SECURE MULTI-PARTY COMPUTATION: HOW TO SOLVE THE CONFLICT BETWEEN SECURITY & BUSINESS INTELLIGENCE

Sumit Chakraborty
Fellow, Indian Institute of Management Calcutta; Bachelor of Electrical Engineering, Jadavpur University, India;
E-mail: schakraborty2010@hotmail.com, surya20046@yahoo.co.in

Abstract: This work defines the security intelligence of a system based on secure multiparty computation in terms of correctness, fairness, trust, transparency, accountability, reliability, consistency, confidentiality, data integrity, non-repudiation, authentication, authorization, correct identification, privacy, safety and audit. It defines the security intelligence of a system comprehensively with a novel concept of collective intelligence. The cryptographic notion of security is applied to assess, analyze and mitigate the risks of bio-terrorism today. This work also tries to resolve the conflict between the security intelligence and business intelligence in the context of bio-terrorism and highlights the new cryptographic challenges.

Keywords: Secure multi-party computation, Security intelligence, Threat analytics, Business intelligence, Cross border bio-terrorism

1. SECURE MULTI-PARTY COMPUTATION

Game theory and cryptography are effectively used to understand the strategic moves of intelligent agents having conflicting interests [1]. But, the focus of the two disciplines have different set of goals and formalisms. Traditionally, the basic objective of cryptography is to design secure multiparty computation protocols satisfying the basic properties of information security and privacy. On the other side, algorithmic game theory is applicable to design intelligent mechanisms in terms of a set of rational agents, input, output, strategic moves, revelation principle, payment function, incentive, rules of interaction and multi-party negotiation. Traditionally, game theory is applied in management science to define business intelligence. Cryptographic techniques such as secure multi-party computation have been effectively used to solve not only game theoretic problems but also to resolve the conflict between security intelligence and business intelligence of a complex system. Game theoretic concepts are also effectively used in secure and fair computation through rational secret sharing.

Let us first focus on the basic properties of secure multi-party computation (SMC). 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 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 [2]. In case of secure multi-party computation, a single building block may not be sufficient to do a task; a series of steps should be executed to solve the given problem. Such a well-defined series of steps is called a SMC protocol. 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 SMC protocol is expected to satisfy a set of essential properties such as privacy, correctness, independence of inputs, guaranteed output delivery and fairness [3]. A protocol 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 the protocol. 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 an agent 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 [4].

The contribution of the present work is as follows. It defines the properties of secure multi-party computation from broader perspectives and in terms of collective intelligence. It adds a set of useful properties to the existing definition of secure multi-party computation. It is important to define and verify the security intelligence of a mechanism in a complex system precisely and comprehensively. This novel concept of secure multi-party computation has been applied to resolve the conflict between the security intelligence and business intelligence for mitigating the risk of bio-terrorism today. The review of existing literature could not find out efficient mechanisms to counter bio-terrorism from the perspectives of security intelligence and business intelligence. The security intelligence has been defined weakly, incompletely and imprecisely. The system lacks intelligent model checking or system verification mechanisms based on rational threat analytics.

The research methodology adopted in the present work includes case based reasoning, threat analytics and review of relevant literature on cryptography, secure multi-party computation and bio-terrorism. The logic of the bio-terrorism mechanism is

explored through hypothetical case based reasoning on healthcare service chain, life-science supply chain, bio-technology and medical practice. The security intelligence is explored through threats analytics on malicious business intelligence. The model checking algorithm assesses the risks of various malicious attacks and relevant risk mitigation plans.

The work is organized as follows. Section 1 starts with introduction which defines the problem and properties of secure multi-party computation. It reviews existing literature and analyzes the gaps, states research methodology and contributions of the work. Section 2 highlights modern bio-terrorism mechanism. Section 3 is focused on threat analytics. Section 4 discusses the cryptographic challenges of secure multi-party computation to resolve the conflict between security intelligence and business intelligence.

2. BIO-TERRORISM MECHANISM

What is bio-terrorism? This is a question of life and death in human society. Traditionally, it is the intentional use of biological or chemical agents to cause disease or destroy food and water supplies for political or economic reasons to achieve malicious business intelligence [5]. Today, it is difficult to classify the illnesses caused by biological, chemical and radiological weapons from naturally occurring ailments. Today, 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 including life-science supply chain and healthcare service chain. Bio-terrorism is basically a management game in today's business world. Traditionally, bio-terrorism deals with use of biological, chemical and radiological weapons in the battle fields. Most surprisingly, the definition of 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 and also flawed digital bio-medical instrumentation. 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? The following section first outlines the intelligence of bio-terrorism mechanism from the perspectives of security.

Agents: Service provider (P), Service consumer (C), partners of life-science supply chain, Adversaries;

Input: Data on agents, healthcare products and services;

Targets: Life-science supply chain, Healthcare service chain;

Life-science supply chain : SCOR, DCOR, CCOR;

SCOR : Planning - demand, inventory, production and capacity, packaging and labeling, MRP; Collaboration and sourcing; Execution - sales and distribution, order management, warehouse management, transportation management, reverse logistics; *DCOR* : innovation, product life-cycle management, pricing; *CCOR* : customer relationship management;

Healthcare service chain: registration, consulting, testing, surgical operations, billing, payment processing and follow-up;

Threats: call threat analytics and assess risks;

