Algorithmic Mechanism Construction bridging Secure Multiparty Computation and Intelligent Reasoning

Sumit Chakraborty

Fellow (Indian Institute of Management Calcutta), Bachelor of Electrical Engineering (Jadavpur University), India, E-mail: surya20046@yahoo.co.in, schakraborty2010@hotmail.com; Phone: 91-9940433441

Abstract

This work presents the construction of intelligent algorithmic mechanism based on multidimensional view of intelligent reasoning, threat analytics, cryptographic solutions and secure multiparty computation. It is basically an attempt of the cross fertilization of distributed AI, algorithmic game theory and cryptography. The mechanism evaluates innate and adaptive system immunity in terms of collective, machine, collaborative, business and security intelligence. It also shows the complexity analysis of the mechanism and experimental results on three test cases: (a) intrusion detection, (b) adaptively secure broadcast and (c) health security.

Keywords: *Algorithmic mechanism, Intelligent reasoning, Threat analytics, Security intelligence, Intrusion detection.*

1. INTRODUCTION

Recently, there is a trend of cross fertilization between two disciplines: game theory and cryptography [1]. Cryptography focuses on secure multi-party computation preserving privacy, fairness and correctness against the threats of malicious agents. Game theory tries to understand the behavior of rational agents with well defined goals in a given situation and designs the rules of interaction. [2] shows the differences between the two disciplines based on specific issues such as players, solution drives, incentives, privacy, trust, early stopping, deviation and collusion. Cryptography assumes honest or malicious players; game theory assumes rational players; the solution drivers are secure protocol and equilibrium respectively. Both disciplines study collaborative interactions among the agents with conflicting interests [4]. It is possible to solve traditional game theoretic problems and design of efficient mechanisms using the concept of cryptographic solutions and secure multi-party computation [5,6]. It is also an interesting research agenda to explore new cryptographic concerns using game theoretic concepts such as secure and fair computation and rational secret sharing [4,7]. Traditionally, cryptographic solutions are focused on the privacy, fairness and correctness to ensure information security. The domain needs a broad outlook for improved efficiency in new applications.

Game theory is concerned with a complex decision making process in which two or more players interact. Each of these players tries to optimize its own objective function. A game can be classified as *cooperative game* or a *non-cooperative game*. In a cooperative game, the players make agreements in order to minimize their common cost or to maximize their common payments. This is not possible in a non-cooperative game. A cooperative game is a game where a group of players enforce a cooperative behavior. The game is defined by (N,u) where N denotes a group of agents and u is a real valued characteristic function. A subset $S \subseteq N$ is called a *coalition*, where N is called the *grand coalition*.

A *mechanism* is defined by various types of elements: a group of agents or players, 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 and revelation principle [3]. Each agent adopts and executes a strategy. A pure strategy is a deterministic policy for a single move game. For many games, an agent can do better with a mixed strategy, which is a randomized policy that selects actions according to a probability distribution. Absolute privacy or confidentiality may result an inefficient mechanism. Therefore, the agents preserve the privacy of strategic data but share critical information. A mechanism is truthful if the agents report their strategic moves correctly. Truth telling may be a dominant strategy. A mechanism is strongly truthful if truth telling is the only dominant strategy. The basic objective of a game is to find an acceptable distribution of cost among the agents. A mechanism tries to implement desired social choices in a strategic setting assuming that different agents of a society act rationally. A social choice is basically the aggregation of the private preferences of different agents to a single joint decision. The concept of mechanisms is applicable in various domains such as policy making in corporate governance, distributed AI, voting, e-market and auction.

Imputations are efficient and individually rational distribution. An imputation $\boldsymbol{y} = (y_1, \ldots, y_N)$ is a vector such that cost y_i is allocated to player and $y(N) = \sum_{i=1}^{N} y_i$. A *solution concept* of the game must satisfy a number of properties. The total cost allocated to the players must be equal to the total cost of the game, y(N) = c(N). The cost allocated to a player should not be higher than the cost the player would have to incur if he acts individually without joining others. This property is known as *individual rationality*. The allocation of cost should be symmetric. The solution should satisfy the property of monotonocity. If the overall cost increases, the allocation of the agent should increase accordingly. The core is the most significant fair solution concept of a game. In a core solution there is no incentive for any player to leave the grand coalition, the core solutions are stable. In a game (N,c), the *core* is defined as those imputations y that satisfy $y(S) \leq c(S)$, $S \subseteq N$ and y(N) = c(N). The total cost allocated to the players in a game should not exceed the cost of a system dedicated to the coalition and should satisfy group and individual rationality constraints. The efficiency constraint implies that the total cost of the game is to be equitably distributed among the players. Bargaining set is a set of objections and counter objections. An imputation y belongs to a *bargaining set* M(c) of the game if for any objection of a player against another with respect to y there exists a counter objection. The agents start negotiation with a set of initial plans, negotiate and settle a set of final plans. The *nucleolus* indicates those imputations that minimize the maximum discontent of any player of a game. The *kernel* of a game indicates the imputations for which no player outweighs another player. The *shapely value* is the unique payoff vector that is symmetric, additive and efficient. This also satisfies anonymity and assigns zero payoffs to dummy players. The order of the players does not affect the costs allocated to the players.

The *contributions* of the current work are as follows. The basic objective is how to construct an efficient mechanism in a computational setting based on multi-dimensional view of intelligent reasoning. First, this study develops artificial immune mechanism (AIM); then performs complexity analysis of AIM in terms of security intelligence and computational intelligence and finally shows the experimental results on three test cases using AIM. The mechanism explores new cryptographic concerns. The mechanism is modeled in terms of a system having states and state relations, a group of agents, 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, payment function, an optimal set of moves, revelation principle and verification protocols. The mechanism evaluates the innate and adaptive immunity of the system in terms of collective, machine, collaborative, business and security intelligence. The agents exchange information and search for a fair consensus. The optimal performance of a system requires the execution of a precise set of strategic moves by the agents since a single move may not be enough to optimize the performance of the system. These moves are not always in the best interest of an agent. The agents often try to optimize their own objectives and it may result poor performance. The performance of the system can be improved if the agents coordinate through a set of moves such that the objective of each agent becomes aligned with the objective of the system. It requires sharing of strategic information for effective coordination among the agents. But, privacy is a critical issue for sharing information. The performance of the system can be optimized if the agents share their strategic information truthfully using protocols based on cryptographic solutions and secure multi-party computation. This work is organized as follows. Section 2 presents the mechanism (AIM). Section 3 shows the complexity analysis of AIM. Section 4 analyzes three test cases on intrusion detection, adaptively secure broadcast and health security through AIM. Section 5 concludes the work.

