductor, while iron is a poor electric and heat conductor. Having a single material that is a great electric conductor is extremely rare. For this reason two unique materials are used for the (pic – I) p and n type semiconductors. Lead Telluride for the n-type and an alloy commonly called Tags for the p-type, which is formed from tellurium, silver, germanium and antimony.



Pic- IV

It consisting two spiral scrolls one stationary and one rotating. Air is taken against the primary stationary scrolls. This continues to happen as the volume between down the spiral, causing an increase in pressure, in this case it takes the energy efficient and reliable. Making them the perfect air pump for the perseverance Rover. The pump feeds the carbon dioxide rich air through a cell stack. Each stack consists of a catalytic cathode, a solid electrolyte and an anode. As air passes over the cathode, which operates at 800

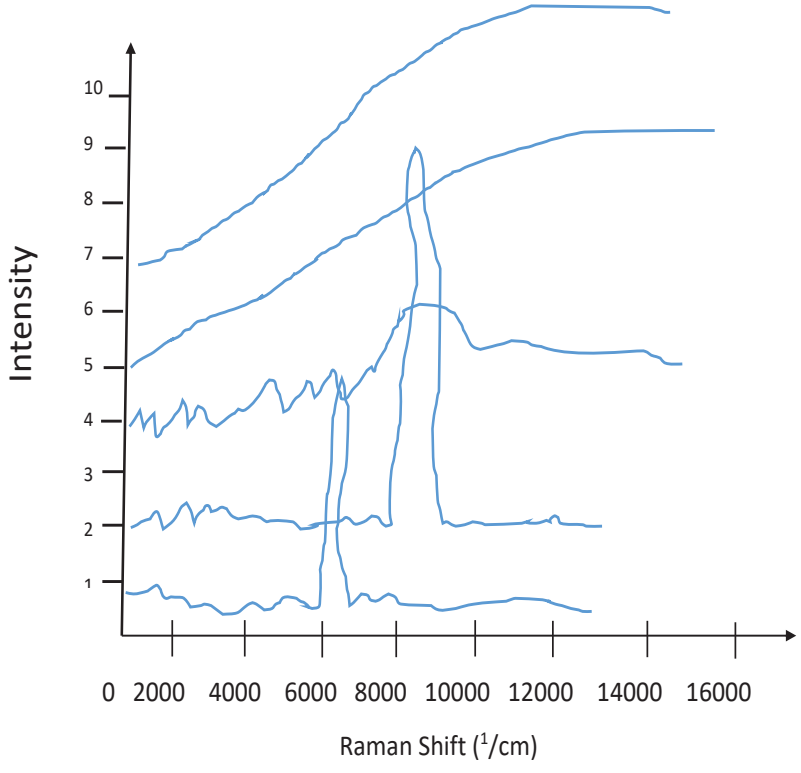


Pic- V

degree Celsius, the Carbon Dioxide is split into carbon monoxide and oxygen ions, according to this reaction. The oxygen ion passes through the solid electrolyte to the anode where it is oxidized, combining with a second oxygen atom, to form gaseous O_2, which is then passed out of the anode cavity and tested for purity.

There is a whole host of new sensors on board that do not collect soil. Each using different forms of electromagnetic radiation to investigate the ground below them. The SHERLOC instrument on the robotic head will look for signs of bio signatures using Raman and Luminescence spectroscopy which both detect molecules based on how they interact with UV light. It will sit about 5 centimetres off the ground where it will focus its UV laser onto the soil and be able to detect chemicals that would indicate the presence of past life, onto the soil and be able to detect

chemicals that would indicate the presence of past life. The Rover also has on X-ray imager can PIXL that will be able to visualise the texture