- Management Information System (MIS) corruption
  - False data injection attack
  - Sybil attack
  - Private data leakage
  - Flawed web security
  - Flawed knowledge management system for creation, storage, transfer and application
- Broadcast corruption through shilling attack
- Technical snags, unreliability and inconsistency in digital bio-medical instrumentation
- Biotechnology based innovation of new germs, viruses and anti-viruses
- Life-science supply chain corruption
- Poor quality of service in healthcare service chain
  - Transaction processing system
  - Decision support system and GDSS
  - Business intelligence system
    - Malicious data mining
    - Insecure data storage
    - False data visualization
    - Poor performance measurement
- Malicious business intelligence
  - Greedy heuristics in payment function for revenue and profit optimization
  - Economic pressure and incentive policy
  - Fraudulent health insurance model
  - Investment for technology management
- Irrational and dull HR policy in talent management
- Chaotics in formulation of public policy, mechanisms, regulatory compliance and corporate governance

Security intelligence verification: safety, authentication, authorization, correct identification, privacy, audit, fairness, correctness, transparency, trust, reliability, consistency, accountability, confidentiality, integrity and non-repudiation;

Strategic moves for risk mitigation: '10S' elements - System, Security, Strategy, Structure, Staff, Skill, Style - governance and regulatory compliance, Shared vision, Service and Social networking;

Output: Plan to counter bio-terrorism

3. THREAT ANALYTICS

Model checking is an automated technique for verifying a finite state concurrent system. Model checking has three steps: represent a system by automata, represent the property of a system by logic and design model checking algorithm. Model checking verifies specific set of properties of a system such as reachability, safety, liveness, deadlock freeness and fairness. In the context of bio-terrorism mechanism, the basic objective of verification or model checking algorithm is to mitigate the risk of various malicious threats intelligently

Theorem 1: The security intelligence is explored through threat analytics on bio-terrorism.

It is essential to verify the security intelligence of the target system (i.e. life-science supply chain and healthcare service chain) in terms of correctness, fairness, trust, transparency, accountability, reliability, consistency, confidentiality, data integrity, non-repudiation, authentication, authorization, correct

identification, privacy, safety and audit. It defines the security intelligence of the system comprehensively with a novel concept of collective intelligence.

In bio-terrorism mechanism, the soft target points of adversaries may be life-science supply chain and healthcare service chain. An intelligent analytics explore miscellaneous types of threats on the targets such as information system corruption through false data injection attack, sybil attack, private data leakage and knowledge management; broadcast corruption through shilling attack; technical snags, unreliability and inconsistency in the performance of digital bio-medical instrumentation; poor quality of service in registration, consulting, testing, surgical operation, billing and payment processing of healthcare service chain; flaws of transaction processing, decision support, group decision support and business intelligence system : malicious data mining in testing, insecure data storage, data visualization techniques and performance measurement; life-science supply chain corruption in planning, collaboration, execution, sales and distribution, product life-cycle management; malicious business intelligence in the modes of greedy heuristics in payment function for revenue and profit optimization, economic pressure and irrational incentive policy, fraudulent health insurance model and financial intelligence, incorrect decision on investment for technology management; biotech innovation of new jerms or viruses and anti-viruses and finally irrational and dull human resource management policy in talent management, reward and recognition. This list is not exhaustive. There are other several critical factors such as non-cooperative corporate culture, power play and politics, ethics, strategic blunder and chaotics in formulation of public policy, mechanisms and corporate governance. It is an open research agenda.

Bioterrorism mechanism explores different scenarios of corruption in terms of service provider, consultant, service consumer, life-science supply chain partners, system administrator and adversaries. The system results correct and fair output if all the agents, communication channel and data are free of corruption. Corruption may occur in various ways. The adversary is capable of corrupting an agent, input or output data. The corruption strategy indicates when and how parties are corrupted. In case of static corruption model, the adversary is given a fixed set of parties whom it controls. Honest parties remain honest throughout and corrupted parties remain corrupted. In case of adaptive corruption model, adaptive adversaries are given the capability of corrupting parties during the computation. The choice of who to corrupt, and when, can be arbitrarily decided by the adversary and may depend on its view of the execution. The basic objective of the threat analytics is to assess risks of different types of malicious attacks and explore risk mitigation plans accordingly.

The mechanism uses '10-S' model as a set of strategic moves of mitigating the risk of aforesaid threats: System, Security, Strategy, Structure, Staff, Skill, Style, Shared vision, Service and Social networking. It is a hard problem. It requires proper coordination and integration among ten elements associated with life-science supply chain and healthcare service chain. The basic objective is to ensure that different organizational elements of the healthcare service provider are appropriately synchronized and work in harmony to improve the quality of service. The hard elements are strategy, organizational structure and system. The soft elements are leadership style, resources, skill, security and shared values. The hard elements can be identified and defined in a relative simple way and directly controlled by corporate management. The soft elements are difficult to define, less tangible and influenced by corporate culture. The strategic fit among these factors is the basic building blocks of organizational effectiveness. A system acts rationally against bio-terrorism when these ten elements are aligned correctly and mutually reinforcing.

Theorem 2 : Technology management is a critical threat factor responsible for bioterrorism through corruption of management information system, corrupted communication schema, malicious bio-medical instrumentation and biotech innovation.