2. Algorithmic Mechanism Construction

This section presents the basic overview of the construction of an algorithmic mechanism. Let us consider a specific problem for this purpose where the basic objective is to evaluate the natural and adaptive immunity of a complex system through an intelligent mechanism. It is not rational to mix the concept of immunity with security. Security is an essential part of immunity; the evaluation of immunity needs the reasoning on the needs and interest of the complex system with a broader outlook. The evaluation of the immunity of a system involves modeling, defining complete specifications and verification. First, it is essential to develop the model (m) a system by proper representation of its various states and programs. Next, it is important to specify the properties (p) of the system through logical reasoning. Finally, it is essential to develop a verification mechanism which justifies: does the model (m) satisfies the properties (p) 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. Let us construct an Artificial Immune Mechanism (AIM) for the aforesaid problem.

Artificial Immune Mechanism (AIM)

##

System : states (local, global, initial, goal), state transition relation;
Agents : Detective, cryptographic objects;
Moves *:*

- *Multidimensional view of intelligent reasoning* (logical, analytical, case based, forward and backward chaining, sequential, parallel, uncertainty, probabilistic, approximation, predictive, imaginative, perception);
- *Define system immunity* (i) = f(a,b,c,d,e); a: collective intelligence, b: machine intelligence, c: security intelligence, d: collaborative intelligence, e: business intelligence; f : secure verification function;
- *Private search* for evidence ;
- *Private communication* using signcryption algorithms;

```
Input : A self-set $S \subseteq U$, a monitoring set $M \subseteq U$ for a given system parameters;
Output: for each element $m \in M$, either self or non-self, danger or normal;
$D \leftarrow$ set of detectors that do not match any $s \in S$;
for each $m \in M$ do
{
    call threat analytics (A) $\rightarrow$ sense danger signal;
    secure function evaluation $\rightarrow$ verify innate and adaptive system immunity i = f(a,b,c,d,e);
}
sense-challenge-respond to system immunity resiliently;
if $m$ matches any detector $d \in D$ then identify m as non-self;
else identify m as self;
check if non-self node is benign or malign;
if it is malign then suppress it else give alert.
```

##

3. Complexity Analysis

Theorem 1 : AIM verifies innate and adaptive system immunity in terms of collective, security, collaborative, machine and business intelligence based on multi-dimensional view on intelligent reasoning.

AIM outlines artificial immune system mechanism algorithmically. It is defined by a set of elements : system, a group of agents, 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, payment function, an optimal set of moves, revelation principle and model checking or system verification protocol. The proposed mechanism evaluates the innate and adaptive immunity of a system which is defined by a set of states (e.g. initial, goal, local and global) and state transition relations. Cryptographic agents models one or more interacting objects involved in secure multi-party computation.

The mechanism follows a set of intelligent moves. The first move of AIM is multidimensional view of intelligent reasoning. Intelligent reasoning is a consortium of methodologies that works synergistically and provides flexible information processing capability for handling ambiguous situations in complex problems. The basic objective is to exploit the tolerance for imprecision, uncertainty, approximate reasoning, and partial truth in tractable, robust and low cost solutions. It is critical for the agents to select appropriate reasoning techniques such as logical, analytical, case based, forward and backward chaining, sequential, parallel, uncertainty, probabilistic, approximation, predictive, imaginative and perception depending on the demand of the mechanism [16-21]. The effectiveness of reasoning depends on various factors : knowledge base, sound and complete logic, inference rules, intelligence and decision making capability of agents and knowledge representation technique. In complex decisions, the expert knowledge may not be expressed in terms of single rules but in the form of chaining multiple rules together based on available data. There are two approaches of inferencing such as forward and backward chaining. *Forward chaining* views IF part of a rule first and the rule makes conclusion when all IF conditions are met. *Backward chaining* is the reverse of forward chaining; it starts from the conclusion and then identifies the IF conditions. *Probabilistic reasoning* evaluates uncertainty which may arise due to laziness and ignorance. It is inescapable in complex, nondeterministic or partially observable environments. Probabilities indicate inability of an agent to reach a definite decision; it summarizes the agent's beliefs relative to the evidence. It is important to combine the agent's beliefs and desires, fixing the best action plan that can improve expected utility. Agents can perform different types of tasks without any measurements and any computations based on *perception*, common *sense reasoning* or heuristics. *Heuristics* are intuitive knowledge or thumb rules learned from experience. Reasoning has multiple dimensions like common sense, automated theorem proving, planning, understanding, hypothetical, simulation dynamics and envisioning through imagination or anticipation of alternatives [19].

The next critical move is how to detect the danger signal from a system [23-25]? The mechanism evaluates system immunity (i) combinatorially in terms of collective intelligence, machine intelligence, security intelligence, collaborative intelligence and business intelligence. The *collective intelligence* (a) is defined in terms of scope, input, output, process, agents and system dynamics. For a complex application, it verifies coordination and integration among system, strategy of growth and development, structure, staff, style, skill and shared vision. What is being done by the various components of a system? Who is doing? Why? How? Where? When? The *machine intelligence* (b) checks the system in terms safety, levelness, concurrency, reachability, deadlock freeness, scalability and accuracy. For example, it should check design flaws, preconditions, post conditions, triggering events, main flow, sub flow, alternate flow, exception flow, computational intelligence, communication cost, traffic congestion, time and space complexity, resources, capacity utilization, load, initial and goal states, local and global states and state transition plans of an information system. The *collaborative intelligence* (d) evaluates the feasibility and effectiveness of human-computer interaction to achieve single or multiple set of goals, information sharing principle and negotiation protocol. The *business intelligence* (e) looks after business rules such as payment function, cost sharing, contractual clauses, bonus, compensation, incentive policy, quality, system's performance and competitive intelligence.

The *security intelligence* (c) verifies the system in terms of authentication, authorization, correct identification, non-repudiation, integrity, audit and privacy; rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, commitment, reliability and consistency [8,9]. The mechanism may not be efficient due to trust deficit; it needs the support of cryptographic solutions (e.g. encryption, decryption, signcryption, privacy preserving data mining) to ensure an efficient revelation principle. Theorem 2 analyzes the security intelligence in details. The basic principle of AIM is artificial immune system (AIS), a novel computational intelligence technique inspired by immunology [10-12]. It is a young and evolving field; the basic objective is to preserve and improve the immunity of a system through negative selection, danger signal detection, clonal selection, suppression and hyper mutation [13-15,22,27]. 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.