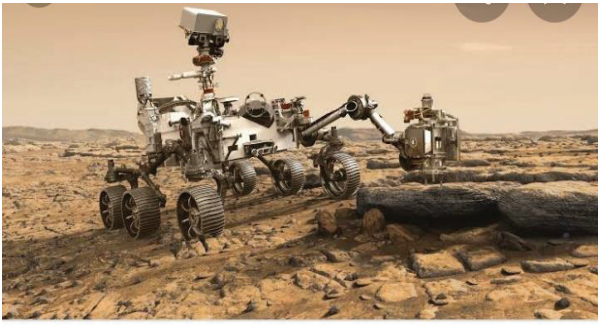


Sample Measurements

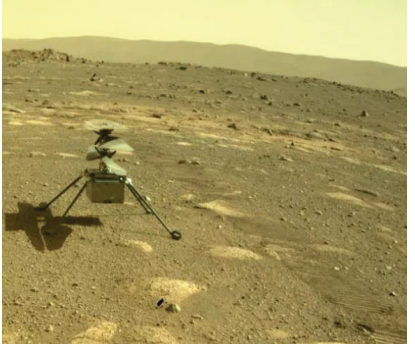
Pic- VI

of the ground below it looking for tiny variations in geology that would indicate that microbial life has altered the environment, while also being able to detect chemical compositions by observing the fluorescence of the target under X-ray electromagnetic radiation. Powered flight on Mars presents many challenges. The atmosphere is about 1% the density of Earth's, meaning there is less air to push down to achieve life. To combat this the propeller blades, which are counter rotating to eliminate the need for a tail rotor, spin much faster than a

traditional helicopter blade at about 2400 RPM. That's about 5 times faster than an equal sized RC helicopter here on earth. To deal with the centrifugal forces that come with that the blades need to be made of high strength carbon composites. These blades also have a much larger angle of attack than your run of the mill blade, allowing then to push a larger volume of air downwards creating an RTG capable of fitting into this tiny 2 kilogram helicopter is unfeasible. Instead it features these solar panels, which will charge 6 lithium ion batteries on board and these in turn will power the motors and cameras aboard. For a max flight time of about 90 seconds.



Pic-VII

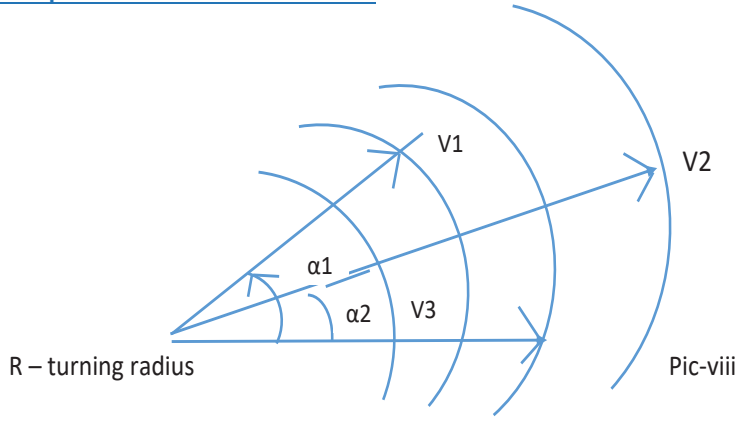


Pic- VIII

All of these enhanced AI capabilities and new ones to come will make it easier for future crewed and robotic missions to Mars and deep space as well. Space missions to outer planets or harsh environments are going to

depend on AI-based autonomy more and more. Part of the challenge is making people comfortable with it, making people believe that we can trust the autonomous system to make good decisions about the spacecraft or to select the right science data. Mars missions could feature algorithms created through machine learning. For now, engineers rely on their knowledge and experience to come up with algorithms. The algorithm doesn't have to be perfect to provide value.