(Case-1.1: Biomedical instrumentation) This is the case of technical snags, unreliability and inconsistency in digital bio-medical instrumentation. Digital transformation requires the intelligence of biomedical engineering, bio-sensors, bio-inspired artificial intelligence and human computer interaction for improved QoS in patient care. A smart healthcare information system should be correctly integrated with bio-medical system appropriately through sensors, robotics, human computer interaction, mobile communication system and internet. An effective digital transformation enables the service provider to offer different innovative patient care services through medical imaging systems, digital radiography, computed tomography, nuclear medicine, computer-integrated interventional medicine, ultrasonic imaging, magnetic resonance imaging, diffuse optical imaging, image compression, medical image retrieval, parametric imaging, brain magnetic resonance imaging, molecular imaging, data processing and analysis by electronic medical record (EMR), image registration, biological computing, picture archiving, medical imaging informatics, digital library, integrated multimedia patient record systems, computer-aided diagnosis and clinical decision support systems. The patients or healthcare service consumers can receive innovative healthcare services such as mobile electrocardiogram (ECG) recording, portable defibrillators, digital X-ray, digital stethoscopes, digital pulse monitoring watches, blood pressure monitors, blood sugar monitors, pacemakers, pregnancy and urine test kits.

The most serious threat of digital biomedical instrumentation is inconsistent and unreliable malfunctioning of the devices and instruments due to intentional and planned attacks by the malicious agents. They may configure the devices incorrectly. There may be problems of regular and preventive maintenance of these devices. A maliciously configured or malfunctioning digital stethoscope or pulse watch may declare a live patient as dead. Attestation verification of biomedical devices is a critical requirement of a smart healthcare service chain as a part of regular and preventive maintenance: check if a device is tampered by an adversary; check the configuration and correct setting of each device; 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 device should be attested with a valid digital test certificate. The verification algorithm must verify the identity and tampering status of each device. The basic objective of device attestation is that a malicious agent should not be able to configure or change correct setting of a device. A challenge response protocol should be called between a trusted external verifier and a biomedical

instrument on periodic basis to check the reliability, consistency and correctness of the system. Bio-medical instruments must use efficient pattern recognition algorithms for patter recognition such as support vector machine for pattern classification, clustering and association rule mining.

(Case-1.2 : Biotechnology) This is the case of biotechnology based innovation of new germs or viruses and anti-viruses. New types of jerms are explored and injected into human body through different common channels such as natural disaster (e.g. rainfall, flood), environmental pollution (e.g. air, water, soil), water supply and pathological tests. It optimizes the revenue of drug companies through increased sale of anti-viruses. On the other side, it reduces the life-cycle of the patients or service consumers. It is basically a malicious management game. Cross-border medical terrorism is becoming a common occurrence in human society today; it may be across countries, inter-state, inter-district, inter-city and inter-villages. The migrants are often subjected to new drugs, medical treatment and surgical operation procedures for risky experiments in medical science. Many people are losing their life prematurely due to such terrorism. The experiment should be done on other animals through intelligent simulation game. The critical causal factor of such type of bio-terrorism is erosion of social values and quality of education at branded technical, medical and management institutes, R&D laboratories and mult-tiered life-science supply chain. The scientists innovate new medicine and biomedical instruments for the benefits of the human society; the business world often uses the innovation maliciously for greater sales, revenue and profit. It requires close watch, monitoring and audit of the activities of these institutes privately and continuously for the good of common people. Absolute autonomy in system administration and freedom of expression may result horrific disasters and chaotics in human society today.

(Case 1.3: False data injection attack). False data injection attack broadcasts incomplete, corrupted, noisy, got-up and incorrect data through intrusion of malicious agents or corrupted sending agent and affects the reliability of corporate communication system. False data injection attack is very common through broadcast such as reproduction mechanisms, sports, body building and energy medicines, joint and knee pain killer medicines and beauty care products (e.g. skincare, hair care) without mentioning the side effects of different chemical compounds and herbal ingredients used in the medicines on human health and mind. A patient can be easily confused and cheated through popular broadcast and digital advertising. For example, detailed ingredients and chemical compositions are not mentioned clearly on the packet of drug Z for hair care though it is very costly product. The public are consuming energy capsules unknowingly and getting attacked with ailments of digestion system, liver and kidney.

The service consumers must verify the fairness, trust and correctness of data communicated by the service provider to detect false data injection attack and mitigate the risk through social choice. The threat of false data injection attack should be mitigated through rational social choice. The verification mechanisms require the intervention of trusted third parties or detectives who should arrest the malicious agents. The recipients must adopt tit-for-tat strategy: honest public campaign against fake broadcast, threats and punishments of the adversaries. The service consumers must verify the quality of broadcast and provide true, honest and intelligent feedback to the broadcasting forum. If the forum is inactive, toothless, clawless and casual, the deceived agents should report to the highest authorities and seek for legal help to corporate governance. The recipients may adopt retaliative moves such as rejection of fraud channels or switching from one service provider to the other for better quality of service.

(Case-1.4: Shilling attack) This is the case of broadcast corruption through shilling attack. Adaptively secure broadcast is essential to resist shilling attack [6]. Malicious broadcast is a real threat to the digital advertising world. If the recipients sense flaws in digital advertising, the system administrator must verify the correctness, fairness and transparency of the system through analytics on ad slot allocation, content of adwords, exposure time and frequency, customization, delivery, click rate, and impression. Today's broadcast is closely associated with advertising as a recommender system. But, there is risk of *shilling attack* in the form of *push* and *nuke* attacks where the rating of target items (e.g. drugs, medicines and cosmetics) are increased and lowered successively. The advertising world may be digitally divided with a flavor of revenge and retaliation due to zero or low investment on advertising by the corporate world. A corrupted broadcasting system may be involved in brand dilution of a good company through baseless, mischievous and false propaganda. Alternatively, the broadcasting system can push a set of targeted items of poor quality and brand to the public through fraudulent adwords, euphemism and attractive presentation of the popular brand ambassadors. But after the disclosure of the information on such types of malicious attacks, the recipients may lose their trust in the adwords of the digital world in future.

