Deep Analytics: Cancer Prevention Mechanism

Sumit Chakraborty
Fellow, Indian Institute of Management Calcutta; BEE(Jadavpur University)
E-mail: schakraborty2010@hotmail.com, surya20046@yahoo.co.in; Mobile: 91-9940433441
&
Suryashis Chakraborty
E-mail : suryashis7@gmil.com, Mobile : 91-9940087140

Abstract: This work presents the construction of a deep analytics based cancer prevention mechanism (DACPM) balancing proactive and reactive approaches. It defines human biological system from the perspectives of application, computing, networking, data and security schema of an information system. The strategic moves of DACPM include deep learning, intelligent reasoning, threat analytics, optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan and adaptive secure multi-party computation. The performance of human biological system is expected to be verified through the properties of adaptive secure multiparty computation : fairness, correctness, accountability, transparency, rationality, trust, commitment; authentication, authorization, correct identification, privacy, audit; safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency, robustness and stability of application integration. This work also shows the application of the mechanism on reasoning eight test cases: (a) cancer of mind, (b) digestion and absorption, (c) respiratory, (d) body fluids circulation, (e) excretory, (f) locomotion and movement, (g) neural control and coordination and (h) chemical coordination and integration. It analyzes the complexity of the mechanism in terms of computational cost of deep learning algorithm. The human biological system is assumed to be a computer. It is not a rational thinking that the most of the causes of cancer are due to bad luck; it is still not known enough about the causes and prevention measures of cancer. Deep analytics does not necessarily mean deep learning algorithm, it is also associated with intelligent reasoning – analytical, logical, common sense, case based reasoning and also perception. A human agent must have common sense healthcare knowledge base for proper biological system control through intelligent self-assessment, self-confidence, life-style, diet control and right decision making at right time. It demands the necessity of learning the basic concept of reasoning and common sense healthcare through an effective knowledge management system based on deep analytics.

Keywords: Deep Analytics, Cancer Prevention, Proactive Approach, Reactive Approach, Bad Luck, Complexity Analysis, Deep Learning, CNN, SVM, Intelligent reasoning.

1. Introduction

Recently, there is a trend of cross fertilization between five disciplines: medical science, management information system, artificial intelligence, artificial neural network and management science. This work is associated with the problem of cancer prevention. Cancer is a costly, global and complex problem; it results a major obstacle to human development and well-being [2]. The attack of cancer has increased from 12.7 million (2008) to 14.1 million (2012) and this trend is projected to continue about 25 million cases over next two decades; the greatest impact will be in low and middle income ill equipped countries [1]. The future of a cancer patient depends on his / her living zone. In less economically developed countries, cancer is diagnosed at more advanced stages while access to effective treatment is limited or unavailable. The highest-income countries often struggle with the spiraling costs of cancer treatment and care. Cancer has a social cost, human potential is lost and cancer care has an escalating economic impact. It is essential to identify the causes and prevention strategies for cancer control [3].

.

The basic objective of this work is to generate a rational cancer prevention plan subject to financial constraints. The work has reviewed the relevant literature on cancer, oncology and deep learning and has adopted analogical reasoning as research methodology. This work is organized as follows. Section 1 defines the problem of cancer prevention. Section 2 outlines the deep analytics based cancer prevention mechanism (DACPM). Section 3 shows the complexity analysis of DACPM in terms of computational cost and security intelligence. Section 4 analyzes eight test cases based on DACPM. Section 5 concludes the work.

2. *Deep Analytics based Cancer Prevention Mechanism [DACPM]*

***Agents**: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);*
***Model**: Human biological system – (a) body, (b) mind;*
***Objectives**: cancer prevention at optimal cost;*
***Constraints**: budget or financial constraint, resources, time, knowledge;*
***Input**: Perception of human agent, performance measures of biological system or test data;*
***Strategic moves**: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;*
***Revelation principle**: The agents preserve privacy of strategic data;*

- ***Defender** : The defenders share critical information collaboratively.*
- ***Attacker** : The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.*

Cancer Prevention Approaches:

- ***Proactive approach**:*
    - ***Identify targets** : computing, data, networking, security and application schema;*
    - ***Threat modeling***
        - *Call threat analytics function (f_a) and assess miscellaneous risk elements;*
        - *Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];*
        - *Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];*
        - *Map threats into a set of risk profiles or classes : LL, LH,HL and HH;*
        - *Estimate requirements of healthcare in terms of demand plan (P^p_d);*
        - *Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.*
            - *Auto-immunity and vaccination;*
            - *Optimal diet intake to fight against malnutrition;*
            - *Life-style : Avoid smoking and alcohols, food habit, drug addiction control, wild polygamy, obesity and overweight control through yoga and physical activities, stress control through meditation;*
- ***Reactive approach**:*
    - *adopt sense-and-respond strategy.*
    - *assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.*
        - *what is corrupted or compromised?*
        - *time series analysis : what occurred? what is occuring? what will occur?*
        - *insights : how and why did it occur? do cause-effect analysis.*
        - *recommend : what is the next best action?*
        - *predict: what is the best or worst that can happen?*

- *verify security intelligence of application, computing, networking, security and data schema of biological system.*
    - ***Level1:** correctness, fairness, accountability, transparency, rationality, trust, commitment;*
    - ***Level 2:** authentication, authorization, correct identification, privacy, audit;*
    - ***Level3:** safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;*
    - ***Level4:** stability, system dynamics, quality of application integration.*
- *Explore risk mitigation plan (P^r_d and P^r_m).*
    - *Do medical testing → Data visualization (Refer Deep Leaning Algorithm of section 2.1)*
    - *Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance;*
    - *Integrated medicine*
    - *Regenerative medicine*
    - *Chemotherapy*
    - *Laser*
- ***Fight against bad luck :** Identify critical risk elements.*
    - *Genetic disorder (sex, race, ethnicity, somatic mutation)*
    - *Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)*
    - *Injuries from accidents, war and crime*
    - *Occupational exposure*
    - *Environmental pollution*
    - *Hostile climate, weather and other locational disadvantages, exposure to sunshine*
    - *Malnutrition due to poverty*
- *Develop risk mitigation plan in terms of organ transplantation, surgical operation, gene therapy, stem cell therapy and migration of human civilization from risky zone.*

Payment function:

- *Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.*
- *Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.*
- *Trade-off proactive vs. reactive security; assign weights to each approach.*
- *Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;*

***Output:** Cancer prevention plan*

2.1 Deep Learning Algorithm

Objective: Computer aided cancer detection and diagnosis with improved accuracy;
Input : Medical images with optimal number of correct features;
System Architecture: Deep Convolutional Neural Network (CNN) / Deep Belief Network;
Training Algorithm: Support Vector Machine (SVM) / Transfer learning / Back propagation;
Output: Pattern recognition for

- *Cancer location identification*

- *Cancer tissue classification*
- *Cancer image segmentation*
- *Cancer image retrieval*
- *Big image data analysis*

3. Complexity Analysis of DAPCM

The computational cost of deep learning mechanism depends on the complexity of threat analytics function, deep learning algorithm and payment function. The cost of computation is a function of the complexity of threat analytics. The threat analytics analyze system performance, sensitivity, trends, exception and alerts along two dimensions: time and insights. Another major computational burden of the deep learning mechanism is the complexity of verification or model checking algorithms. The cost of computation also depends on the complexity of payment function.

3.1 Computational Complexity of Deep Learning

Deep learning represents a class of machine learning techniques that exploit many layers of non-linear information processing for supervised or unsupervised feature extraction and transformation, pattern recognition (e.g classification) [4]. It is used for learning multiple levels of representation to model complex relationships among data. Higher level features and concepts are defined in terms of lower level ones and such a hierarchy of features is known as deep architecture [5]. Deep learning is based on learning representations. An observation such as an image can be represented in many ways like a vector of pixels, but some representations make it easier to learn from examples. Deep learning is a set of algorithms in machine learning to learn in multiple levels and at different levels of abstraction. It typically uses artificial neural networks such as multi-layer feedforward neural network and convolutional neural network.

There are three classes of deep learning architectures and techniques: (a) Deep networks for unsupervised or generative learning, (b) Deep networks for supervised learning and (c) hybrid deep networks [6]. Unsupervised learning is used to capture high order correlation of the visible data when no information about target class labels is available. In case of supervised learning, target label data are always available in direct or indirect forms. Hybrid deep networks use both unsupervised and supervised learning techniques. Many machine learning techniques use shallow structured architectures consisting of at most one or two layers. Shallow architectures are effective in solving simple problems are not effective for complicated applications due to limited modeling and representational power. Human information processing mechanisms needs deep architectures for extracting complex structure and building internal representation from rich sensory inputs. The basic concept of deep learning comes from the domains of ANN, AI, graphical modeling, optimization, pattern recognition and signal processing. Deep learning has several advantages as compared to shallow architecture: increased chip processing abilities, significantly increased size of training data and recent advances in machine learning research have enabled the deep learning methods to exploit complex and nonlinear functions, to learn distributed and hierarchical feature representations and effective use of both labeled and unlabeled data.