Negative selection is an immune inspired classification scheme. For a given set of self sensor nodes, it generates a set D of detectors that do not match with any element of *S*. Then, these detectors are used to partition a monitor set M into self and non-self elements. The problem faced by human immune system is similar to that of information and communication technology schema. It is difficult to defend a system against a previously unknown danger. The only reliable knowledge is the normal behavior of the system which is equivalent to self nodes of the distributed system. Negative selection mimics the human immune system; it generates a set of detectors that do not match with self nodes, these detectors are used to monitor the abnormal behavior of the distributed system caused by the attack of non-self nodes. *Danger* threatens living organisms; the danger theory suggests that the human immune system detects danger to trigger appropriate immune responses. The optimal trade-off between the concentration of danger and safe signals within human tissues produce proper immune responses. Danger also threatens distributed computing systems. Danger theory can be applicable to intrusion detection. It is an interesting option to build a computational model which can define and detect danger signals. The danger signals should be detected fast and automatically to minimize the impact of malicious attacks by the intruders on a distributed system.

The mechanism verifies system immunity through a set of verification algorithms which include model checking, simulation, testing and deductive reasoning for automated verification. Simulation is done on the model while testing is performed on the actual product. It checks the correctness of output for a given input. Deductive reasoning tries to check the correctness of a system using axioms and proof rules. There is risk of state space explosion problem in case of a complex system with many components interacting with one another; it may be hard to evaluate the efficiency of coordination and integration appropriately. Some applications also demand semi-automated and natural verification protocol. The mechanism calls threat analytics and assesses risks of single or multiple attacks on the system under consideration: analyze performance, sensitivity, trends, exception and alerts; checks what is corrupted or compromised: agents, protocol, communication / data / application / computing schema? Performs time series analysis: what occurred? what is occuring? what will occur? assess probability of occurrence and impact; explores insights : how and why did it occur? do cause-effect analysis; recommends : what is the next best action? predicts: what is the best or worst that can happen?

Theorem 2 : AIM verifies security intelligence collectively through rational threat analytics.

The security intelligence of AIM is a multi-dimensional parameter which is defined in terms of rationality, fairness, correctness or accuracy, resiliency, adaptation, transparency, accountability, trust, reliability, consistency, commitment; safety, liveness, synchronization, reachability, deadlock freeness; authentication, authorization, correct identification, non-repudiation, integrity, audit and privacy. AIM addresses the issues of authentication, authorization, correct identification, privacy and audit through cryptographic solutions. For any secure service, the system should ask the identity and authentication of one or more agents involved in a communication. 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, a service should address the issue of authorization. The system should be configured in such a way that an unauthorized agent cannot perform any 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; an agent can view only the information according to authorized access rights. A protocol 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.

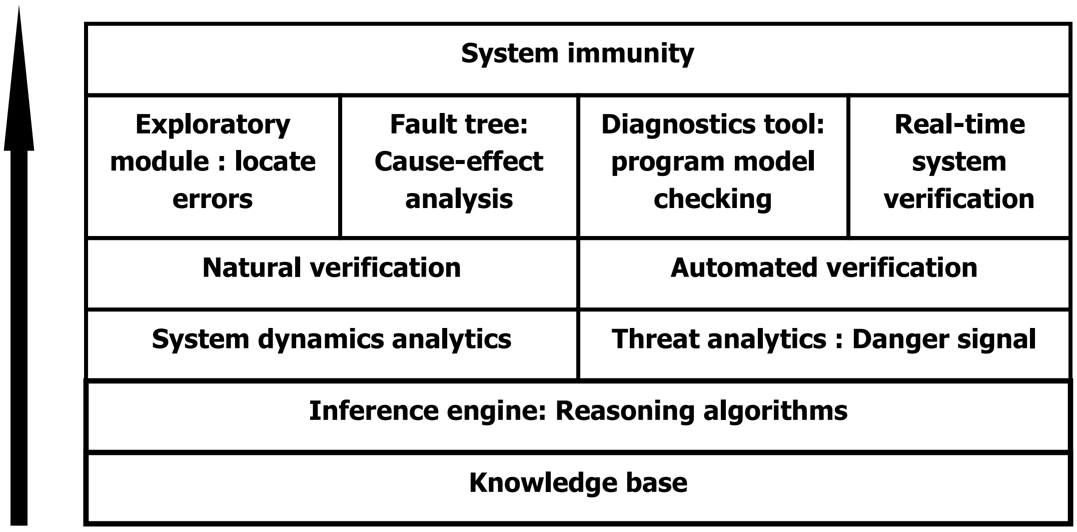
Privacy is the primary concern of the revelation principle of a mechanism; the issue can be addressed through the concept of cryptography and secure multiparty computation [9]. The fundamental objectives of cryptography are to provide confidentiality, data integrity, authentication and non-repudiation. Cryptography ensures privacy and secrecy of information through encryption methods. The sender (S) encrypts a message (m) with encryption key and sends the cipher text (c) to the receiver (R). R turns c back into m by decryption using secret decryption key. In this case, an adversary may get c but cannot derive any information. R should be able to check whether m is modified during transmission. R should be able to verify the origin of m. S should not be able to deny the communication of m. There are two types of key based algorithms. Symmetric key encryption scheme provides secure communication for a pair of communication partners; the sender and the receiver agree on a key k which should be kept secret. In most cases, the encryption and decryption key are same. In case of asymmetric or public-key algorithms, the key used for encryption (public key) is different from the key used for decryption (private key). The decryption key cannot be calculated from the encryption key at least in any reasonable amount of time. The widely-used public–key cryptosystem are RSA cryptosystem (1978), Elgamal's cryptosystem (1985) and Paillier's cryptosystem (1999).