This is the most dangerous threat on a broadcasting system where the sender and the recipients may be honest but the sources of broadcasted data are corrupted. The recipients must threaten and refuse false adwords and complain to the broadcasting forum, quality control and detective agencies and government authorities in time against fraudulent business intelligence. The profiles of shilling attackers must be deleted with the help of collaborative filtering and efficient ranking system. The problem should be solved through regulatory compliance (e.g. RTI, consumer protection acts), cryptology and network security jointly.

(Case-1.5.1 : Sybil attack on Cancer treatment) : This is the case of cancer treatment today. The patients are 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.

(Case-1.5.2 : Sybil attack on herbal and unani drugs) : Herbal and Unani drugs are often sold at very high price in the market in the form of sophisticated labels and packaging of scientific drugs. The poor patients are forced to spend high amount of money on

account of fake drugs. The consumer protection ministry should detect this fake drug racket to save the people. If a herbal or ayurvedic or unani drug is really effective for a healthcare problem; it should be recognized through proper channel, marketing, branding, pricing, promotional and distribution strategy.

It is really complex to trace the corrupted players in the broadcast. A broadcasting communication network is defined by 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 through messages. 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 [7].

There are various types of tracing mechanisms against sybil attack: trusted explicit and implicit certification, robust authentication, resource testing and incentive based game [8]. In case of trusted certification, a centralized authority assigns a unique identity to each entity. The centralized authority verifies computing, storage and bandwidth capability of the entities associated with the broadcasting system on periodic basis. The recipients validate the received data from the sender and checks logically whether there is any inconsistency or chance of injection of false data in the decrypted message. Another approach of tracing is to adopt incentive based game wherein the objective of the detective is to compute the optimum possible reward that reveals the identity of maximum number of corrupted agents. 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.

(Case-1.6 : E-healthcare) : E-health is a significant development of the use of emerging information and communication technologies i.e internet in the healthcare environment. E-health while promising also presents new business challenges in terms of acceptable standards, choice of technologies, overcoming traditional jurisdictional boundaries, upfront investment, privacy and confidentiality. New and evolving information and communication technologies are being adopted by healthcare sector worldwide. It is becoming a commonplace for healthcare systems to deploy an e-healthcare architecture that consists of extranet, intranet and the internet to create a seamless access to data across a set of distributed healthcare systems.

E-healthcare is able to promote bio-terrorism intelligently through many ways. The content of medical and healthcare websites must be carefully designed and audited to resist false data injection attack on the details of drugs, medicine, treatment procedure, doses and side effects. It may not be possible for the common public to treat their ailments just through web search. Clinical decision making is a complex and multi-dimensional problem which needs specialized skill, training and experience of the healthcare consultants. An website should provide detailed information on the availability of healthcare institutes, consultants, distribution and retail outlets and offered healthcare services to the common people correctly. But, it is risky to give detailed data on medical treatment procedure which may confuse the public to take correct clinical decisions.

The model checking algorithms must verify a set of critical parameters such as the risk of snooping and phishing, validation of service oriented computing schema in terms of logic, main flow, sub flows and exception flows of the application, cross site scripting, injection flaws, malicious file injection by testing application programming interfaces and code, insecure direct object reference, cross site request forgery, information leakage and improper error handling, broken authentication and session hijack, insecure cryptographic storage and failure to restrict URL access [9].

Secure service oriented computing should protect the users from various types of malicious attacks. *Phishing* is the misrepresentation of a web link where the malicious agents use social engineering to appear as a trusted identity. They leverage the trust of the users to gain vulnerable information via web link, e-mail or instant messages. The phishers try to capture usernames, passwords and other private information of the users by attacking social web sites, auction sites and online payment processors and cause damages ranging from denial of service to financial loss. There are different types of phishing techniques such as link manipulation, filter evasion, website forgery and cross site scripting. The common resolution techniques are user training and the security measures to be embedded in SOC. The users should be able to recognize phishing attempts and should follow privacy and security policies and license agreements. Anti-phishing measures should be embedded in browsers and website login procedures. The website should be authenticated such a way that it indicates that the connection is in authenticated mode and confirms the authenticity and correctness of the particular site to the user.

In case of *cross site scripting [XSS]*, the attacker executes malicious script in the browser of a user and may hijack the session of the user, deface web site and introduce worms. XSS flaws occur whenever an application takes the data from the user and sends it to a web browser without validating or encoding the content. Preventing XSS requires a secure architectural approach such as input validation, strong output encoding and monitoring of canonicalization errors on a regular basis. The system should validate the configured business rules and reject invalid inputs. The data supplied by the users should be appropriately entity encoded. The inputs must be decoded and canonicalized to the internal representation of the application before proper validation. *Cross site request forgery* attack forces the browser of an active user to send a pre-authenticated request to an web application and forces the victim's browser to perform a malicious action for the

benefit of the attacker. The system should not rely on the credentials or tokens being automatically submitted by the browsers. Reauthentication of sensitive data is required to verify a genuine request.

SQL, HTML and XML *injection flaws* occur when an interpreter receives the data from a user as a part of a command or query; the malicious data force the interpreter to execute unintended commands and the attackers can create, read, edit or delete any data. SOC should support a standard input validation mechanism, strongly typed parameterized query application programming interfaces and object relational mapping libraries. The application should avoid dynamic query interfaces and simple escaping functions and should monitor canonicalization errors. Malicious file execution allows the attackers to perform remote code execution, remote root kit installation and total system compromise. SOC should use an indirect object reference map and strongly validate user's inputs. The firewall rules should prevent the web servers making new connections to external web sites and internal systems**.** Insecure direct object reference occurs when a developer exposes a reference to an internal object like file, directory, database record or key. The attackers can manipulate those references to access other objects without authorization. SOC should not expose private object references to the users, validate any private object reference and verify authorization to all reference objects.