Deep Learning is basically credit assignment in adaptive systems with long chains of causal links between actions and consequences. It is accurately assigning credit across many stages. A standard neural network consists of many simple connected processors or units each producing a sequence of real valued activations. Input units get activated through sensors perceiving the environment, other units through connections with weights from previously active units. Learning or credit assignment is to find weights that make the neural network exhibit desired behavior [7]. A complex problem may require long causal chains of computational stages. Convolutional Neural Networks (CNN) *architecture are widely used for computer vision. The receptive field of a unit with given weight vector is shifted step by step across input values. The resulting array of subsequent activation events of a unit can provide inputs to higher level units.*

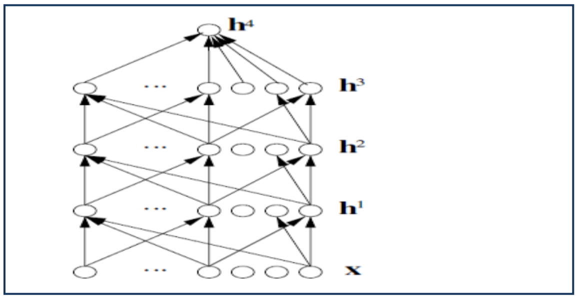

Figure 1: Deep architecture for supervised learning in prediction or classification
***x**: input nodes; h^1, h^2,h^3 : hidden layers, h^4 : output node*

3.2 Security intelligence

The deep learning mechanism is basically a security game i.e. fight against cancer. It is defined by various types of elements: a group of agents or players, model, actions, a finite set of inputs of each agent, a finite set of outcomes as defined by output function, a set of objective functions and constraints, payments, a strategy profile, a dominant strategy which maximizes the utility of an agent for all possible strategies of other agents involved in the mechanism, security intelligence and revelation principle [8]. There are two agents in the security game: a defender (D) and the attacker (A). Each agent adopts and executes a or a set of strategies. A pure strategy is a deterministic policy for a single move game. For many games, an agent can do better with a mixed strategy. The best strategy may depend on the knowledge of the defender about prospective attacks and the sunk costs incurred when upgrading information security schema reactively. The payment function of the mechanism estimates an optimal investment plan for the protection of human biological system.

The mechanism verifies the security intelligence of human biological system; it is a multi-dimensional parameter which is defined in terms of rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, reliability, consistency, commitment; safety, liveness, synchronization, reachability, deadlock freeness; authentication, authorization, correct identification, non-repudiation, integrity, audit and privacy [9,12,13]. The search procedure addresses the issues of authentication, authorization, correct identification, privacy and audit. The system should ask the identity and authentication of one or more agents involved in the mechanism. The agents of the same trust zone may skip authentication but it is essential for all sensitive communication across different trust boundaries. After the identification and authentication, the procedure should address the issue of authorization. The system should be configured in such a way that an unauthorized agent cannot perform any information searching task out of scope. The system should ask the credentials of the requester; validate the credentials and authorize the agents to perform a specific task as per agreed protocol. Each agent should be assigned an explicit set of access rights according to role. Privacy is another important issue; a searching agent can view only the information according to authorized access rights. The system preserves privacy if no agent learns anything more than its output; the only information that should be disclosed about other agent's inputs is what can be derived from the output itself. The agents must commit the confidentiality of data exchange associated with private communication. Privacy is the primary concern of the revelation principle; the issue can be addressed in terms of confidentiality, data integrity, authentication and non-repudiation.

The security intelligence is evaluated in terms of fairness, correctness, transparency, accountability, confidentiality and trust. The system is expected to ensure correctness in correct computation free *from any false data injection attack; each recipient must receive the same correct data in time without any change and modification done by any malicious agent. Fairness is associated with the commitment, honesty and rational reasoning and trust. Fairness ensures that something will or will not occur infinitely often under certain conditions; it is important from the perspective of fair resource allocation. The system must ensure the accountability and responsibility of the agents in access control and data mining. In fact, accountability is associated with collective intelligence. The transparency of the system is associated with communication protocols, revelation principle and automated system verification procedures. For example, the defender should be able to define goal state transparently.*

The performance and quality of service of the human biological system is expected to be consistent and reliable; it should be validated through audit of miscellaneous transactions. Reachability ensures that some particular state or situation can be reached. Safety indicates that under certain conditions, an event never occurs. Liveness ensures that under certain conditions an event will ultimately occur. Deadlock freeness indicates that a system can never be in a state in which no progress is possible; this indicates the correctness of a real-time dynamic system. The system is expected to be a resilient system. The resiliency measures the ability to and the speed at which the information system can return to normal performance level following a disruption. Adaptability is about responding to change effectively and decisively through reactive approach: the ability to identify the change in search space for the adversaries, understanding the probable impacts of the hit by the adversaries, rapid quantification what is under its control to compensate, identification what modifications to the environment are necessary and adoption of risk mitigation measures in time without any hesitation.

The DAPCM mechanism evaluates security intelligence of the human biological system based on proactive and reactive approaches. The vulnerability of the system to a disruptive event should be viewed as a combination of likelihood of a disruption and its potential severity. The defender must do two critical tasks: assess risks and mitigate the assessed risks. To assess risks, the defender should explore: what can go wrong in the operation of the system? what is the probability of the disruption? how severe it will be? what are the consequences if the disruption occurs? A vulnerability map can be modeled through a set of expected risk metrics, probability of disruptive event and the magnitude of consequences. For example, the map has four quadrants in a two dimensional space; the vertical axis represents the probability of disruptive event and the horizontal axis represents the magnitude of the consequences. The mechanism faces a set of challenges to solve the problem of resiliency: what are the critical issues to be focused on? what can be done to reduce the probability of a disruption? what can be done to reduce the impact of a disruption? How to improve the resiliency of the system? The critical steps of risk assessment are to identify a set of feasible risk metrics; assess the probability of each risk metric; assess severity of each risk metric and plot each risk metric in the vulnerability map. The critical steps of risk mitigation are to prioritize risks; do causal analysis for each risk metric; develop specific strategies for each cell of vulnerability map and be adaptive and do real-time system monitoring.

The defender tries to define the payment function associated with healthcare in terms of aspiration point, reservation point and adjustment of various preferential thresholds (e.g. indifference, strong preference, weak preference, veto) and preferred solutions. The value of the objective function which is desirable or satisfactory to the decision maker or defender is defined as aspiration point. The value of the objective function that the defender wants to avoid is reservation point. The defender can use various preference thresholds in order to compare alternatives and to define outranking relations. There is an interval of preference wherein it is not possible for the defender to distinguish between different alternatives and this is defined as indifference threshold. Strict preference threshold is defined as minimal increase or decrease of any objective that makes the new alternative strictly preferred with respect to this objective. There exists an intermediate region between indifference and strict preference threshold where the defender may hesitate to compare alternatives. It is defined as weak preference threshold. Veto threshold indicates what is the minimal increase or decrease of any objective that makes the new alternative unacceptable regardless of the value of other objectives.

The payment function selects appropriate heuristics of fund allocation such as selective based on ranks, linear and proportional allocation. When the budget of the defender is more than the total projected demand, the agent may be able to fight against cancer systematically. However, when the budget is less than total demand, the agent should find the investment plan based on various types of allocation heuristics, objectives and constraints [9]. *Linear allocation* is an equal sharing of the pain or shortage of capacity among various components of IS security schema. The threat T_i is allocated fund $q_i = d_i$ – (1/n) max (0, $\sum_{i=1}^{n} d^*_i$ - C) where n is the number of threats and C is the budget capacity of the defender. In case of *proportional allocation*, the threat T_i is allocated fund q_i = min {d^*_i, C.d^*_i/($\sum_{i=1}^{n} d^*_i$)}. Reactive approach may consider reinforcement learning strategy and allocates more budget to easier-to-defend edges of the attack graph. When new edges are revealed, the budget is reallocated uniformly from the already revealed edges to the newly revealed edges. Myopic bug chasing is most likely an ineffective reactive approach. But, the strategy of gradually reinforcing attacked edges by shifting budget from unattacked edges of the attack graph may be cost effective [10,11]. Another fund allocation strategy is *selective allocation* based on the computation of the rank of the threats which is computed based on probability of occurrence (*p*) and impact or sunk cost (c).