An Implemented a custom six wheel: -



Pic- IX

Discussion :

Ackermann Steering Geometry : Gradient Convolution Heuristic: -

Given a terrain height map around a rover, the gradient convolution heuristic is calculated as follows:

1. Convolve the height map with normalized 3X3 sobel operators to find the x and y gradient

$$G_x = \frac{1}{2r} \cdot \frac{1}{4} \begin{bmatrix} +1 & 0 & -1 \\ +2 & 0 & -2 \\ +1 & 0 & -1 \end{bmatrix} * A$$

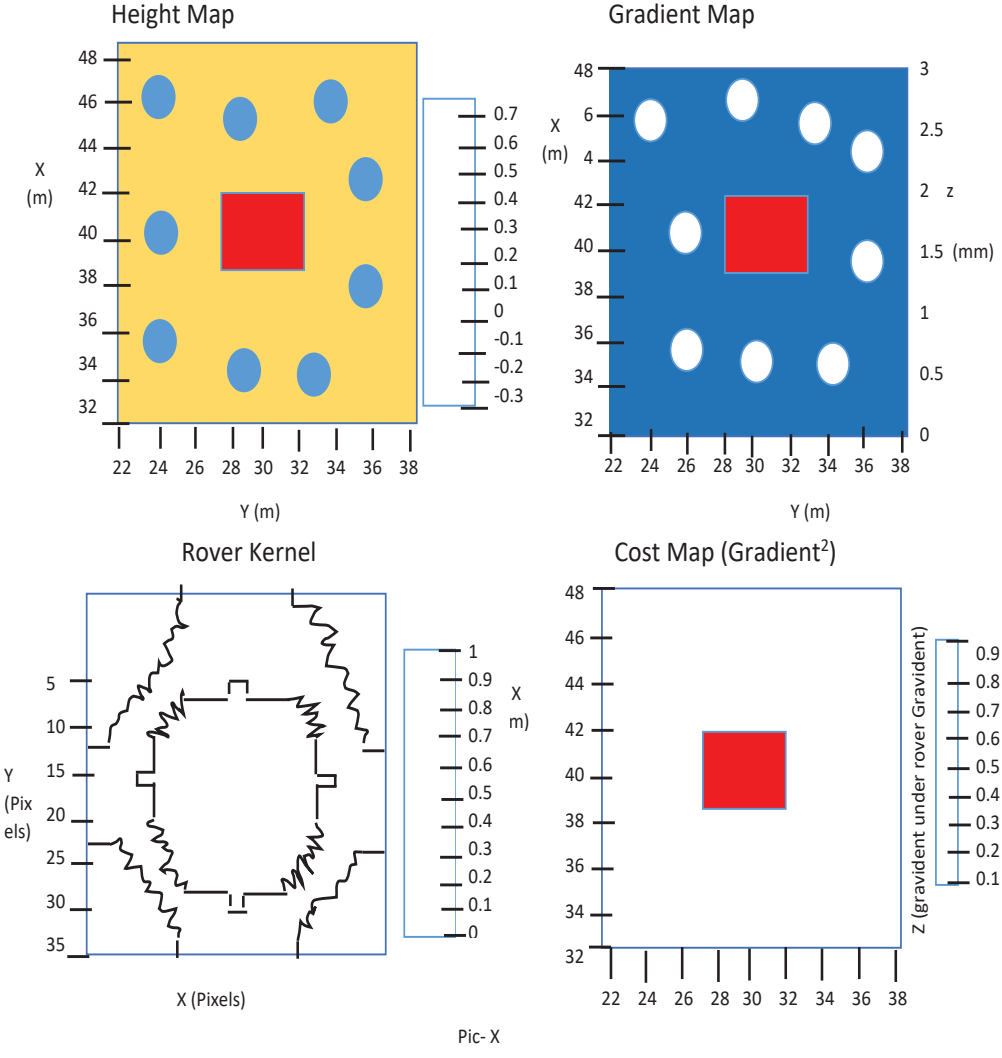
$$G_y = \frac{1}{2r} \cdot \frac{1}{4} \begin{bmatrix} +1 & +2 & +1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} * A$$