A service oriented application should not disclose their configuration and private functions through error message, debugging and path information or other means. This requires an efficient exception handling approach. The other critical issues are broken authentication, session management and insecure cryptographic storage. Proper authentication and session management is critical to secure service oriented computing. Account credentials and session tokens should be properly protected so that the attackers can not compromise passwords or keys or to assume the identities of the users. Secure SOC should properly authenticate the users and protect their identities and associated credentials. Attackers may use weakly protected data to conduct identity theft. The application should encrypt sensitive information in a data warehouse. The link of a web application should not be disclosed to the unauthorized users. Proper access control should be enforced in the presentation layer and the business logic for all URLs in the application. Section 3 presents a healthcare electronic market based on the proposed secure service oriented computing model.

Theorem 3 : 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. Product recalls are often seen in life-science supply chain. During November 27–December 31, 2013, there were eight recalls by FDA in USA [10]. Today's life chain requires an effective 'Drug Quality and Security Act' 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.

A complex life-science supply chain is a network of firms that satisfies the demand of the customers for healthcare products and medical services. The basic objective is to improve the quality of service in patient care by integrating different business units through systematic coordination of material, information and financial flows. In the context of bio-terrorism, the target points of a complex multi-tier life-science supply chain are SCOR, DCOR and CCOR. *SCOR includes supply chain planning* in terms of demand forecasting, inventory control, production and capacity planning, packaging and labeling, materials requirement planning (MRP); supply chain collaboration and sourcing; supply chain execution through sales and distribution planning, order management, warehouse management, transportation management and reverse logistics. *DCOR includes* innovation, product life-cycle management (PLM) and pricing and *CCOR includes* customer relationship management. A malicious agent is able to launch attacks on a life-science supply chain through these channels. The following cases support the reasoning of the theorem.

(SCOR Case-3.1) : Misleading and confusing content, statistical jugglery and data mining on packaging and label of medicines and drugs distributed through consultants, retailers, wholesalers, distributors and other common channels : It is observed on various products such as (a) hair care products, (b) nutritional food supplement i.e. multi-vitamin, multi-minerals tablets. This is a fundamental problem of supply chain management of life-science products. Herbal and Unani drugs are sold at high price in retail outlets in the camouflage of allopathic medicine.

(a) Drug X: It is prescribed to the aged patients as a multi-vitamin, multi-minerals capsule. The detailed data on ingredients are not clearly mentioned on dark red colored label and packet of drug X. Who is verifying and validating the authenticity of ingredients and chemical compositions of drug X? The consumers suffer from constipation and gastric problem after regular use of drug X. They have become suspicious about the side-effects and authenticity of the drug.

(b) Drug Y: On its packet, the ingredients are mentioned as Zinc Sulphate Monohydrate, Copper Sulphate Pentahydrate, Borage oil, Gamma Linolenic acid, Selenium and others. Are these elements good for human health? Do they have radioactive effect or any other side effects on human cell? It is not clearly mentioned whether this medicine can be used for hair care though the picture of hair of a young man is shown on the packet. It is also confusingly stated that the product is not intended to diagnose, treat, cure or prevent of any disease and the product is proprietary food dietary supplement not for medicinal use. It is also mentioned not to exceed the stated recommended daily dose. But, the dermatologists and hair care specialist prescribe the product for hair care treatment. Why the label is not clearly informing that it is a hair care product or a product suitable for chemotherapy treatment; who should not use the products; what are the adverse side effects of the use of the medicine? The information should be transparent and accountable and also trust worthy. There is no short pamphlet or product brochure in the packet of drug Y. Both drugs X and Y have color such as orange

and light blue. When the tablets are put in normal water, colors are mixing with water. Are these color pigments enhancing the risk of cancer of the consumers?

(SCOR Case-3.2) : This is the case of corrupted sales and distribution system of toxic and tasty junk food and beverages in the open market. The public including the children regularly suffer from the sale of junk food in the open market such as banana chips, spicy biriyani, masala paste, mughlai roll and cutlet, herbal drugs, country liquor, noodles, pasta, colored soft drinks, colored sweets, chocolates, pickle, tobacco products (e.g. gutkha, biri) and fast food and snack items and often affected with cancer, stomach and liver upset and digestions problems due to the presence of artificial preservatives, color and flavor. In an industrial town, it is often seen the association of a meat slaughter shop (e.g. chicken, mutton, fish), non-vegetarian food outlet (e.g. biriyani) and liquor shop side by side. The poor and uneducated laborers of factories consume such junk food and beverage and suffer from hepatitis, jaundice, liver and pancreatic cancer and die prematurely. There is no action from consumer protection department to ban the sales and distribution of these malicious elements in open market. Fraudulent advertisements of cosmetics and creams are often broadcasted on beauty care; are they really effective? There should be more focus on the nutrition of the children, boys, girls and the youth of the world for their proper health and development of body They should be able to lead a good life-style and stress free life. What is the responsibility of SD module of ERP system in life-science supply chain management? The solution is strict regulatory compliance imposed by a sensible and responsible corporate governance.

