Mobile Commerce: Secure Multi-party Computation & Financial Cryptography

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: The basic objective of this work is to construct an efficient and secure mechanism for mobile commerce applying the concept of financial cryptography and secure multi-party computation. The mechanism (MCM) 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, payment function, a strategy profile, dominant strategy and revelation principle. The mechanism adopts a set of intelligent moves as dominant strategies: (a) flexible use of hybrid payment system which supports cash, e-payment and m-payment, (b) secure multi-party computation to ensure information security and privacy and (c) call intelligent analytics to assess and mitigate possible threats on m-commerce service. The mechanism supports three different types of transaction processing protocols (P_1, P_2 and P_3) and calls a cryptographic protocol (P_c). The cryptographic protocol performs a set of functions sequentially such as authentication, authorization, correct identification, privacy verification and audit of correctness, fairness, rationality, accountability and transparency of secure multi-party computation on each m-transaction. The basic building blocks of the cryptographic protocol are signcryption, proofs of knowledge, commitments and secret sharing. This work also presents the complexity analysis of the mechanism in terms of computational cost, communication cost, security and business intelligence.

Keywords: Secure multi-party computation, Financial cryptography, Mobile commerce mechanism, Threat analytics, Digital economy

1. Introduction

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 [1,2]. 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 [3]. 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 [4].

Recently, there is a trend of cross fertilization between two disciplines: game theory and cryptography [5]. 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. [6] 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. 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 [7,8]. 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 [9,10,11,12,13]. 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 such as mobile commerce.

The rapid expansion of global market, the explosion of technology and aggressive competition have redefined brick-and-mortar business models. In such a complex and turbulent environment, web technologies - through Internet, Intranet and Extranet - strategically impact traditional business applications. It is possible to explore e-business opportunity practically anywhere in the value chain of a brick and mortar business model - it may be automation of administrative process, supply chain reconfiguration and integration, reengineering of primary infrastructure, enhanced selling process or provision of customer service. However, nearly all e-commerce applications developed so far assume stationary users with wired infrastructure; but this is likely to change with the emergence and wide spread adoption of mobile communication technology.

Mobile commerce is the use of radio based wireless devices such as cell phones and personal digital assistants to conduct business-to-business and business-to-consumer transactions over wired, web based e-commerce system. It means any transaction with a monetary value that is conducted via a mobile telecommunications network. Mobile Commerce is commonly known as M-Commerce or mobile electronic commerce or wireless electronic commerce. According to this definition, m-commerce represents a subset of all e-commerce transactions. Regular SMS messages from one person to another are not included in the definition of mobile commerce, while SMS messages from an information service provider, that are charged at a premium rate, do represent mobile commerce. The scope of mobile commerce has been explored in various types of applications such as banking and financial services, retail, logistics, utilities, travel and hospitalities [14,15,16]. Distributed computing considers the scenario where a number of distinct, yet connected computing agents wish to execute a joint computation. The objective of secure multi-party computation is to enable these agents to carry out such distributed computing tasks in a secure manner. The advancement of computer network technologies, multi-agent system and cryptography has improved the efficiency of secure multi-party computation significantly. The basic objective of this work is to explore the scope of secure multi-party computation for mobile commerce in a digital economy.

Let us discuss the contributions of this work. First it defines the traditional concept of secure multi-party computation. Next, it has redefined the concept of SMC from a broader perspective. The complexity and efficiency of secure multi-party computation are analyzed in terms of rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, reliability, consistency, commitment; safety, liveness, synchronization, reachability, deadlock freeness; authentication, authorization, correct identification, non-repudiation, integrity, audit and privacy. This broad outlook of secure multi-party computation is essential to define the objectives and motivation of digital payment system: what are the economic benefits? How to do the cost-benefit analysis? How to mitigate the risks of black money, fake currencies, terrorism, corruption and ease of doing business in a digital economy? The concept of SMC has been applied to construct a secure m-commerce mechanism with the support of proofs of knowledge, commitments, digital signature, signcryption and secret sharing. The research methodology includes the review of literature on secure multi-party computation and financial cryptography, reasoning on a case of digital m-payment system, thesis on secure multi-party computation [17] and summer project on mobile commerce [14]. This work is organized as follows. Section 1 defines the problem. Section 2 presents

secure mobile commerce mechanism (MCM). Section 3 highlights the complexity analysis of the proposed mechanism in terms of computational cost, communication cost, security and business intelligence. Section 4 concludes the work.