2. Find the squared gradient as the element – wise multiplication of the X and Y gradient:

$$G_{sq} = G_X \circ G_X + G_Y \circ G_Y$$

3. Convolve the gradient map with an annulus – shaped kernel representing the footprint of the rover:

$$G_e = \frac{K}{\sum Ri} R * G_{sq}$$

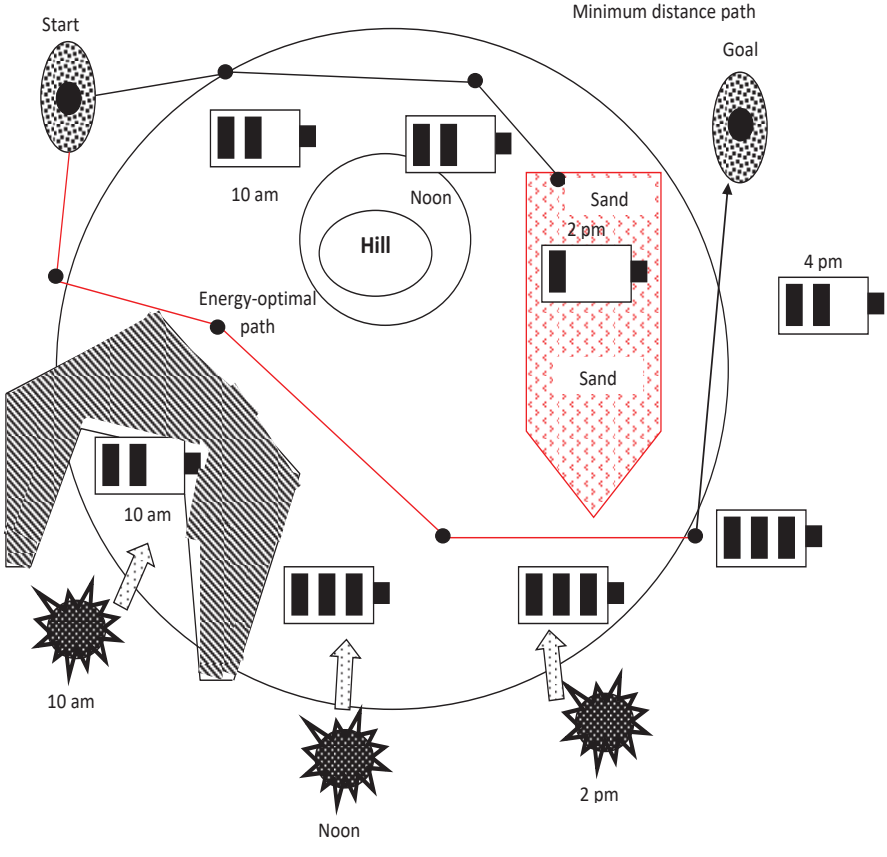


Machine Learned Heuristic: -

Architecture: -

- ☒ Data – driven framework to automatically learn the heuristic.
- ☒ Uses an encoder – decoder style convolution at Neural Network based on U – Net to predict the outcomes of the of ACE algorithm for a given terrain map.
- ☒ Using this prediction, Enav can reduce its search space by more optimally sorting its initial list of potential paths.
- ☒ ACE check is still done on the final selected path before execution, ensuring classical safety guarantees.