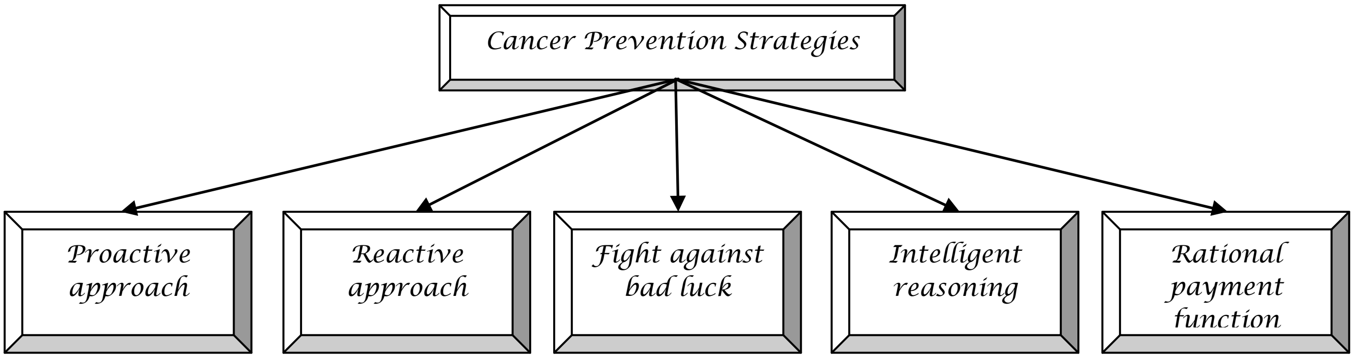

Figure 2: Strategic moves of DACPM mechanism

Caution from malicious learning system

The basic objective is to protect learning systems in adversarial setting from various types of threats such as use of flawed learning algorithm or intentional change of training and testing data distribution [14,15]]. The malicious agents may act consciously to limit or prevent accurate performance of the learning system for economic incentives. It is a common problem where machine learning is used to prevent illegal or unsanctioned activities. Traditional techniques (e.g. efficient algorithm, linear classification) are necessary but not sufficient to ensure the security of the machine learning system. It is a hard problem and needs the support of an efficient mechanism equipped with intelligent threat analytics and adaptive secure multi-party computation algorithms. Malicious business intelligence is a critical threat to machine learning system. The conflict between security intelligence and business intelligence is inevitable. It needs fair, rational and intelligent business model innovation [16].

Example : Malicious business intelligence may attack a life-science supply chain and healthcare service chain through greedy heuristics in payment function for revenue and profit optimization, economic pressure and incentive policy, fraudulent health insurance model, flaws in investment decision on technology management, irrational and dull HR policy in talent management and *chaotics in formulation of public policy, mechanisms and corporate governance. In fact, the conflict between business intelligence and security intelligence is inevitable. The deep learning mechanism is applicable to resolve this conflict between security and business intelligence through audit of '10S' elements associated with a machine learning system : System, Security, Strategy, Structure, Staff, Skill, Style - governance and regulatory compliance, Shared vision, Service and Social networking.*

Let us consider a specific instance of machine learning in healthcare service chain. The deep learning mechanism must call the threat analytics to audit various critical processes associated with a healthcare service chain such as registration, consulting, testing, surgical operations, billing, payment processing and follow-up. Generally, different types of information systems are commonly used to support these processes: transaction processing system (TPS), decision support system (DSS), group decision support system (GDSS), knowledge management system (KMS) and business intelligence (BI) system. The primary objective of these information systems is to ensure fairness and correctness in computation of registration card, appointment slip for consulting, prescription by consultant, surgery schedule, quality control certificate, medical test report, discharge certificate, bills and payment receipt, feedback form and patient's guide. The other important issue is to preserve the privacy of patient's personal and medical data. The deep learning mechanism should verify the security of the computing schema associated with the machine learning system in healthcare service chain to identify probable sources of errors.

- *Incorrect data provided by the service consumers or patients to the registration associate during registration intentionally or due to lack of knowledge or incorrect perception of the patients or their attendants; the patients or their attendants may be irrational in information sharing properly with the service providers.*
- *No verification of patient's identity correctly during registration; the cases of emergency situation or accidents may skip verification due to unavailability of data about the patients.*
- *Wrong entry of data into various information systems by the healthcare associates due to time and resource constraints or misunderstanding or lack of validation of input data.*
- *Computational errors due to wrong configuration of enterprise applications and / or errors in the heuristics, deep learning algorithms and quantitative models and / or no updating of data (e.g. service charge, tariff of testing, price of drugs and healthcare products; low accuracy of pattern recognition algorithms in image processing system may result incorrect medical diagnosis.*
- *Access control problem causing dangerous errors in information system; a malicious agent may enter false data into HIS during the absence of authorized users.*
- *A malicious agent may launch attacks on TPS, DSS, GDSS, KMS and BIS through malicious data mining, insecure data storage, flaws in data visualization and image processing algorithms and transaction processing logic.*
- *Swap or mixing of test data of various patients or drugs administration due to confusion, poor document management, lack of clear understanding or training of the healthcare workforce; false data injection on viruses in test reports are serious threats in today's healthcare practice. The patients are not often given test reports today by the service provider to hide malicious trading practice or to charge extra amount. Testing of uncommon viruses enhance the cost of testing unnecessarily. Sometimes, broadcast of epidemic results panic among the public and this critical and helpless situation is exploited by malicious testing and medicare practice inhumanly.*
- *Errors in decision making by the health consultants due to lack of proper knowledge management system (e.g. case based reasoning, intelligent DSS and GDSS) or misperception or lack of coordination among the workforce of various departments or inappropriate enterprise application integration or error in test reports; incomplete prescription due to memory failure or silly mistakes.*

- *Errors in scheduling due to exceptions (e.g. unfit patients, non-availability of healthcare experts), flawed and inadequate doctor-patient ratio;.*
- *surgical operation by unauthorized and unskilled workforce, intentional errors due to malicious business practice, lack of ethics, casual approach and dull HR policy; unintentional errors due to physical and mental fatigue for excessive workload and sickness, non-availability of basic infrastructure and logistics arrangements;*
- *Lack of verification of correctness of computation in medical billing and payment processing by the service provider and / or service consumer;*
- *Incorrect data in patient's help guide may cause confusions and mismatch between the computed results and perceived one;*
- *Incorrect feedback by the patients or their attendants due to misperception, misunderstanding of feedback form, lack of knowledge and critical observations or casual attitude.*
- *Sybil attack: It is really complex to trace the corrupted players A malicious agent may control multiple pseudonymous identities and can manipulate, disrupt or corrupt a distributed computing application that relies on redundancy by injecting false data or suppressing critical data; it is sybil attack. The patients may be treated incorrectly and diagnosed as cancer casually though there is another simple medical problem. Natural intuition and perception are not applied for simple medical problems. The patients are incorrectly recommended for costly treatment. They are often recommended for costly treatment procedure repeatedly (e.g. CT scan, X-ray), drugs and surgical operations. The poor and helpless patients are forced to validate and verify the test reports and medical diagnosis at various healthcare institutes. This is an instance of modern biological, chemical and radiological terrorism. Fairness and correctness of computation and testing is a critical concern in healthcare practice. Knowledge management is another critical success factor; case based reasoning may be a good solution for correct clinical decision making.*

For effective deep learning system, digital technology management is not only the critical success factor (CSF). There are other several CSFs such as HR policy in talent management, motivation and commitment, quality of education in terms of trust, ethics and values, intelligent public policy, mechanisms and corporate governance.