Two or more agents want to conduct a computation based on their private inputs but neither of them wants to share its proprietary data set to other. The objective of *secure multiparty computation* (SMC) is to compute with each party's private input such that in the end only the output is known and the private inputs are not disclosed except those which can be logically or mathematically derived from the output [8]. Traditionally, the properties of SMC protocol are evaluated in terms of privacy, correctness, independence of inputs, guaranteed output delivery and fairness. SMC ensures *correctness* if each party receives correct output. Corrupted (or malicious) parties select their inputs independently of the inputs of honest parties and honest parties must receive their output. Corrupted parties should receive their outputs if and only if the honest parties receive their outputs and this ensures *fairness* of SMC. In the study of SMC problems, two models are commonly assumed : *semi-honest* model and *malicious* model. A semi-honest party follows the protocol properly with correct input. But after the execution of the protocol, it is free to use all its intermediate computations to compromise privacy. A malicious party does not need to follow the protocol properly with correct input; it can enter the protocol with an incorrect input. A third party may exist in a protocol. A trusted third party is given all data; it performs the computation and delivers the result. In some SMC protocols, an untrusted third party is used to improve efficiency. A protocol 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. Secure multi-party computation preserves privacy of data in different ways such as adding random noise to data, splitting a message into multiple parts randomly and sending each part to a DMA through a number of parties hiding the identity of the source, controlling the sequence of passing selected messages from an agent to others through serial or parallel mode of communication, dynamically modifying the sequence of events and agents through random selection and permuting the sequence of messages randomly. Another important technique is secure function evaluation. Alice with an input x and Bob with an input y want to evaluate a function z = f(x,y) based on their joint inputs in such a way that does not allow any party to gain more information than that is implied by its inputs and the function value. Alice and Bob can achieve this through *secure function evaluation.*

Traditionally, cryptographic solutions are focused to ensure information security and privacy. But there are other different types of cryptographic concerns since the security intelligence is evaluated in terms of fairness, correctness, transparency, accountability, confidentiality and trust. A communication protocol ensures correctness if the sending agent broadcasts correct data free from any false data injection attack and each recipient receives 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 on payment function, trust and quality of service. Fairness ensures that something will or will not occur infinitely often under certain conditions. The recipients expect fairness in private communication according to their demands plan, objectives and constraints. The sending agent expects fairness from the recipients in terms of true feedback and commitment on confidentiality of data. The mechanism must ensure the accountability and responsibility of the agents in access control, data integrity and non-repudiation. In fact, accountability is also associated with collective intelligence. The transparency of the mechanism is associated with communication protocols, revelation principle and automated system verification procedures. For example, a mechanism should clearly state its goal to define a policy. The performance of the system and quality of service is expected to be consistent and reliable. 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 AIS can return to normal performance level following a disruption. Real-time security management involves high cost of computation and communication. The vulnerability of AIS to a disruptive event should be viewed as a combination of likelihood of a disruption and its potential severity. The AIS administrator must do two critical tasks: assess risks and mitigate the assessed risks. To assess risks, the system administrator should explore basic security intelligence: 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? An AIS 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.

Theorem 3 : The computational intelligence is associated with the cost of verification algorithms of system immunity and the complexity of threat analytics.



System immunity

Exploratory module : locate errors

Fault tree: Cause-effect analysis

Diagnostics tool: program model checking

Real-time system verification

Natural verification

Automated verification

System dynamics analytics

Threat analytics : Danger signal

Inference engine: Reasoning algorithms

Knowledge base

Figure 1 : Computational Intelligence of AIM

The verification system requires both automated and semi-automated verification options. The verification system calls threat analytics and a set of model checking algorithms for various phases : exploratory phase for locating errors, fault finding phase through cause effect analysis, diagnostics tool for program model checking and real-time system verification. Model checking is basically the process of automated verification of the properties of the system under consideration. Given a formal model of a system and property specification in some form of computational logic, the task is to validate whether or not the specification is satisfied in the model. If not, the model checker returns a counter example for the system's flawed behavior to support the debugging of the system. Another important aspect is to check whether or not a knowledge based system is consistent or contains anomalies through a set of diagnostics tools.

There are two different phases : explanatory phase to locate errors and fault finding phase to look for short error trails. Model checking is an efficient verification technique for communication protocol validation, embedded system, software programmers', workflow analysis and schedule check. The basic objective of the model checking algorithm is to locate errors in a system efficiently. If an error is found, the model checker produces a counter example how the errors occur for debugging of the system. A counter example may be the execution of the system i.e. a path or tree. A model checker is expected to find out error states efficiently and produce a simple counterexample. There are two primary approaches of model checking: symbolic and explicit state. Symbolic model checking applies a symbolic representation of the state set for property validation. Explicit state approach searches the global state of a system by a transition function. The efficiency of model checking algorithms is measured in terms of automation and error reporting capabilities. The computational intelligence is also associated with the complexity of threat analytics equipped with the features of data visualization and performance measurement.

The computational intelligence may be associated with four decisions depending on the type of an application (e.g. intrusion detection): encoding, similarity measure, selection and mutation. Antigens and antibodies are encoded in the same way. An antigen is the target or solution. The antibodies are the remainder of the data. After the fixing of efficient encoding and suitable similarity measure, the algorithm performs selection and mutation both based on similarity measure until stopping criteria are met. The threat analytics analyze system performance, sensitivity, trends, exception and alerts along two dimensions: time and insights. The analysis on time dimension may be as follows: what is corrupted or compromised in the system: agents, communication schema, data schema, application schema, computing schema and protocol? what occurred? what is occuring? what will occur? Assess probability of occurrence and impact. The analysis on insights may be as follows : how and why did the threat occur? What is the output of cause-effect analysis? The analytics also recommends what is the next best action? It predicts what is the best or worst that can happen?

4. Experimental Results

The research methodology adopted in the present work includes intelligent reasoning, threat analytics and review of relevant literature. The mechanism (AIM) is applied on three test cases: (application 1) intrusion detection for IT security, (application 2) adaptively secure broadcast and (application 3) health security.

4.1 Test case 1: Intrusion Detection

The problem : An intrusion is considered as an activity that violates the security policy of a system. Intrusion detection systems are based on the assumption that the behavior of an intruder is different from that of an authorized user and the unauthorized activities can be detected by analyzing user's profile and activities, host based IDs, network based IDs and application based IDs. Auditing is required at different levels of granularity for the detection of misuse and anomaly. An intruder tries to gain access to an unauthorized system to which it has no legitimate access. It occurs by exploiting system vulnerabilities or by simply cracking the user_ids and passwords of legitimate users. If a malicious agent is able to access the system, it is considered as an authorized user and is granted the access rights of the user. The basic objective is to effectively detect and prevent insider misuse.

Solution* : *[AIM - ID]

###

***System** : Distributed computer / broadcasting / sensor / SCADA network;*

Agents : Detective, cryptographic objects;

***Moves** :*

- *Multidimensional view of intelligent reasoning* {logical, analytical, case based, forward and backward chaining, probabilistic, predictive, perception based approximation reasoning};
- Define system immunity (i') combinatorially: i' = f(a',b',c',d',e'); a': collective intelligence, b': machine intelligence; c': security intelligence; d': collaborative intelligence; e': business intelligence;
- *Private search* for evidence in breadth and depth;
- The cryptographic objects are involved in private communication using signcryption algorithms.