(SCOR Case-3.3): Inventory management is a critical challenge in life science supply chain due to uncertainty of demand and short time interval between manufacturing date and expiry date. The healthcare consultants are often pressurized by the sales people of life-science firms to push new or slow moving drugs, medicines and bio-medical devices of old models for the use of service consumers. Today, the healthcare consultants often prescribe drugs and medicines based on the availability of stock in the retail outlet. Analytics should be intelligently used for efficient inventory management to monitor dead stock, slow moving stock, ABC analysis and XYZ analysis. It is essential to minimize the wastage of blood and donated organs through improved storage system. Intelligent heuristics should be used to reduce overstock or stock out situation. Example: EOQ = Forecasted demand + Safety stock – Pending order – Current stock. The overstock should be distributed to the poor and needy people in time through efficient distribution planning. The basic objective is to attain zero wastage.

(DCOR Case-3.4): Product life-cyle management is a critical part of life-science supply chain. Still today, effective medicines, drugs, biomedical devices, surgical operations and treatment procedure are not discovered for different life-threatening ailments such as diabetes, cancer, cancer of mind, migraine and headache rheumatic arthritis, joint and knee pain and orthopedic problems of aged people. In case of diabetes, there is no permanent solution for recovery. A diabetic patient is forced to take medicines continuously for blood sugar control within safe limit. If he / she stops medication, the blood sugar will be out of control. This is the failure of modern medical science. The life-science supply chain needs innovation in product life-cyle management

E-health is a promising IT platform of healthcare services. An efficient information system integrates various enterprise applications such as life-science supply chain and healthcare service chain while maintaining individual autonomy and self-governance. The system should support confidentiality, message integrity, non-repudiation, auditing and availability of service in time. The system should support sharing of data in a collaborative business environment wherein a group of trading agents can exchange strategic business information maintaining the privacy of critical data. Increased organizational agility is required for the cooperation of adaptive enterprises. Information technology can improve the quality of service and reduce cost in healthcare services. The demand for critical patient care is growing. But, many small rural healthcare centers are facing problems to develop and maintain a costly IT infrastructure. This forces those healthcare centers to search for innovative IT platform. A life-science supply chain can be protected from threats of disruption through intelligent coordination mechanisms, intelligent contracts, multi-party negotiation, economic modeling, buyer-seller behavior, security and privacy of the trading agents, payment determination, dynamic pricing strategy and information flow. E-health provides different types of benefits in terms of greater geographical reach, global sourcing, reduced transaction costs, improved customer service, accuracy, ease of processing, increased productivity and quick access to information.

Theorem 4* : *Healthcare service chain is another soft target of bio-terrorism.

The critical processes associated with a healthcare service chain are 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. There may be the risks of failure of secure multi-party computation due to following reasons:

(**Case-4.1**) 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.

(**Case-4.2**) 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.

(**Case-4.3**) 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.

(**Case-4.4**) Computational errors due to wrong configuration of enterprise applications and / or errors in the heuristics, 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.

(**Case-4.5**) Access control problem causing dangerous errors in information system; a malicious agent may enter false data into HIS during the absence of authorized users.

(**Case-4.6**) 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.

(**Case-4.7**) 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.

(**Case-4.8**) Errors in scheduling due to exceptions (e.g. unfit patients, non-availability of healthcare experts).

(**Case-4.9**) 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.

(**Case-4.10**) Lack of verification of correctness of computation in medical billing and payment processing by the service provider and / or service consumer.

(**Case-4.11**) Incorrect data in patient's help guide may cause confusions and mismatch between the computed results and perceived one.

(**Case-4.12**) Incorrect feedback by the patients or their attendants due to misperception, misunderstanding of feedback form, lack of knowledge and critical observations or casual attitude.

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. A secure service oriented computing model must address correct identification, authentication, authorization, privacy and audit for each e-transaction. 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 his scope. The system should ask the credentials of the requester; validate his credentials and authorize the user to perform a specific task. Each trading agent should be assigned an explicit set of access rights according to his role. Privacy is another important issue. A trading agent can view only the information according to his authorized access rights. Finally, the system should audit each transaction - what has happened after the execution of a specific service.

Today, healthcare faces critical legal, ethical and psychological issues from the perspectives of security, privacy, confidentiality and organizational policy. Security and privacy of data is important from the perspectives of access control, data storage, version control of critical applications, accountability, traceability and transparency E-healthcare information should be managed in a digital environment through efficient security principles, privacy laws and policies in the domain of shared and managed care. Shared care is a healthcare service that is delivered at multiple locations and by multiple service providers through sharing of the medical information of the patients. Managed care is characterized by cost reduction and quality enhancement techniques practiced by either healthcare service providers or insurance companies. Both paradigms require secure exchange of patient's private data through internet. Another important issue is effective implementation of Hospital Protection Act in the event of the death of the patients and the arrest prevention act of healthcare professionals.

Theorem 5: Malicious business intelligence is a critical threat factor of bio-terrorism. The conflict between security intelligence and business intelligence is inevitable.

Malicious business intelligence attacks 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. It is a disguised form of capital punishment. The properties of secure multi-party computation are applicable to resolve this conflict between security and business intelligence.

(Case-5.1): A critical patient Alice is treated in intensive care unit unnecessarily for long duration even there is no hope of recovery. AC charge is billed even after her death. There is another instance of a patient Bob having a simple medical problem. But, he is prescribed costly medical drugs and is treated through different costly testing procedures (e.g. CT Scan, USG, MRI scan) unnecessarily to enhance the cost of treatment. The basic objective is to maximize the revenue from medical bills.

(Case-5.2 : Health Insurance) : This is the case of a people-friedly affordable health insurance model. Health is wealth. But, life is full of uncertainties. The cost of healthcare is rising but the earning is getting low. In this situation, the people are forced to drain all their savings to pay hospital bills. They can get high quality of healthcare service and tax benefits through a set of intelligent health insurance plans.