4. Test Cases

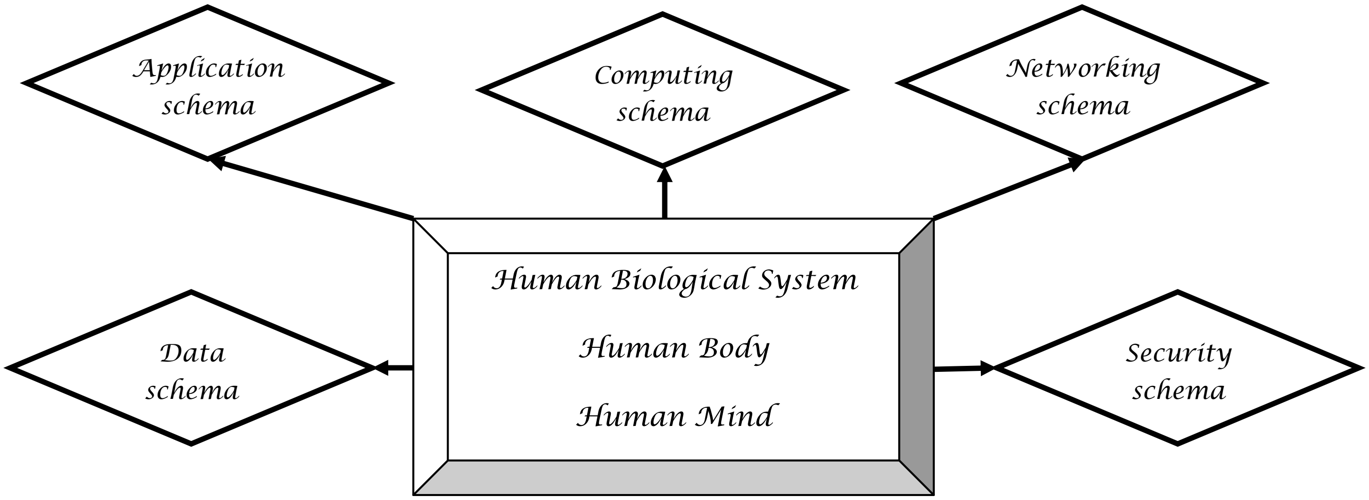

Figure 3: Miscellaneous schema of human biological system

Let us first look at bio-statistics of cancer [1]. It is a major cause of morbidity and mortality, with about 14 million new cases and 8 million deaths in 2012, affecting populations in all countries and all regions. Among men, five most common sites of cancer were lung (16.7%), prostate (15.0%), colorectum (10.0%), stomach (8.5%), and liver (7.5%). Among women, five most common sites of cancer were breast (25.2%), colorectum (9.2%), lung (8.7%), cervix (7.9%), and stomach (4.8%). There were 8.7 million people (older than 15 years) alive with cancer diagnosed in the previous year, 22.0 million in the previous 3 years, and 32.6 million in previous 5 years. The worldwide estimate for the number of cancers diagnosed in childhood (ages 0-14 years) in 2012 is 165 000 (95 000 in boys and 70 000 in girls). The highest incidence rates are associated with high income countries of North America and western Europe, Japan, Korea, Australia, and New Zealand. More than 60% of cases and 70% of deaths occur in Africa, Asia, and Central and South America. Cancers are caused by mutations that may be inherited or caused by environmental factors or DNA replication errors (R) [2].

This work defines human biological system from the perspectives of application, computing, networking, data and security schema of an information system. The application schema is related to the function and features and a specific biological system. The networking schema is related to the configuration of the system such as nodes and interconnections among the nodes. The computing schema deals with the protocol, process, procedure and mechanisms of a system and its various components. The data schema is associated with various entities, their attributes and interrelationships, inputs and output of a system. The security schema verifies the disorders of a system.

4.1 Cancer of mind

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human mind;
Objectives: cancer prevention at optimal cost;
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: intelligent reasoning, optimal mix of proactive and reactive approaches, rational payment function and budget plan;
Revelation principle: The agents preserve privacy of strategic data;

- **Defender** : The defenders share critical information collaboratively.
- **Attacker :** The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.

Cancer Prevention Approaches:

- **Proactive approach:**
  - **Identify targets :**
    - application schema – human mind;
    - networking schema – brain and nervous system,
    - computing schema – nerve impulse and release of neurotransmitter;
    - data schema – symptoms of abnormal, selfish behavior, narrow outlook, jealousy, negative thinking, devil's thought, fear of death;
    - Security schema – change in behavior, physical appearance and personality;
  - **Threat modeling**
    - Call threat analytics function (f_a) and assess miscellaneous risk elements;
    - Estimate requirements of healthcare in terms of demand plan (P^p_d);
    - Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.
      - Auto-immunity and vaccination;
      - Optimal diet intake to fight against malnutrition;

        - *Life-style : Avoid smoking, alcohols and drug addiction;*
        - *Stress control through yoga and meditation, deep sleep;*
        - *Listen soft relaxation music during idle time in subconscious mind.*

- ***Reactive approach**:*
    - *adopt sense-and-respond strategy.*
    - *assess risks of single or multiple attacks on the mind; analyze performance, sensitivity, trends, exception and alerts.*
        - *what is corrupted or compromised?*
        - *time series analysis : what occurred? what is occuring? what will occur?*
        - *insights : how and why did it occur? do cause-effect analysis.*
        - *recommend : what is the next best action?*
        - *predict: what is the best or worst that can happen?*
    - *verify security intelligence of application, computing, networking, security and data schema of human mind.*
        - ***Level1**: correctness, fairness, accountability, transparency, rationality, trust, commitment;*
        - ***Level 2**: authentication, authorization, correct identification, privacy, audit;*
        - ***Level3:** safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;*
        - ***Level4:** stability, system dynamics, quality of application integration.*
    - *Explore risk mitigation plan (P^r_d and P^r_m).*
        - *Do medical testing → Data visualization of brain scan;*
        - *Integrated medicine*
- ***Fight against bad luck :** Identify critical risk elements.*
    - *Genetic disorder*
    - *Reproductive disorder (personal, hormonal and family history)*
    - *Occupational exposure*
    - *Injuries from accidents, war and crime;*
    - *Hostile climate, weather and other locational disadvantages, exposure to sunshine*
    - *Develop risk mitigation plan in terms of deaddiction and rehabilitation.*

***Payment function**:*

- *Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.*
- *Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in the security requirements.*
- *Trade-off proactive vs. reactive security: assign weights to each approach.*
- *Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;*

***Output**: Prevention plan of cancer of mind*

*Let us analyze DACPM in the context of cancer of mind caused by drug addiction. There is slight difference between cancer of mind and madness. A human agent suffering from cancer of mind may act selfishly with narrow outlook and malicious business intelligence. But, a mad man generally acts irrationally. Any chemical substance other than food used for the prevention, diagnosis, alleviation, treatment or cure of a disease of human agents or animals is called a **drug** or medicine or therapeutic agent. Drug addiction is the habitual, physiological and psychological dependence on a substance or a practice which is beyond voluntary control of an addict. Addictive drug modifies the* *biological, psychological and social behavior of the addicted person by stimulating, depressing or distorting the function of their body and mind. Use is basically taking a drug for medical treatment like disorder or injury. Drug abuse is the wrong, improper, injurious and misuse of drugs for non-medical purposes which affects physical and mental health of the drug abuser. They use drugs without the prescription of the doctors secretly; taken frequently and regularly; habituating substances; may affect brain and nervous system and changes behavior; gives temporary pleasure or relief from stress. A doctor prescribes drugs for the treatment of diseases or for the improvement of physical and mental health and the drugs are withdrawn as soon as the desired effect is achieved. Repeated use of some drugs on a periodic or continuous basis may make the body dependent on those drugs, It is **drug dependence**. The drug action is affected by a set of factors such as the form, type, dose, mode of use, period of consumption and susceptibility of the addicted person. The addicted person becomes drug dependent through various stages such as experimental use for curiosity, recreational use, situational use, compulsive use and dependence. The addicted person shows some abnormal symptoms such as poor academic performance, indifference in the duties and responsibilities, change in behavior (e.g. telling lies, violence, unrest), change of physical appearance (e.g. loss of weight, vigor and appetite) and change in personality. There are two types of drug dependence - psychological and physical or neuroadaptation. In case of physical dependence, intake of drugs is essential to maintain physiological equilibrium. In case of psychological dependence, a person believes that the normal state can only be achieved with the action of the drugs.*

*There are several critical **causal factors** of **drug addiction** such as curiosity, the pressure from friends and relatives, high stress, pleasure, temporary relief from mental stress, frustration and depression, poor academic performance, problems in relationship management, job loss, unemployment, desire for more work, looking for a different world, relief from pain, family history, easy availability of drugs and money and excitement and adventure. Some students take drugs to keep awake the whole night for the preparation of their examinations or to manage high work load or backlog. It is a malpractice and bad habit.*

*Drugs act on brain and central nervous system. The structural and functional units of nerve cells are neurons; the message passes from one neuron to the other through **synapses**. Arrival of the nerve impulse causes the release of a chemical **neurotransmitter**. The drugs act at the synapses. The depressant drugs (e.g. alcohol, narcotics) inhibit the production of neurotransmitter or inactivation of the neurotransmitter more quickly or modify postsynaptic membrane. The stimulants increase the production of neurotransmitter and increase stimulation of the neurons. The general symptoms of drug addiction include excitement, violent nature, exhausted and drowsy appearance, poor concentration, memory loss, loss of interests in works, studies and social life, reduced appetite, vigor and weight and disorder of sleep. Ultimately, it results the cancer of mind of drug addicted people.*

*The addicts often suffer from the problems of central nervous system, psychosis, Hepatitis-B, AIDS, impotency, chromosal abnormalities and genetic disorder. Many of them have a dull unhappy life. They create problems for their families, neglect duties and may lose jobs. It may deprive a family of basic needs and may result frustration and insecurity of the children. The family members may suffer from physical and psychiatric problems such as headache, anxiety, insomnia and depression. The drug users get drugs from illegal sources encouraging smuggling, criminal activities, bio-terrorism and accidents. The drug addicts are less efficient and unreliable as workers and often lose their job or may not get employment anywhere. Life-science supply chain is a soft target of bio-terrorism. The drugs and medicines sold through popular distribution channels may be tainted, compromised and mislabeled. It needs strong support of drug quality and security act. The life-science supply chain has developed and produced breakthrough drugs and medicines that enhance the average life span in the world. Unfortunately, when bad things happen in life-science supply chain, the public get hurt. Today's life science supply chain requires an effective '**Drug Quality and Security Act and Standard**s' which is able to clarify with transparency the authority, roles and responsibilities of food and drugs administration and consumer protection ministry, regulate pricing*

of drugs, develop a national track-and-trace system to audit the functions of the life-science supply chain and minimize the risks of contamination, adulteration, diversion or counterfeiting.
It is essential to adopt a set of *good habits* by the students and youth as **proactive approach** through a value based education system at school and colleges to mitigate the risks of drug abuse.