Input : A self-set $S \subseteq U$, a monitoring set $M \subseteq U$ for a given system parameters;

***Output**: f*or each element $m \in M$, either self or non-self;

```
D ← set of detectors that do not match any s ∈ S.
for each m ∈ M do
{
    call threat analytics (A') → sense danger signal;
    secure function evaluation → verify innate and adaptive system immunity i' = f(a',b',c',d',e');
}
sense-challenge-respond to system immunity resiliently;
if m matches any detector d ∈ D then identify m as non-self else identify m as self;
check if non-self or suspicious node is benign or malign danger node; if it is malign then suppress it else give alert.
```

###

Intrusion may occur in various forms on a distributed network such as sybil, cloning or node replication, wormhole denial of service, key interception and node capture. Traditional intrusion detection techniques may not be able to sense danger signal or perform negative or clonal selection due to non-availability of intelligent threat analytics and ill-defined system immunity. Possible functionalities, constraints like computational and communication complexities and systematic features influence the perception of security and trust of a distributed network. For example, the computational power, memory capacity and energy limitations enforce slightly different approaches to the problems of security and privacy in sensor networks. In an open environment, sensor nodes operate without any supervision; a malicious attacker can capture a node for reconfiguration or extract the private data stored in the node through cryptanalysis. An attacker may be able to deploy multiple physical nodes with same identity through cloning or node replication attack. An adversary may be able to deploy multiple identities of a node to affect the trust and reputation of the system through Sybil attack. The attacker may be able to build an additional communication channel to capture private communication through wormhole attack. A key can be compromised either by physical extraction from a captured node or by breach in SMC protocol. The denial of service attack renders a node by overloading it with unnecessary operations and communication and may be able to make the whole network inoperable. Coremelt attacks can target communication links blocking the exchange of useful information. Replay attacks allows an attacker to record messages at one instance and replay it later at different locations.

There are possibilities of blackhole, jellyfish, neighbor and rushing attacks. A blackhole attacking agent tries to intercept data packets of the multicast session and then drops some or all data packets it receives instead of forwarding the same to the next node of the routing path and results very low packet delivery ratio. A jellyfish attacker intrudes into the multicast forwarding group and delays data packets unnecessarily and results high end-to-end delay and degrades the performance of real-time application. A neighborhood attacking agent forwards a packet without recording its ID in the packet resulting a disrupted route where two nodes believe that they are neighbors though actually they are not. Rushing attack exploits duplicate suppression mechanisms by forwarding route discovery packets very fast.

AIM-ID explores the concept of next generation Intrusion Detection System (IDS) based on bio-inspired artificial intelligence and immunological theories. The critical challenge of information security is to determine the difference between normal and malicious activities. Traditionally, a distributed system is protected by access control policy that blocks malicious events. Actually, it should be protected by artificial immune systems through automated and adaptive verification mechanisms based on negative selection i.e. self / non-self discrimination, clonal selection and danger signal detection. Different strategic moves are useful for different situations.

A distributed network consists of a set of entities, a broadcast communication cloud and a set of pipes connecting the entities to the communication cloud. The entities can be partitioned into two subsets: correct and faulty. Each correct entity presents one legitimate identity to other entities of the distributed system. Each faulty entity presents one legitimate identity and one or more counterfeit identities to the other entities. Each identity is an informational abstract representation of an entity that persists across multiple communication events. The entities communicate with each other through messages. A malicious agent may control multiple pseudonymous identities and can manipulate, disrupt or corrupt a distributed computing application that relies on redundancy. This is known as sybil attack [28]. Sybil attacks may affect fair resource allocation, routing mechanisms, voting, aggregation and storage of distributed data by injecting false data or suppressing critical data. A large-scale distributed system is highly vulnerable to Sybil attack; it includes sensor and mobile ad hoc networks, p2p applications and DCS network.

The basic objective of AIM–ID to monitor the actions of the users on distributed network and detect the occurrence of any intrusion. Here the challenge is how to perform negative selection, clonal selection and danger signal detection. Auditing is primarily required to validate the security policies and to review the observed behaviors of distributed applications, users and database. User profiling monitors and analyzes the activities of the users. Data profiling analyzes the managed data. In case of anomaly detection, the data of repetitive and usual behavior of the users is collected and suitably represented as normal profiles. The profile and the activities of the current user is compared with the normal profile. If there is significant mismatch, it indicates an intrusion in the network. It is useful for unknown attack. Misuse detection is useful for known attack.

AIM-ID follows a set of moves to detect the risk of intrusion:

- *multi-dimensional view of intelligent reasoning* {logical, analytical, case based, forward and backward chaining, probabilistic, predictive, perception based approximation reasoning} for system monitoring;
- define system immunity (i) combinatorially: i = f(a',b',c',d',e'); a': collective intelligence, b': machine intelligence; c': security intelligence; d': collaborative intelligence; e': business intelligence;
- *assess system immunity* (S_i) through a hybrid approach in terms of negative selection, danger signal detection, clonal selection and suppression*;*
- *verify collective intelligence in terms of* policy, scope, input, output, process, agents, location and system dynamics;
- define *collaborative intelligence* (revelation principle);
- *evaluate business intelligence in terms of* payment function and incentive;
- *monitor machine intelligence* in terms of safety, liveness, concurrency, reachability, deadlock freeness, scalability and accuracy. For an information system, it should check preconditions, post conditions, triggering events, main flow, sub flow, alternate flow, exception flow, computational intelligence, communication cost, traffic congestion, time and space complexity, resources, capacity utilization, load, initial and goal states, local and global states, state transition plans*;*
- *check security intelligence in terms of* safety, authentication, authorization, correct identification, non-repudiation, integrity, audit and group, forward and backward privacy; rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, reliability, consistency, commitment).
  - Recognize pattern of intrusion attack like sybil, cloning or node replication, wormhole and node capture;
  - Sense possibilities and impact of secondary threats such as coremelt, blackhole, jellyfish, rushing, neighbor, replay and shilling attacks;
  - Select single or multiple approaches from trusted explicit and implicit certification, robust authentication checking of e-passport, resource testing, auction and incentive based sybil detection game;
  - Verify efficiency of cryptographic signcryption algorithms for private communication.