A health insurance plan should cover hospitalization expenses including consulting testing and surgical operations, ambulance, room rent, boarding and nursing expenses. Thus, the common people can avail financial security, high quality of healthcare service and tax benefits. But, they should be rational in buying appropriate health insurance plans considering various terms and conditions, scope, needs and budget. Generally, health insurance is a yearly policy which should be renewed each year subject to certain exclusions and waiting period. Health insurance can be claimed in two ways: reimbursement and cashless. In case of reimbursement, a person gets admitted in a hospital, pays hospital bills, submit the documents and claim form to the insurance service provider for reimbursement. On the other side, a health insurance service provider may have a network of hospitals with specific arrangement for direct billing. An insurance person is

admitted in a network hospital by submitting a cashless card. The hospital processes cashless admission of the patient and hospital expenses are paid by the insurance service provider covered by the plan.

The financial intelligence of healthcare service is associated with multiple payment processing options such as health insurance, credit card, direct cash payment, bank loan and donation. Another important issue is discriminatory pricing of drugs, biomedical devices, helathcare and surgical products and services and also combinatorial pricing plan for different packages. The basic building block of digital transformation is a well-designed web application schema. The content of the web portal should be defined intelligently and is expected to provide a transparent overview of various types of health insurance plans, their benfits and limitations, business rules, group buying strategy, cliam processes (reimbursement and cashless), payment processing options and discriminatory singular or combinatorial pricing strategy. An online premium calculator should be able to compute premium and service tax for a selected health insurance product, age band and sum insured with a comprehensive cost-benefit analysis, risk assessment and mitigation strategies and tax savings. The service consumers and health insurance service providers should be able to process buy, renew, claim and reimburse functions online maintaining privacy, fairness, correctness, trust, transparency and rational information exchange. Additionally, the web enabled application should provide detailed information on help guide, buying tips, free helpline number, mobile commerce model, customer service contact number and e-mail id, legal and regulatory compliance issues correctly. The payment function should be designed innovatively, fairly and rationally in terms of intelligent contract, pricing strategy, payment terms, incentives and penalty function. It is essential to audit malicious business intelligence of a health insurance model by verifying transparency and accountability of the payment mechanism from the perspectives of violation in contractual clauses among the agents, flaws in payment function computation or pricing algorithm and package configuration and commitment.

(Case-5.3) For effective healthcare system innovization, digital technology management is not only the critical success factor. There are other several factors such as HR policy in talent management, quality of medical education, intelligent public policy, mechanisms and corporate governance. The healthcare consultants, specialists and work force need a good human resource management model for proper talent acquisition and retention, research and innovation, career growth planning, incentive, reward, recognition and retirement planning. The healthcare service provider may have a flawed business model based on old legacy information technology, malicious healthcare practice due to economic and financial pressure, mechanical HR policy and bad resource allocation mechanism. The patients or service consumers may lose trust in health care products and practice due to costly treatment procedure, complicated and fraudulent business rules and vague computational intelligence. Such an inefficient system increases the risk of bio-terrorism through malicious behavior of the trading agents, administrative inefficiencies, collusion of the trading agents against regulatory compliance, financial fraud in e-transactions, quality problems in testing and sourcing, non-availability, poor performance and failure of medical equipments, malicious work culture, medical negligence, unauthorized absence, excessive work load, strikes and physical security problem of healthcare service provider. The healthcare workforce expect to work freely in a collaborative, flexible and ethical work culture without any financial, physical, mental and cultural constraints and pressures.

Globally healthcare organizations are undertaking massive business process reengineering initiatives and many of these reforms are supported by the strategic use of advanced information and communication technology. It should provide better integration and improved coordination of flows of material, information and funds within and across healthcare firms, experts and patients. This results improved patient care, greater accuracy, cost efficiency, ease of processing, increased productivity and fast response time in healthcare service. Service oriented computing results improved interoperability, increased federation, and organizational agility through a standardized, flexible, reliable and scalable architecture. However, it enhances the risk of various types of malicious attacks on the healthcare service chain and life-science supply chain and these are the emerging threats of bio-terrorism today.

4. CRYPTOGRAPHIC CHALLENGES

Theorem 6: It is essential to develop new cryptographic tools and techniques to satisfy multi-dimensional properties of secure multi-party computation for ensuring security intelligence of a complex system at improved cost of computation and communication. It is clearly shown by threat analytics.

Traditionally, the concept of encryption and decryption has been used to preserve the privacy of critical data for an intelligent healthcare information system [11]. It is used for private communication and secure data storage. Intelligent transaction processing systems have used cryptographic techniques effectively to ensure authentication, authorization, access control, correct identification, privacy and audit of electronic transactions [12]. The most critical issue is the cost of computation of security algorithms. In the context of secure communication, cryptography ensures privacy and secrecy of sensitive data through encryption method. S encrypts a message (m) with encryption key and sends the cipher text (c) to the recipients (R). R transforms c into m by decryption using secret decryption key. 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 and public key. 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 keys are same. Secure broadcast authentication is hard with symmetric encryption key with untrusted recipients. 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. Asymmetric RSA encryption achieves broadcast authentication where each recipient can verify the authenticity of received data but can not generate authentic messages.