- Intelligent reasoning through common sense, logical and analytical mind set;
- Be proactive and take responsibility of your life. Avoid bad habits and negative thinking; adopt good habits;
- Be dedicated, motivated and committed in learning;
- Define vision, mission and goals in life rationally and innovatively;
- Control physical and mental stress through yoga, meditation, relaxation music and extracurricular activities;
- Be conscious of physical, mental and social health;
- Prioritize multiple tasks through proper planning and time management and do the most important things first;
- Think win-win; have an everyone-can-win attitude with confidence, patience and perseverance;
- Listen to the other people carefully and sincerely. First try to understand and then to be understood;
- Promote synergy and collaborative intelligence, work together to achieve more through group dynamics;
- Sharpen the saw - renew yourself regularly. Analyze as-is state; find out gap and innovate to-be-state;
- Contribute to the society and environment through activities, thoughts and plans.

There are various strategies to mitigate the risk of drug abuse and drug addiction for **reactive approach**: deaddiction, childcare, drugs as social stigma, legal punitive action, strict regulatory compliance through effective corporate governance, corporate social responsibilities and good habit development through an effective education system. The physicians should prescribe drugs with responsibility and the pharmacists should not sell drugs without the valid prescriptions of the doctors. The parents should keep a watch and monitor the activities, attitude and behavior of their children. The social workers and policemen should be alert and inform the parents or deaddiction centers in time. In fact, law and the public should take joint responsibility against drug abuse.
Deaddiction is basically treatment of drug addiction or withdrawal symptoms of drugs. The major steps of deaddiction include master health check up (e.g. blood test, brain scanning), pharmacotherapy, psychosocial therapy, health restoration, psychological treatment and prevention of relapse. If a drug dependent person fails to get drugs, feels severe physical severe physical and psychological disturbances depending on the type and dosage of drugs. The general treatment of **withdrawal symptoms** of a drug is to replace the drug with a less reinforcing and legally available drug that can be gradually eliminated with decreasing doses. It is Pharmacotherapy. For the drug combination addiction, it is required to withdraw one drug at a time and maintain the others. After the withdrawal symptom subsides, psychological treatment persists and cause craving for the drugs. At this stage, the drug addicts need the moral support of their parents, relatives and friends. They may need the treatment at rehabilitation centers; it is a long term treatment requiring behavioral training of the patients. **Rehabilitation** involves the psychological and social therapy in the form of counseling by relatives, friends and physicians in a sympathetic manner. The patients should learn the ill effects of drug addiction through Psychosocial therapy. The patient also needs supportive measures such as administration of vitamins, proper nutrition, restoration of electrolytic balance and proper hydration. Vitamin C checks the rise of the level of cAMP in human brain. The patient may also need Psychological treatment. Finally, **readdiction** may occur; many addicts restart taking drugs after deaddcition. They should be watched by their near and dear ones.

4.2 Digestive system

Agents*: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);*
Model*: Human digestive system;*
Objectives*: cancer prevention at optimal cost;*
Constraints*: budget or financial constraint, resources, time, knowledge;*
Input*: Perception of human agent, performance measures of digestive system or test data;*
Strategic moves*: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;*
Revelation principle*: The agents preserve privacy of strategic data;*

- ***Defender*** *: The defenders share critical information collaboratively.*
- ***Attacker :*** *The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.*

Cancer Prevention Approaches:

- ***Proactive approach:***
  - ***Identify targets***
    - *application schema : digestive system;*
    - *networking schema :*
      - *alimentary canal – mouth, vestibule, oral cavity – tongue, teeth, pharynx, oesophagus, stomach, small intestine, large intestine;*
      - *digestive glands – salivary gland, gastric glands, liver, pancreas, intestinal glands,*
    - *computing schema :*
      - *nutrition mechanisms – autotrophic, holophytic, heterotrophic, symbiotic and holozoic;*
      - *movement of alimentary canal;*
      - *hormonal control of digestive secretion;*
      - *ingestion, digestion - intracellular, extracellular and mixed, egestion, absorption and assimilation;*
    - *data schema : nutrients – food (carbohydrates, protein, fat), minerals, vitamins, bile*
    - *security schema : malnutrition, over nutrition, incomplete digestive tract, cancer of alimentary canal (e.g. intestine) and digestive glands (e.g. liver, pancreas), oral cancer;*
  - ***Threat modeling***
    - *Call threat analytics function (f_a) and assess miscellaneous risk elements;*
    - *Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];*
    - *Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];*
    - *Map threats into a set of risk profiles or classes : LL, LH,HL and HH;*
    - *Estimate requirements of healthcare in terms of demand plan (P^p_d);*
    - *Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.*
      - *Auto-immunity and vaccination against hepatitis B and C;*
      - *Optimal diet intake to fight against malnutrition;*
      - *Life-style : Avoid smoking and alcohols, food habit, drug addiction control, obesity and overweight control through yoga and physical activities;*
- ***Reactive approach:***

- *adopt sense-and-respond strategy.*
- *assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.*
    - *what is corrupted or compromised?*
    - *time series analysis : what occurred? what is occuring? what will occur?*
    - *insights : how and why did it occur? do cause-effect analysis.*
    - *recommend : what is the next best action?*
    - *predict: what is the best or worst that can happen?*
- *verify security intelligence of application, computing, networking, security and data schema of biological system.*
    - ***Level1**: correctness, fairness, accountability, transparency, rationality, trust, commitment;*
    - ***Level 2**: authentication, authorization, correct identification, privacy, audit;*
    - ***Level3:** safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;*
    - ***Level4:** stability, system dynamics, quality of application integration.*
- *Explore risk mitigation plan (P^r_d and P^r_m).*
    - *Do medical testing → Data visualization of images (e.g. liver, pancreas and alimentary canal, Refer Deep Leaning Algorithm of section 2.1)*
    - *Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance;*
    - *Insulin injection*
    - *Artificial pancreas transplantation*
    - *Integrated medicine*
    - *Regenerative medicine*
    - *Chemotherapy*
    - *Laser*

- ***Fight against bad luck :** Identify critical risk elements.*
    - *Genetic disorder (sex, race, ethnicity, somatic mutation)*
    - *Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)*
    - *Injuries from accidents, war and crime*
    - *Occupational exposure*
    - *Water and soil pollution*
    - *Hostile climate, weather and other locational disadvantages, exposure to sunshine*
    - *Malnutrition due to poverty*
    - *Develop risk mitigation plan in terms of organ transplantation, surgical operation, gene therapy, stem cell therapy and migration of human civilization from risky zone.*

***Payment function**:*

- *Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.*
- *Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.*
- *Trade-off proactive vs. reactive security; assign weights to each approach.*
- *Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;*

***Output**: Cancer prevention plan*

4.3Respiratory system

Agents: *Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);*
Model: *Human respiratory system;*
Objectives: *cancer prevention at optimal cost;*
Constraints: *budget or financial constraint, resources, time, knowledge;*
Input: *Perception of human agent, performance measures of biological system or test data;*
Strategic moves: *deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;*
Revelation principle: *The agents preserve privacy of strategic data;*

- ***Defender*** : *The defenders share critical information collaboratively.*
- ***Attacker*** : *The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.*

Cancer Prevention Approaches:

- ***Proactive approach:***
  - ***Identify targets***
    - *application schema : respiratory system;*
    - *networking schema : respiratory tract, respiratory organs – lungs, tissues, larynx;*
    - *computing schema : breathing mechanism – inspiration, air filtering, exchange of gases in alveoli, expiration; nervous and chemical control of respiration, transport of gases in blood (O_2, CO_2), artificial respiration mechanism;*
    - *data schema (^) : respiratory rate, pulmonary air volume and capacity, composition of inspired, expired and alveolar air, TV, IRV,ERV,RV,VC,IC,FRC,TLC;*
    - *security schema : lung cancer, hypoxia, asphyxia, bad cold, bronchitis, bronchial asthma, pneumonia, emphysema, occupational respiratory disorder, carbon monoxide poisoning;*
  - ***Threat modeling***
    - *Call threat analytics function (f_a) and assess miscellaneous risk elements;*
    - *Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];*
    - *Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];*
    - *Map threats into a set of risk profiles or classes : LL, LH,HL and HH;*
    - *Estimate requirements of healthcare in terms of demand plan (P^p_d);*
    - *Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.*
      - *Auto-immunity and vaccination;*
      - *Optimal diet intake to fight against malnutrition;*
      - *Life-style : Avoid smoking and alcohols, food habit, drug addiction control, obesity and overweight control, yoga (deep breathing exercises) and physical activities, stress control through meditation;*
- ***Reactive approach:***
  - *adopt sense-and-respond strategy.*
  - *assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.*
    - *what is corrupted or compromised?*