There are various approaches of sybil detection: trusted explicit and implicit certification, robust authentication protocol, resource testing, auction and incentive based sybil detection game [29,30]. In case of trusted certification, a centralized authority assigns a unique identity to each entity. The centralized authority can verify computing, storage and bandwidth capability of the entities on periodic basis. A local identity (l) accepts the identity (i) of an entity (e) if e presents i successfully to l. An entity may validate the identity of another identity through a trusted agency or other entities or by itself directly. In the absence of a trusted authority, an entity may directly validate the identities of other entities or it may accept identities vouched by other accepted entities. The system must ensure that distinct identities refer to distinct entities. An entity can validate the identity of other entities directly through the verification of communication, storage and computation capabilities. In case of indirect identity validation, an entity may validate a set of identities which have been verified by a sufficient count of other identities that it has already accepted. But, a group of faulty entities can vouch for Sybil identities. AIM-ID tries to detect intrusion through Sybil attack based on multi-dimensional view of reasoning and therefore it is more efficient than other approaches as said above.

A *wormhole* attacker records packets at one point in adhoc wireless communication network, tunnels the packets possibly selectively to another point and retransmits them there into the network. The attacker may not compromise any hosts and even if all communication protocols provide authenticity and confidentiality correctly. *Packet leashes* may be used for detecting and defending against wormhole attacks. A leash is any information that is attached with a packet to restrict its maximum allowed transmission distance. A geographical leash ensures that the recipient of the packet is within a certain distance from the sending agent. A temporal leash ensures that the packet has an upper bound on its lifetime which restricts the maximum travel distance.

Sensor node attestation verification is an intelligent move to detect intrusion: check if a sensor node is tampered by an adversary; check the configuration and correct setting of each sensor node; detect whether malicious software is loaded into sensor nodes; verify the integrity of the code; perform secure code updates and ensure untampered execution of code. Each node should be attested with a valid digital test certificate. The verification algorithm must verify the identity and tampering status of each node. The basic objective of device attestation is that a malicious agent should not be able to configure or change correct setting of each node. A challenge response protocol is employed between a trusted external verifier and a sensor node.

Each sensor node should be is provided with an 'e-passport' which should have unique identification features like biometric traits. It is an open issue of research: can a sensor node be equipped with traits like unique biometric features of a human being (e.g. voice, fingerprints, retina, vein patterns and facial dimensions)? An e-passport should have unique passport identification number, time stamp (or date of birth), erection testing and commissioning history, location, digital signature of issuing authority and neighborhood data. It is essential to check the authenticity of e-passport data of each sensor node periodically or for specific suspicious cases to detect intrusion. A single move may not be sufficient to detect intrusion.

4.2 Test case 2: Adaptively Secure Broadcast

This test case presents an Adaptively Secure Broadcast Mechanism (AIM-ASB) based on threats analytics. It defines the security intelligence of a broadcast system comprehensively with a novel concept of collective intelligence. The basic objective of ASBM is to improve the quality of broadcast through fundamental rethinking and radical redesign of a reliable communication schema. ASBM is based on following *assumptions:* (a) Broadcast communication must satisfy the basic requirements of security and privacy from the perspectives of collective intelligence of a rich knowledge base. (b) The analytics must explore the risk of all possible threats on a broadcasting system. (c) Another critical issue is low computation and communication overhead for security intelligence. (d) The broadcasting system must support scalability and reliability. The sender tries to distribute real-time data reliably through a private communication channel, the recipients validate and use the received data as it arrives. Reliability detects missing or corrupted data.

Adaptively Secure Broadcast Mechanism (AIM-ASB)

```
####################################################################
Agents: {S, $R_{i;i=1,..,n}$, A}; or {S, $R_{i;i=1,..,n}$};
Network Topology: Dynamic or Fixed network;
Communication model: 1-n or m-n or 1-n-p or m-n-p;
Moves :
        • Multidimensional view of intelligent reasoning {logical, analytical, case based, forward and backward
          chaining, probabilistic, predictive, perception based approximation reasoning};
        • Define system immunity (i'') combinatorially: i'' = f(a'',b'',c'',d'',e''); a'': collective intelligence, b'': machine
          intelligence; c'': security intelligence; d'': collaborative intelligence; e'': business intelligence;
Input: Data stream $D_{j;\, j=1,..,x}$ or secret (D);
Negotiation protocol:
R → S : $P_d$ [d, b];
R ↔ S : [$P_b$, $p_f$];
    objectives: minimize $t_r$, minimize n′, minimize T, maximize r subject to
    constraints: time deadline : $t \le t_d$, budget : $b \le b_{max}$, profit margin : $m_{min} \le m' \le m_{max}$ ;
    strategies : select single or multiple strategies of communication from a list of options (FIFO, LIFO, priority queue,
    load consolidation, data filtering, unidirectional, bidirectional, synchronous, asynchronous, single round, multiple
    rounds communication);
    payment function: commit on ($P_b$, $p_f$) through multi-party negotiation or swing option;
Cryptographic security set up:
        Sender's set up : S generates, refreshes adaptively and distributes keys to R for private broadcast through
        (encryption and decryption) or digital signature or (signcryption and unsigncryption) or privacy preserving data
        mining (ppdm : randomization, summarization, aggregation, generalization, suppression, de-identification and k-
        anonymity);
        Receiver's set up : The recipients acknowledge S after the receipt of authentication keys;
        S → $R_{i;i=1,..,n}$ : broadcasts encrypted data D′ = { $D_{;j=1,..k}$}$_{ke}$ or non-encrypted data D or perception of signal by R
        from S without using any channel;
        $R_{i;i=1,..,n}$ : decrypts or unsigncrypts data. {D′}$_{kd}$ or receives D.
        call threat analytics (A'') → verify innate and adaptive system immunity (i'') in terms of colletive intelligence (a''),
        machine intelligence (b''), security intelligence (c''), collaborative intelligence (d'') and business intelligence (e'');
            ♦ assess risks of single or multiple attacks on broadcasting system; analyze performance, sensitivity,
              trends, exception and alerts.
            ♦ what is corrupted or compromised: agents, communication schema, data schema, application schema,
              computing schema and broadcast mechanism?
            ♦ time series analysis : what occurred? what is occuring? what will occur? assess probability of occurrence
              and impact.
            ♦ 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?
The honest agents compute penalty function and charge the corrupted agents.
Output: Broadcasting system immunity;
##################################################################
```