A *digital signature* is a cryptographic primitive by which a sender (S) can electronically sign a message and the receiver (R) can verify the signature electronically [13]. S informs his public key to R and owns a private key. S signs a message with its private key. R uses the public key of S to prove that the message is signed by S. The digital signature can verify the authenticity of S as the sender of the message. A digital signature needs a public key system. A cryptosystem uses the private and public key of R. But, a digital signature uses the private and public key of S. A digital signature scheme consists of various attributes such as a plaintext message space, a signature space, a signing key space, an efficient key generation algorithm, an efficient signing algorithm and an efficient verification algorithm. Digital signature provides authentication and non-repudiation through asymmetric property of cryptography at high cost of computation and communication. One way hash function may be used as the basic building block of asymmetric RSA digital signature and cryptographic commitment. A one-way function is a function that is easy to compute but computationally infeasible to invert. If x is a random string of length k bits and F is a one-way function then *F* can be computed in polynomial time as y = F(x) but it is almost always computationally infeasible to find x' such that F(x') = *y*. Merkle hash tree is an efficient construction of one way function.

Another alternative interesting option for secure broadcast authentication is signcryption [14]. Traditional signature-then-encryption is a two step approach. At the sending end, the sender signs the message using a digital signature and then encrypts the message. The receiver decrypts the cipher text and verifies the signature. The cost for delivering a message is the sum of the cost of digital signature and the cost of encryption. Signcryption is a public key primitive that fulfills the functions of digital signature and public key encryption in a logically single step and the cost of delivering a signcrypted message is significantly less than the cost of signature-then-encryption approach. A broadcasting system is vulnerable to insecure communication. The basic objective is that the system properly signcrypts all sensitive data. A pair of polynomial time algorithms (S,U) are involved in signcryption scheme where S is called signcryption algorithm and U is unsigncryption algorithm. The algorithm S signcrypts a message m and outputs a signcrypted text c. The algorithm U unsigncrypts c and recovers the message unambiguously. (S,U) fulfill simultaneously the properties of a secure encryption scheme and a digital signature scheme in terms of confidentiality, unforgeability and nonrepudiation. *Signcryption* can ensure efficient secure broadcast communication. In a triplet Elgamal signature scheme [r,e,s], the commitment r is computed as $r = g^k [\text{mod } p]$ where g and p are part of the public key and the commitment k is an integer independent to such values [15]. The signature generation scheme permits the receiver to recover the commitment by computing $r = g^s y^e (\text{mod } p)$. The sender computes the commitment in such a way that it is only recoverable by the receiver. The commitment value can be used as a symmetric key shared between the sender and the receiver and this symmetric encryption provides message confidentiality. The recoverable commitment value of Elgamal triplet signature scheme is used as the symmetric key to achieve symmetric encryption of the message while the triplet signature serves the signature.

Alternatively, the agents may adopt different types of privacy preserving data mining (PPDM) strategies such as randomization, summarization, aggregation, generalization, suppression, de-identification and k-anonymity. Intelligent PPDM strategies may improve the cost of computation in secure communication. The basic objective is to provide confidentiality, data integrity, authentication and non-repudiation in the communication of sensitive data.

Let us now conclude this work. The threat analytics clearly shows cryptographic challenges of secure multi-party computation for intelligent and complex systems and critical applications. It is essential to develop new cryptographic techniques and tools which should be able to provide collective security intelligence in terms of correctness, fairness, trust, transparency, accountability, reliability, confidentiality, data integrity, non-repudiation, authentication, authorization, correct identification, privacy, safety and audit of complex information systems. Another critical agenda is to improve the cost of computation and communication of secure multi-party computation protocols. Efficient signcryption and unsigncryption algorithms should be implemented practically in the form information security solutions. The properties of secure multi-party computation are useful to resolve the conflicts between the security intelligence and business intelligence of a complex mechanism. It is an interesting option to explore the application of secure multi-party computation for the design of intelligent mechanisms through the cross fertilization of cryptography and algorithmic game theory.

REFERENCES

1. G.Kol and M.Naor. Cryptography and game theory: Designing protocols for exchanging Information. Proceedings from 5th Theory of Cryptography Conference (TCC), 2008.
2. W. Du. A study of several specific secure two-party computation problems. Doctoral dissertation, Purdue University, USA. 2001.
3. Y.Lindell. Composition of secure multi-party protocols a comprehensive study. Springer. 2003.
4. S.Chakraborty. A study of several privacy-preserving multi-party negotiation problems with applications to supply chain management. Doctoral dissertation (unpublished), Indian Institute of Management Calcutta, 2007.
5. A.L.Melnick. Biological, chemical and radiological terrorism. Springer, NY,USA, 2008.
6. S. Chakraborty. Security intelligence for broadcasts: Threat analytics. Technical report. 2012.
7. J.Douceur. The sybil attack. Proceedings of Workshop on P2P systems (IPTPS). 2002.
8. A.K.. Pal, D.Nath and S.Chakraborty. A Discriminatory Rewarding Mechanism for Sybil Detection with Applications to Tor, WASET, Brazil.2010.
9. M.Shema. edited by A.Ely. Seven deadliest web application attacks. Elsevier. 2010.
10. F.A.Kuglin. Pharmaceutical supply chain drug quality and security act. CRC Press, Taylor & Francis Group, Boca Raton, USA, 2015-16.
11. G.Ateniese, R.Curtmola, B. Medeiros and D.Davis. Medical information privacy assurance: Cryptographic and system aspects, Technical Report, John Hopkins University,2003.
12. M.Gertz and S.Jajodia. Handbook of database security applications and trends. 2008.
13. B. Schneier. Applied Cryptography, John Wiley, New York,1996.
14. W.Mao. Modern Cryptography Theory & Practice, Pearson Education.2007.
15. Y.Zheng. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption). LNCS 1318, Springer-Verlag.