        - ♦ *time series analysis : what occurred? what is occuring? what will occur?*
        - ♦ *insights : how and why did it occur? do cause-effect analysis.*
        - ♦ *recommend : what is the next best action?*
        - ♦ *predict: what is the best or worst that can happen?*
    - *verify security intelligence of application, computing, networking, security and data schema of biological system.*
        - ♦ ***Level1**: correctness, fairness, accountability, transparency, rationality, trust, commitment;*
        - ♦ ***Level 2**: authentication, authorization, correct identification, privacy, audit;*
        - ♦ ***Level3:** safety, reliability, consistency, liveness, deadlock freeness, reachability, resiliency;*
        - ♦ ***Level4:** stability, system dynamics, quality of application integration.*
    - *Explore risk mitigation plan (P^r_d and P^r_m).*
        - ♦ *Do medical testing of data schema (^);*
        - ♦ *Data visualization of X-ray report of lungs and also biopsy report;*
        - ♦ *Treating tobacco induced injuries in the air way, viral and bacterial infection, chronic inflammation; medication against chronic disease;*
        - ♦ *Integrated medicine*
- ***Fight against bad luck :** Identify critical risk elements.*
        - ♦ *Genetic disorder (sex, race, ethnicity, somatic mutation)*
        - ♦ *Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)*
        - ♦ *Injuries from accidents, war and crime*
        - ♦ *Occupational exposure*
        - ♦ *Air pollution*
        - ♦ *Hostile climate, weather and other locational disadvantages, exposure to sunshine, snowfall and very cold climate;*
        - ♦ *Malnutrition due to poverty*
    - *Develop risk mitigation plan in terms of organ transplantation, surgical operation, and migration of human civilization from risky zone.*

***Payment function**:*

- ♦ *Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.*
- ♦ *Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.*
- ♦ *Trade-off proactive vs. reactive security; assign weights to each approach.*
- ♦ *Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;*

***Output**: Cancer prevention plan*

4.4 Body fluids circulation – Cardiovascular system

***Agents**: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);*
***Model**: Human biological system – (a) body, (b) mind;*
***Objectives**: cancer prevention at optimal cost;*
***Constraints**: budget or financial constraint, resources, time, knowledge;*
***Input**: Perception of human agent, performance measures of biological system or test data;*

Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;

Revelation principle: The agents preserve privacy of strategic data;

- **Defender** : The defenders share critical information collaboratively.
- **Attacker :** The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.

Cancer Prevention Approaches:

- **Proactive approach**:
  - **Identify targets**
    - application schema : cardiovascular system;
    - networking schema : heart, blood vascular system – open and closed circulatory system, arterial and venous system, blood, tissue fluid, lymphatic system – spleen, thymus, tonsils
    - computing schema : pulmonary and systemic circulation, blood clotting or coagulation mechanism, blood flow mechanism
    - data schema : blood group, efficiency of heart, heart rate, heart output, pulse, heart sound;
    - security schema : blood cancer, blood pressure disorder (SP, DP), cardiovascular diseases – Stroke (CVA or cardiovascular accident), rheumatic heart disease (RHD), coronery artery disease (CAD), hepertensive heart disease, atrial fibrillation, tachycardia, vacuities;
  - **Threat modeling**
    - Call threat analytics function (f_a) and assess miscellaneous risk elements;
    - Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];
    - Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];
    - Map threats into a set of risk profiles or classes : LL, LH,HL and HH;
    - Estimate requirements of healthcare in terms of demand plan (P^p_d);
    - Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.
      - Auto-immunity and vaccination;
      - Optimal diet intake to fight against malnutrition;
      - Life-style : Avoid smoking and alcohols, food habit, drug addiction control, wild polygamy, obesity and overweight control through yoga and physical activities, stress control through meditation;
- **Reactive approach**:
  - adopt sense-and-respond strategy.
  - assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.
    - what is corrupted or compromised?
    - time series analysis : what occurred? what is occuring? what will occur?
    - insights : how and why did it occur? do cause-effect analysis.
    - recommend : what is the next best action?
    - predict: what is the best or worst that can happen?
  - verify security intelligence of application, computing, networking, security and data schema of biological system.
    - **Level1**: correctness, fairness, accountability, transparency, rationality, trust, commitment;
    - **Level 2**: authentication, authorization, correct identification, privacy, audit;

        - ***Level3:*** *safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;*
        - ***Level4:*** *stability, system dynamics, quality of application integration.*
    - *Explore risk mitigation plan (P^r_d and P^r_m).*
        - *Do medical testing → Data visualization of ECG*
        - *Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance;*
        - *Medication for blood pressure control;*
        - *Integrated medicine*
        - *Regenerative medicine*
        - *Chemotherapy*
        - *Laser*
- ***Fight against bad luck :*** *Identify critical risk elements.*
        - *Genetic disorder (sex, race, ethnicity, somatic mutation)*
        - *Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)*
        - *Injuries from accidents, war and crime*
        - *Occupational exposure*
        - *Air and sound pollution*
        - *Hostile climate, weather and other locational disadvantages, exposure to sunshine*
        - *Malnutrition due to poverty*
    - *Develop risk mitigation plan in terms of organ transplantation, surgical operation, blood substitution and migration of human civilization from risky zone.*

Payment function:

- *Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.*
- *Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.*
- *Trade-off proactive vs. reactive security; assign weights to each approach.*
- *Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;*

Output: *Cancer prevention plan*

4.5 Excretory system

Agents: *Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);*
Model: *Human excretory system;*
Objectives: *cancer prevention at optimal cost;*
Constraints: *budget or financial constraint, resources, time, knowledge;*
Input: *Perception of human agent, performance measures of biological system or test data;*
Strategic moves: *deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;*
Revelation principle: *The agents preserve privacy of strategic data;*

- ***Defender :*** *The defenders share critical information collaboratively.*
- ***Attacker :*** *The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.*

Cancer Prevention Approaches:

- ***Proactive approach***:
  - ***Identify targets***
    - *application schema : excretory system;*
    - *networking schema : kidney - nephron, ureters, urinary bladder and urethra; skin – sweat, lungs – CO_2,*
    - *computing schema : urea and urine formation, mechanism of kidney;*
    - *data schema : urine and stool – quantity, physical properties, chemical compositon and renal threshold;*
    - *security schema : kidney disorder - renal failure, kidney stone; uremia, cystitis, glomerrulonephritis, pyelonephritis, skin cancer, lungs cancer;*
  - ***Threat modeling***
    - *Call threat analytics function (f_a) and assess miscellaneous risk elements;*
    - *Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];*
    - *Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];*
    - *Map threats into a set of risk profiles or classes : LL, LH,HL and HH;*
    - *Estimate requirements of healthcare in terms of demand plan (P^p_d);*
    - *Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.*
      - *Auto-immunity and vaccination;*
      - *Optimal diet and water intake to fight against malnutrition;*
      - *Life-style : Avoid smoking and alcohols, food habit (e.g soft drinks), drug addiction control, wild polygamy, obesity and overweight control through yoga and physical activities;*
- ***Reactive approach***:
  - *adopt sense-and-respond strategy.*
  - *assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.*
    - *what is corrupted or compromised?*
    - *time series analysis : what occurred? what is occuring? what will occur?*
    - *insights : how and why did it occur? do cause-effect analysis.*
    - *recommend : what is the next best action?*
    - *predict: what is the best or worst that can happen?*
  - *verify security intelligence of application, computing, networking, security and data schema of biological system.*
    - ***Level1**: correctness, fairness, accountability, transparency, rationality, trust, commitment;*
    - ***Level 2**: authentication, authorization, correct identification, privacy, audit;*
    - ***Level3:** safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;*
    - ***Level4:** stability, system dynamics, quality of application integration.*
  - *Explore risk mitigation plan (P^r_d and P^r_m).*
    - *Do medical testing → Data visualization of kidney scan (Refer Deep Leaning Algorithm of section 2.1, transferring a Convolutional Neural Network, trained on images for detection of kidney problem in ultrasound images).*
    - *Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance;*
    - *Artificial kidney or kidney transplantation*
    - *Integrated medicine*
    - *Regenerative medicine*
    - *Chemotherapy*