In the existing works of adaptively secure broadcast, broadcast corruption is not assessed properly. The issues of broadcast corruption have been defined imprecisely and incompletely through statistical reasoning. A broadcast protocol allows a sender to distribute a secret through a point-to-point network to a set of recipients such that (i) all recipients get the same data even if the sender is corrupted and (ii) it is the sender's data if it is honest. Broadcast protocols satisfying these properties are known to exist if and only if $t < n/3$, where n denotes the total number of parties, and t denotes the maximal number of corruptions. When a setup allowing signatures is available to the parties, then such protocols exist even for $t < n$. It is not rational to state the bound of adaptively secure broadcast protocol in a simple straight forward way. Adaptively secure broadcast mechanism (ASBM) results correct and fair output if and only if all the agents (sending agent, receiving agents and broadcast system administrator), communication channel, broadcast mechanism, broadcast data, payment function and payment mechanism are free of corruption [31]; this work also shows the complexity analysis through a set of examples. The security intelligence is verified in terms of authentication, authorization, correct identification, privacy: group, forward and backward, audit; fairness, correctness, transparency, accountability, confidentiality, trust, integrity, non-repudiation, commitment, reliability, consistency; liveness, deadlock freeness, lack of synchronization, safety and reachability. It also assesses and mitigates the risks of false data injection, sybil, node replication, wormhole, blackhole, jellyfish, rushing, neighbor, coremelt, node deletion, flaws in broadcast schedule, poor QoS, malicious business intelligence, corruption in secret sharing, information leakage, replay and shilling attack on a broadcasting system.

4.3 Test Case 3 : Health security

The problem : The World Health Organization (WHO) is expected to redefine and implement global healthcare policy for improved immunity :" Healthcare for all at reasonable cost and optimal quality of service maintaining rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, reliability, consistency, commitment, safety, liveness, synchronization, reachability, deadlock freeness; authentication, authorization, correct identification, privacy, non-repudiation, integrity and audit through collaborative and collective intelligence". How to code the program?

AIM - GHS

```
####################################################################
```

System : Biological system of human agents; life-science supply chain, healthcare service chain;
Agents : Patients, healthcare consultants, service staffs;
Moves :

- *Multidimensional view of intelligent reasoning* {common sense, logical, analytical, case based, forward and backward chaining, sequential, parallel, uncertainty, probabilistic, approximation, predictive, imaginative, perception};
- *Define system immunity* (S_i) in terms of innate or natural immunity and adaptive immunity (humoral and cell mediated); sense negative selection, danger signal detection, clonal selection, somatic hypermutation and suppression;
- *Private search* for evidence in breadth and depth;
- The cryptographic objects and agents are involved in private communication using signcryption algorithms.

```
Input : A self-set $S \subseteq U$, a monitoring set $M \subseteq U$ for a given system parameters;
Output: for each element $m \in M$, either self or non-self / danger or normal;
$D \leftarrow$ set of detectors that do not match any $s \in S$.
for each $m \in M$ do
{
    call threat analytics ($A'''$) → sense danger signal;
    secure function evaluation → verify innate and adaptive system immunity $i''' = f(a''',b''',c''',d''',e''')$;
}
sense-challenge-respond to system immunity resiliently;
if $m$ matches any detector $d \in D$ then identify m as non-self;
else identify m as self;
check if non-self or suspicious element is benign or malign danger;
if it is malign then suppress it else give alert.
####################################################################
```

What is bio-terrorism? This is a question of life and death in human society globally. Traditionally, it is the intentional use of biological or chemical agents to cause disease or destroy food and water supplies or capture and kill human agents for political or economic reasons to achieve malicious business intelligence. Today, it is difficult to classify the illnesses caused by biological, chemical and radiological weapons from naturally occurring ailments. Our society is going through an excellent progress of life-science supply chain management and healthcare service and medical practice. But, there is threat of bio-terrorism on the soft targets such as life-science supply chain and healthcare service chain. It is basically a management game in today's business world. It is generally related to the use of biological, chemical and radiological weapons in the battle fields. Most surprisingly, the definition of bio-terrorism has been changed from the use of bullets and explosives towards slow poisoning of the innocent public through innovation of new viruses, anti-viruses, drugs and toxic tasty junk food, soft drinks and beverages, flawed digital bio-medical instrumentation and unethical medical practice. It is a silent trap of death. The conflicts between security intelligence and business intelligence are inevitable. Today's healthcare system must satisfy the basic requirements of security and safety for the benefits of the common people of the world. The analytics must explore the risk of all possible threats on the soft targets. Our society needs rational decision support system, microsoft healthcare policy and innovative medical practice to resist bio-terrorism. Is it a mission impossible? AIM-GHS mechanism follows a set of intelligent moves to evaluate the immunity of a biological system.

Move 1 : *Multidimensional view of intelligent reasoning based on rational selection of single or multiple techniques from the list of* logical, analytical, case based, forward and backward chaining, sequential, parallel, uncertainty, probabilistic, approximation, predictive, imaginative and perception based reasoning. AI reasoning is a consortium of methodologies that works synergistically and provides flexible information processing capability for handling ambiguous situations in healthcare domain. The basic objective is to exploit the tolerance for imprecision, uncertainty, approximate reasoning, and partial truth in tractable, robust and low cost solutions. Let us review the scope of these reasoning techniques to ensure health security.

Move 2 : Define system immunity (S_i) in terms of innate or natural immunity and adaptive immunity (humoral and cell mediated); sense negative selection, danger signal detection, clonal selection, somatic hypermutation and suppression.

Move 3 : *Define collective intelligence* (a''') in terms of system dynamics (scope, input, output, feedback, process, agents and system dynamic), local and global healthcare policy, immunization programmes, benchmarked and standardized medical practice and education, common sense healthcare and hygiene (system control, self confidence: how to manage self? self assessment and monitoring, family planning), resource planning, efficiency of life-science supply chain and healthcare service chain.

Move 4: *Define machine intelligence* (b''') in terms of (preconditions, post conditions, triggering events, main flow, sub flow, alternate flow, exception flow, computational intelligence, accuracy, communication cost, traffic congestion, time and space complexity, resources, capacity utilization, load, initial and goal states, local and global states) for bio-medical instrumentation and digital transformation, artificial organ transplantation (brain, heart, blood, neural system, stomach, liver, kidney, pancreas, limbs, bone marrows), wearable computing, pervasive computing and biosensors, nano-medicine and surgical robotics.

Move 5 **:** *Define collaborative intelligence* (d''') and assess its impact on the immunity of biological system in terms of information sharing principle, negotiation protocol and planning, intelligent broadcast protocol, organ donation and breast-milk feeding for childcare.