Vision – based Estimation of Expending generating energy for Rovers: -



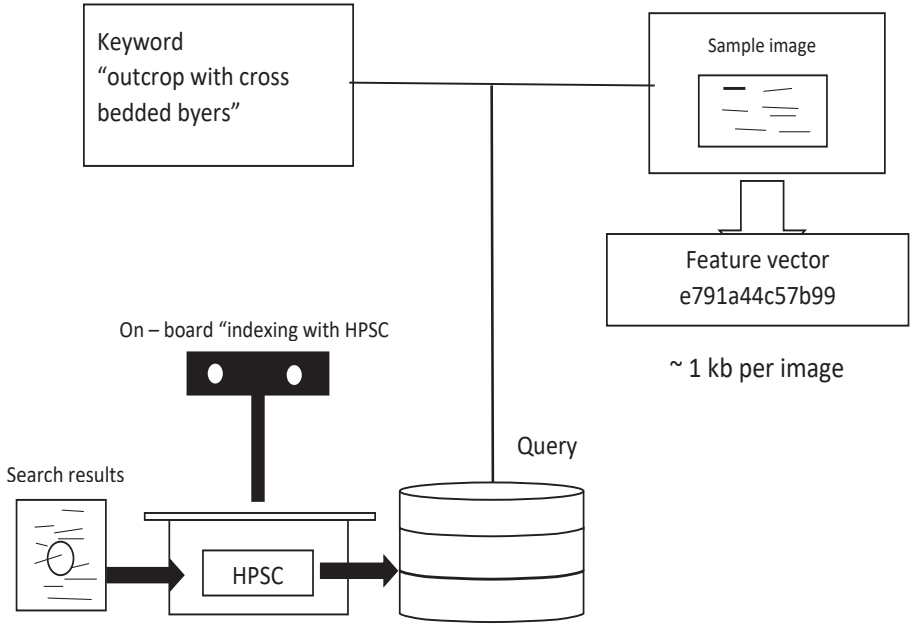
Pic - XI

Analytic capabilities are as follows:

Scientists/Rover planners

~500 Mbit/sol

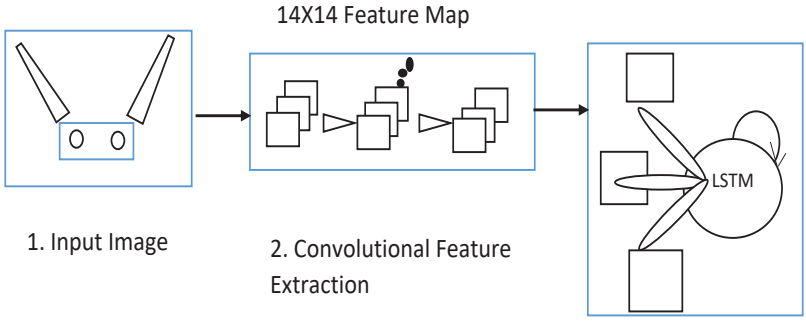
= 60 MB/sol



Pic - XII

<u>Science captioning of Terrain Images</u> (For on – board "Indexing)

CNN + LSTM architecture derived from "Show, attend and Tell" model



Pic - XIII

$$\text{Average specific impulse } I_{sp} = \frac{\text{Thrust Force}}{\text{Fuel Flow Rate}}$$

Conclusion :

NASA has built many advanced exploratory vehicles and machines in the past. They are not really what really a trained robotics would yet call intelligent. There's a growing need for future spacecraft to be autonomous, self-aware and have the ability to make critical decisions on their own, despite the challenges of distance. What a great experience. "Imagine having a team of 100+ engineers and scientists sitting on the earth, controlling each of those assets and the craziest things is that a Artificial Intelligence is going to be a key ingredient in making it happen. A lot of work right now is under technology development and our hope is to infuse them into future Mars rovers in next three to five years. It has a huge potential to revolutionize space exploration in future, but there are a lot of key challenges that still remain.

The new Rover has 23 cameras, which capture a ton of visual data from Mars, but the robot has to rely on human operators to interpret

most of those images. The rover has enhanced AI to help it avoid obstacles and it will get even better if you chip in. The varied measurements of carbon atoms could suggest three very different things about ancient Mars. The origin of the Carbon is likely due to cosmic dust, ultraviolet degradation of carbon dioxide, or the ultra violet degradation of biologically produced methane. All these scenarios are unconventional, unlike processes common on Earth, according to the researchers. This research accomplished, a long-standing goal for Mars exploration.

Reference :

1. https: //accessmans · with google.com
2. https:/www.enterpriseai.news
3. https://www.scienced aily.com>releases>2020/08
4. http://learningenglish.voanews.como>nasa-seeks–publi