- Laser

- ***Fight against bad luck :*** *Identify critical risk elements.*
  - *Genetic disorder (sex, race, ethnicity, somatic mutation)*
  - *Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)*
  - *Injuries from accidents, war and crime*
  - *Occupational exposure*
  - *Water pollution*
  - *Hostile climate, weather and other locational disadvantages, exposure to sunshine*
  - *Malnutrition due to poverty*
- *Develop risk mitigation plan in terms of organ transplantation, surgical operation, gene therapy, stem cell therapy and migration of human civilization from risky zone.*

Payment function:

- *Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.*
- *Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.*
- *Trade-off proactive vs. reactive security; assign weights to each approach.*
- *Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;*

Output: *Cancer prevention plan*

4.6 Locomotion and movement

Agents: *Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);*
Model: *Human biological system – (a) body, (b) mind;*
Objectives: *cancer prevention at optimal cost;*
Constraints: *budget or financial constraint, resources, time, knowledge;*
Input: *Perception of human agent, performance measures of biological system or test data;*
Strategic moves: *deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;*
Revelation principle: *The agents preserve privacy of strategic data;*

- ***Defender :*** *The defenders share critical information collaboratively.*
- ***Attacker :*** *The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.*

Cancer Prevention Approaches:

- ***Proactive approach:***
  - ***Identify targets :***
    - *application schema : human skeletal and mascular system;*
    - *networking schema :*
      - *skeleton – bone (skull, spinal column, ribs, sternum, girdles, limb), cartilage, joints;*
      - *muscles – red and white;*
    - *computing schema : locomotion and movement mechanism, autonomic and induced movement, muscle contraction mechanism;*
    - *data schema : oxygen debt, muscle fatigue;*

        - *security schema : bone cancer, cervical cancer, breast cancer, sprain, arthritis, osteoporosis, dislocation, slipped disc, fracture of bones, bursitis, tetany, myasthenia gravis and muscular dystrophy.*
    - ***Threat modeling***
        - *Call threat analytics function (f_a) and assess miscellaneous risk elements;*
        - *Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];*
        - *Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];*
        - *Map threats into a set of risk profiles or classes : LL, LH,HL and HH;*
        - *Estimate requirements of healthcare in terms of demand plan (P^p_d);*
        - *Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.*
            - *Auto-immunity and vaccination;*
            - *Optimal diet intake to fight against malnutrition;*
            - *Life-style : Avoid smoking and alcohols, food habit, drug addiction control, wild polygamy, obesity and overweight control*
            - *yoga and physical mascular activities, stress control through meditation;*
            - *Use computers, tablets and laptops with a safe posture;*
            - *Avoid wearing tight dress and safe message to avoid breast cancer.*

- ***Reactive approach**:*
    - *adopt sense-and-respond strategy.*
    - *assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.*
        - *what is corrupted or compromised?*
        - *time series analysis : what occurred? what is occuring? what will occur?*
        - *insights : how and why did it occur? do cause-effect analysis.*
        - *recommend : what is the next best action?*
        - *predict: what is the best or worst that can happen?*
    - *verify security intelligence of application, computing, networking, security and data schema of biological system.*
        - ***Level1**: correctness, fairness, accountability, transparency, rationality, trust, commitment;*
        - ***Level 2**: authentication, authorization, correct identification, privacy, audit;*
        - ***Level3:** safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;*
        - ***Level4:** stability, system dynamics, quality of application integration.*
    - *Explore risk mitigation plan (P^r_d and P^r_m).*
        - ***Do medical testing → Data visualization of digital x-ray***
        - *Convolutional network for tumor detection in breast mammography (Refer Deep Leaning Algorithm of section 2.1)*
        - *Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance;*
        - *Physiotherapy*
        - *Integrated medicine*
        - *Regenerative medicine*
        - *Chemotherapy*
- ***Fight against bad luck :** Identify critical risk elements.*
    - *Genetic disorder (sex, race, ethnicity, somatic mutation)*
    - *Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)*

        - ♦ *Injuries from accidents, war and crime*
        - ♦ *Occupational exposure*
        - ♦ *Environmental pollution*
        - ♦ *Hostile climate, weather and other locational disadvantages, exposure to sunshine*
        - ♦ *Malnutrition due to poverty*
    - *Develop risk mitigation plan in terms of organ transplantation, surgical operation, and migration of human civilization from risky zone.*

Payment function:

- ♦ *Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.*
- ♦ *Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.*
- ♦ *Trade-off proactive vs. reactive security; assign weights to each approach.*
- ♦ *Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;*

Output*: Cancer prevention plan*

4.7 Neural control and coordination

Agents*: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);*
Model*: Human nervous system, sensory system;*
Objectives*: cancer prevention at optimal cost;*
Constraints*: budget or financial constraint, resources, time, knowledge;*
Input*: Perception of human agent, performance measures of biological system or test data;*
Strategic moves*: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;*
Revelation principle*: The agents preserve privacy of strategic data;*

- ♦ ***Defender :*** *The defenders share critical information collaboratively.*
- ♦ ***Attacker :*** *The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.*

Cancer Prevention Approaches:

- ***Proactive approach:***
    - ***Identify targets***
        - ♦ *application schema : Nervous and sensory system;*
        - ♦ *networking schema :*
            - ▪ *Nervous system : CNS – Brain, spinal chord; PNS, Neurons, nerves, cerebrospinal fluid, brain stem, meninges, neuroglia, ependymal cells, neurosecretory cells;, cerebral nerve, spinal nerve;*
            - ▪ *Sensory organs : eye, ear, nose, toungue, skin;*
        - ♦ *computing schema : nerve impulse, reflex, neurotransmitter, neurosecretion, chemoreception; control and coordination, integration, memory, mechanism of sensory organs – see, hear, smell, feel, taste;*
        - ♦ *data schema : sensory receptors – photo, chemo, thermo, electro and mechanoreceptors; structure of sensory organs;*
        - ♦ *security schema : disorders of nervous system – brain tumor, memory loss, poliomyelitis, meningitis, sciatica, neuritis, synaptic delay, synaptic fatigue;*

Eye defects – myopia, hypermetropia, astigmatism, presbiopia, cataract, glaucoma; skin cancer;

- ***Threat modeling***
  - *Call threat analytics function (f_a) and assess miscellaneous risk elements;*
  - *Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];*
  - *Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];*
  - *Map threats into a set of risk profiles or classes : LL, LH,HL and HH;*
  - *Estimate requirements of healthcare in terms of demand plan (P^p_d);*
  - *Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.*
    - *Optimal diet intake to fight against malnutrition;*
    - *Life-style : yoga and physical activities, stress control through meditation;*
    - *Eye, ear and skin care against hostile climate (e.g. snowfall, scorching sunshine)*

- ***Reactive approach:***
  - *adopt sense-and-respond strategy.*
  - *assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.*
    - *what is corrupted or compromised?*
    - *time series analysis : what occurred? what is occuring? what will occur?*
    - *insights : how and why did it occur? do cause-effect analysis.*
    - *recommend : what is the next best action?*
    - *predict: what is the best or worst that can happen?*
  - *verify security intelligence of application, computing, networking, security and data schema of biological system.*
    - ***Level1:*** *correctness, fairness, accountability, transparency, rationality, trust, commitment;*
    - ***Level 2:*** *authentication, authorization, correct identification, privacy, audit;*
    - ***Level3:*** *safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;*
    - ***Level4:*** *stability, system dynamics, quality of application integration.*
  - *Explore risk mitigation plan (P^r_d and P^r_m).*
    - *Do medical testing → Data visualization of brain scan (Refer Deep Leaning Algorithm of section 2.1)*
    - *Treating viral and bacterial infection, chronic inflammation, pain;*

- ***Fight against bad luck :*** *Identify critical risk elements.*
  - *Genetic disorder (sex, race, ethnicity, somatic mutation)*
  - *Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)*
  - *Injuries from accidents, war and crime*
  - *Occupational exposure*
  - *Environmental pollution*
  - *Hostile climate, weather and other locational disadvantages, exposure to sunshine*
  - *Malnutrition due to poverty*
  - *Develop risk mitigation plan in terms of organ transplantation, surgical operation, and migration of human civilization from risky zone.*

Payment function:

- Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.
- Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.
- Trade-off proactive vs. reactive security; assign weights to each approach.
- Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;

Output: Cancer prevention plan

4.8 Chemical coordination and integration

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human endocrine system;
Objectives: cancer prevention at optimal cost;
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- **Defender** : The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM);
- **Attacker :** The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.