*Move 6***:** *Define business intelligence* (e''') and assess its impact on the immunity of biological system in terms of business rules, contractual clauses, incentive, payment function and competitive intelligence.

Move 7 : Define security intelligence (c''') of life-science supply chain and healthcare service chain and assess its impact on the immunity of biological system in terms of rationality, fairness (honesty, ethics), 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; assess the impact on immunity by social security (poverty, malnutrition, physical and mental stress, erosion of social values), bio-terrorism, artificial organ transplantation, artificial reproduction, climate change, natural disaster and environmental pollution.

Move 8: Use new cryptographic solutions (besides encryption, digital signature and signcryption) to ensure privacy, fairness and correctness in multi-party computation.

Critical observation : A biological system ensures optimal level of immunity by balancing natural and artificial intelligence based on intelligent reasoning. A human agent must have common sense healthcare knowledge base for proper biological system control through intelligent self-assessment and self-confidence i.e. how to manage self against non-self. It demands the necessity of learning the basic concept of 'immune system' through artificial intelligence. It is possible to redefine global healthcare policy based on AIM-GHS mechanism. [32] shows the complexity analysis of this mechanism, the conflict between business intelligence and security intelligence and related cryptographic challenges.

5. Conclusion

This work finds a set of interesting research agenda for future work: (a) explore new cryptographic concerns using game theoretic concepts and intelligent reasoning; (b) how to design an intelligent threat analytics; (c) how to design automated verification algorithms; (d) how to rationalize SMC protocols and (e) how to quantify and code miscellaneous security intelligence parameters? Artificial intelligence (AI) is basically simulation of human intelligence. Recently, there are debates on AI. Today's world needs to be super careful with AI because it is potentially more dangerous than nukes [33]. Is it really true or an instance of rational reasoning? An intelligent reasoning system demands new data structure beyond knowledge base with envision, 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 [19]. A rational reasoning system needs the support of an intelligent analytics. We need a new outlook, imagination and dream to solve a complex problem through a set of simple mechanisms.

References

1. Y. Dodis, S. Halevi and T. Rabin. 2000. A Cryptographic Solution to a Game Theoretic Problem. In CRYPTO'00, Springer-Verlag (LNCS 1880), pages 112- 130.
2. Y. Dodis and T. Rabin. 2007. Cryptography and Game Theory. In Algorithmic Game Theory. Cambridge University Press.
3. N. Nisan and A.Ronen. 1999. Algorithmic mechanism design. In 31st Annual ACM symposium on Theory of Computing (STOC), pp 129 -140.
4. G.Asharov, R.Cannetti and C.Hazay. 2014. Towards a game theoretic view of secure multiparty computation. Eurocrypt.
5. J. Katz. 2008. Bridging Game Theory and Cryptography: Recent Results and Future Directions. In 5th TCC, Springer-Verlag (LNCS 4948), pages 251-272.
6. G. Kol and M. Naor. 2008. Games for exchanging information. In 40th STOC, pages 423-432.
7. G. Kol and M. Naor. 2008. Cryptography and Game Theory: Designing Protocols for Exchanging Information. In 5th TCC, Springer-Verlag (LNCS 4948), pages 320-339.
8. Y. Lindell. 2003. Composition of secure multi-party protocols a comprehensive study. Springer.
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. D. Dasgupta (ed). 1999. Artificial Immune Systems and Their Applications. Springer.
11. D.Dasgupta and F.Gonzalez. 2002. An immunity-based technique to characterize intrusions in computer networks. IEEE Trans Evol Comput 6:1081–1088.
12. J.D.Farmer, N.H. Packard and A.S. Perelson. 1986. The immune system, adaptation, and machine learning. Physica 22:187–204.
13. E.Hart and J.Timmis. 2008. Application areas of AIS: the past, the present and the future. Appl Soft Comput 8:191–201.
14. S.Forrest, A.S. Perelson, L. Allen and R. Cherukuri. 1994. Self–nonself discrimination in a computer. In: Proceedings of the IEEE symposium on research in security and privacy, Oakland, CA, USA, pp 202–212.
15. S. Hofmeyr and S. Forrest. 2000. Architecture for an artificial immune system. Evol Comput 7:1289–1296.
16. E.Rich and K. Knight. 1991. Artificial intelligence, 2nd edn. McGraw-Hill, New York
17. G.Luger. 2005. Artificial intelligence: structures and strategies for complex problem solving, 5th edn. Addison-Wesley, New York.
18. A.Cawsey. 1998. The essence of artificial intelligence. Prentice-Hall, Englewood Cliffs.
19. D. Perlis. 2016. Five dimensions of reasoning in the wild. AAAI.
20. S. J. Russell and E. H. Wefalld. 1991. Do the Right Thing: Studies in Limited Rationality. MIT Press.
21. A. Konar. 1999. Artificial Intelligence and Soft Computing. CRC Press.
22. J.Kim, P.Bentley, U.Aickelin, J.Greensmith, G.Tedesco and J.Twycross. 2007. Immune system approaches to intrusion detection - a review. Nat Comput 6:413–466.
23. P.Matzinger. 1994. Tolerance, danger and the extended family. Ann Rev Immunol12:991–1045.
24. P.Matzinger. 2001. The danger model in its historical context. Scand J Immunol 54:4–9.
25. P.Matzinger. 2002. The danger model: a renewed sense of self, Science 296:301–305.
26. L. Castro and C.J.Timmis. 2002. Artificial Immune Systems : A New Computational Intelligence Approach. Springer.
27. Tarakanov et. al. 2003. Immunocomputing : Principles and applications. Springer.
28. J.Douceur. 2002. The sybil attack. Proceedings of Workshop on P2P systems (IPTPS).
29. A.K.Pal, D. Nath and S.Chakraborty. 2010. A Discriminatory Rewarding Mechanism for Sybil Detection with Applications to Tor. WASET, Brazil.
30. N.B. Margolin and B.N. Levine. 2007. Informant: Detecting Sybils Using Incentives. In Proceedings of Financial Cryptography'07.
31. S. Chakraborty. 2014. Security intelligence for broadcast: threat analytics. Technical report. Crypto E-print archive, 2015/332.
32. S.Chakraborty. Secure multi-party computation: how to solve the conflict between security and business intelligence. Technical report. Crypto E-print Archive, 2015/804.
33. N.Bostrum. 2014. Superintelligence : Path, dangers, strategies. Oxford University Press.