Cancer Prevention Approaches:

- **Proactive approach**:
    - **Identify targets :**
        - application schema : Endocrine, Exocrine and Heterocrine system
        - networking schema : Glands – hypothalamus, pituitary, pineal, thyroid, parathyroid, thymus, adrenals, pancreas, gonads : testes and ovaries, kidneys;
        - computing schema : coordination between endocrine and nervous system, interaction among glands, hormone action mechanism (formation of Camp);
        - data schema : hormones (informational molecules secreted by endocrine cells), hypothalamus – neurohormones > release hormones (RH), inhibitory hormones (IH); pituitary – FSH LH, GTH, TSH, ACTH, GH (*),LTH, OT; pineal – melatonin; thyroid – thyroxine (**), calcitonin; parathyroid – PTH (#), thymus - thymosine, adrenals - aldosterone, glucocorticoids, sexcorticoids (##); pancreas – insulin ($), glucagon, SS; gonads : testes – LH and ovaries – Estrogen, Progesterone and Relaxin; kidneys - Renin; primary, secondary and final targets;
        - security schema :
            - over secretion – Gigantism (*); Grave's disease(**), osteoporosis (#)
            - deficiency – Dwarfism(*), Goitre(**), Addison's disease (##), Diabetes mellitus ($);
    - **Threat modeling**
        - Call threat analytics function (f_a) and assess miscellaneous risk elements;
        - Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];
        - Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];

- Map threats into a set of risk profiles or classes : LL, LH,HL and HH;
- Estimate requirements of healthcare in terms of demand plan (P^p_d);
- Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.
    - Optimal diet intake to fight against malnutrition;
    - Life-style : Avoid smoking and alcohols, food habit, drug addiction control, obesity and overweight control through yoga and physical activities, stress control through meditation;

- **Reactive approach**:
    - adopt sense-and-respond strategy.
    - assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.
        - what is corrupted or compromised?
        - time series analysis : what occurred? what is occuring? what will occur?
        - insights : how and why did it occur? do cause-effect analysis.
        - recommend : what is the next best action?
        - predict: what is the best or worst that can happen?
    - verify security intelligence of application, computing, networking, security and data schema of biological system.
        - **Level1**: correctness, fairness, accountability, transparency, rationality, commitment;
        - **Level 2**: authentication, authorization, correct identification, privacy, audit;
        - **Level3:** reliability, consistency, liveness, resiliency;
        - **Level4:** stability, system dynamics, quality of application integration.
    - Explore risk mitigation plan (P^r_d and P^r_m).
        - Do medical testing → Data visualization
        - Treating hormonal imbalance through hormone therapy;
        - Integrated medicine
        - Regenerative medicine
- **Fight against bad luck :** Identify critical risk elements.
    - Genetic disorder (sex, race, ethnicity, somatic mutation)
    - Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)
    - Malnutrition due to poverty
    - Develop risk mitigation plan in terms of surgical operation, gene therapy, stem cell therapy.

Payment function:

- Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.
- Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.
- Trade-off proactive vs. reactive security; assign weights to each approach.
- Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;

Output: Cancer prevention plan

5. Conclusion

This work explores the importance of a deep analytics based mechanism for cancer prevention in the context of human biological system. It presents a new framework of human biological system in terms of computing, data, networking, application and security schema of an information system based on analogical reasoning. DACPM promotes a hybrid approach which recognizes the role of both proactive and reactive approaches in making decisions on healthcare investment for cancer prevention. The reactive approach may outperform proactive one against the threats that never occur actually. Sometimes, reactive approach may be cost effective as compared to proactive approach. The basic building blocks of the proposed mechanism are threat analytics and adaptive secure multiparty computation. The threat analytics monitor the system performance of human biological system based on time series data, detects and analyzes different types of vulnerabilities on the biological system.

Artificial intelligence (AI) is basically simulation of human intelligence. An intelligent reasoning system demands new data structure beyond knowledge base with envison, perception and proper assessment of a problem; reasoning is not effective when done in isolation from its significance in terms of the needs and interests of an agent with respect to the wider world. A rational reasoning system needs the support of an intelligent analytics. The basic objective is to evaluate the natural and adaptive immunity of a complex system. The evaluation of the immunity of a system involves modeling, defining complete specifications and verification. First, it is essential to model the human biological system by proper representation of its various states and programs. Next, it is important to specify the properties of the system through logical reasoning. Finally, it is essential to develop a verification mechanism which justifies: does the model satisfy the properties indicating a healthy immune system? The evaluation of immunity of a system can be done by exhaustive search of the state space (local, global, initial and goal states and state transition relations) of a system through simulation, testing, deductive reasoning and model checking based on intelligent search. The procedure terminates with positive or negative answer; the positive answer indicates a healthy immune system; the negative results provide an error trace indicating incorrect modeling or specification of the system or the occurrence of malicious threats. The human immune system is an adaptive, robust, complex and distributed information processing system which protects the health of the biological system from the attacks of malicious foreign pathogens (e.g. virus, bacteria, fungi, protozoa, parasitic worms). It discriminates the self from non-self elements. The immunity is either innate or adaptive; innate immunity detects and kills specific known invading organisms; adaptive immunity responds to previously unknown foreign organisms. AI community needs a new outlook, imagination and dreams to solve a complex problem like prevention of cancer through a set of simple mechanisms. There are some types of cancer due to bad luck. But, we still do not know enough about the causes and preventive measures of different types of cancer.

This work finds a set of interesting research agenda for future work: (a) explore new risk factors and causes of cancer, classifying cancers, opportunities for early detection and prevention and cost reduction of cancer care; (b) how to design an intelligent threat analytics; (c) how to design intelligent verification mechanisms; (d) how to rationalize DACPM, (e) how to quantify and code miscellaneous security intelligence parameters, (e) check the performance of kernel based learning algorithms with CNN, (g) how to apply integrated medicine and exercise allopathic, homeopathy, herbal , yoga and naturopathy effectively for various purposes such as pain management, combating side effects of radiation and chemotherapy (e.g. hair fall, nausea, vomiting), every cancer patient requires specific treatment considering complexity of disease and (g) explore new approaches of cancer prevention such as vaccination for auto-immunity, laser therapy, integrated and regenerative medicine, gene therapy and stem cell therapy.

Acknowledgment : The first author has got the inspiration and motivation of this work from various experiences such as attending courses on Artificial Neural Networks and Management Information Systems and thesis work as part of Fellow Programme at IIM Calcutta, India; courses such as Measurement and Instrumentation for biomedical engineering as part of Bachelor of Electrical Engineering at Jadavpur University, Kolkata and IT consulting experience on a healthcare supply chain in USA. The second author has got motivation from his project of drug abuse and preventive measures. This work may be the example of an interesting project for ANN and Machine Learning of various technical, medical and management education programmes.

REFERENCES

1. B. W. Stewart, C. P. Wild, Eds., World Cancer Report 2014, IARC.
2. C.Tomasetti C and B.Vogelstein. 2015. Cancer etiology. Variation in cancer risk among tissues can be explained by the number of stem cell divisions. Science, 347(6217):78–81.
3. A.Albini, F. Tosetti, VW Li. 2012. Cancer prevention by targeting angiogenesis. Nat Rev Clin Oncol. 9(9):498–509.
4. G. Anthes. 2013. Deep learning comes of age. Communications of the Association for Computing Machinery (ACM), 56(6):13–15.
5. I. Arel, C. Rose, and T. Karnowski. 2010. Deep machine learning — a new frontier in artificial intelligence. IEEE Computational Intelligence Magazine,5:13–18.
6. Y. Bengio. 2013. Deep learning of representations: Looking forward. In Statistical Language and Speech Processing, pages 1–37. Springer.
7. L. Deng. 2011. An overview of deep-structured learning for information processing. In Proceedings of Asian-Pacific Signal & Information Processing Annual Summit and Conference (APSIPA-ASC). October 2011.
8. N. Nisan and A.Ronen. 1999. Algorithmic mechanism design. In 31st Annual ACM symposium on Theory of Computing, pp 129 -140.
9. S. Chakraborty. 2007. A study of several privacy preserving multi-party negotiation problems with applications to supply chain management. Indian Institute of Management Calcutta, India.
10. A.Barth, B.Rubinstein, M.Sundararajan, J.Mitchell, D.Song and P.L. Bartlett. 2010. A learning-based approach to reactive security. In: Radu, S. (ed.) Financial Cryptography' 2010. LNCS, vol. 6052, pp. 192–206. Springer.
11. R.Bohme and T.W.Moore. 2009. The iterated weakest link: A model of adaptive security investment. In: Workshop on the Economics of Information Security (WEIS), University College, London, UK.
12. Y. Lindell. 2003. Composition of secure multi-party protocols a comprehensive study. Springer.
13. R.Canetti, U.Feige, O.Goldreich and M.Naor. 1996. Adaptively secure multi-party computation.
14. M.Kearns and M. Li. 1993. Learning in the presence of malicious errors. SIAM Journal on Computing 22(4), 807–837.
15. M.Barreno, B.Nelson, R. Sears, R., A.D. Joseph and J.D.Tygar. 2006. Can machine learning be secure? In Proceedings of the ACM symposium on Information, computer, and communications security.
16. S.Chakraborty. 2015. Secure multi-party computation: how to solve the conflict between security and business intelligence. Technical report.