2. Mobile Commerce Mechanism (MCM)

##
Objectives : efficient fast transaction processing, ease of doing business, monitoring of corruption, black money flow, fake currency and terror funding;
Constraints : cost, skill;
Agents : service consumer or user (C), mobile or internet service provider (P), merchant (M), bank (B);
System :

- Digital Payment System (DPS): micro payment, e-wallet, debit card, net card, pre-paid card, post- paid credit card, digital only zero balance accounts, health card, e-cash;
- Mobile system : communication, application, data and computing schema;

Input : username, password, e-cash;
Protocol : call ***transaction processing protocols*** (P_1 or P_2 or P_3); call ***cryptographic protocol*** (P_c);
$P_1 \rightarrow$ B: E-cash set up $\rightarrow$ Generate bank key and user key $\rightarrow$ C: Withdraw $\rightarrow$ Spend $\rightarrow$ M: Deposit $\rightarrow$ B: verify correctness;
$P_2 \rightarrow$ C: Spend using post-paid credit card or borrow $\rightarrow$ Login $\rightarrow$ Pay debt $\rightarrow$ Log out;
$P_3 \rightarrow$ C: Log in $\rightarrow$ Deposit $\rightarrow$ Withdraw $\rightarrow$ Spend using pre-paid card $\rightarrow$ Log out;
Cryptographic protocol (P_c) :
authentication : fix contractual clauses of m-service through *cryptographic commitment. A*sk the valid identity of an agent for each m-transaction.
authorization : ask the credentials (e.g. username, password and security pin) of the requester through *secret sharing*; validate the credentials and authorize the agent to perform a specific task as per an explicit set of access rights assigned to a role.
correct identification : verify *trust* by validating *proofs of knowledge* of the agent on credentials, business rules (e.g. limits on deposit and withdrawal) and contractual clauses.
privacy : ensure private communication among the agents through *signcryption*. An agent should be able to view only the information according to authorized access rights.
***audit* :** verify *correctness, fairness, rationality, accountability and transparency* of secure multi-party computation on each m-transaction (e.g. account balance after deposit, withdrawal or borrowing) as per commitment.
Revelation principle: call threat analytics and audit *security intelligence* of mobile commerce service.

- what is corrupted or compromised: agents, communication schema, data schema, application schema, computing schema?
- detect type of threat : coercion or rubber hose attack, denial of service, web security flaws : session hijack, phishing, hacking, defacement of websites, probing of critical networks and servers, unauthorized access of system and data, malicious code attack, identity theft, spoofing and phishing, attacks on critical infrastructure and wireless networks, attacks on e-governance, e-commerce and m-commerce websites etc.;
- time : 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 on performance, sensitivity, trends, exception and alerts.
- recommend : what is the next best action?
- predict : what is the best or worst that can happen?
- verify rationality, fairness, correctness, transparency, accountability, resiliency, reliability, consistency and scalability;
- verify liveness, deadlock freeness, reachability, synchronization and safety of m-service;

Payment function: audit *computational intelligence* of payment function (f_p) : payment mode - prepaid or postpaid, payment terms, service tax per transaction, reward or incentive and penalty or interest;
Moves:

- *flexible use of hybrid payment system* which supports cash, e-payment and m-payment;
- *secure multi-party computation* to ensure information security and privacy;
- *call intelligent analytics* to assess and mitigate possible threats on mobile communication system.
    - Effective firewall and virtual private network (VPN) for blocking unsolicited internet connection, getting secure and encrypted internet connection or WiFi networks from hacking and sniffing of passwords and personal data;
    - Encrypt messages in a secure form for mobile applications;
    - A locker or file vault to protect the hard disks of mobile phones;
    - Maintain a master password for passwords through password manager; configure strong password and change on periodic basis; the agent must not share own username and passwords with the others. Biometric protection based on fingerprints is expected;
    - Two-factor-authentication to access and protect e-mail and social media accounts through mobile phones;
    - Use a browser plug-in (HTTPS) to ensure use of secure form of websites for the protection from various forms of surveillance and hacking and encrypted connection to the website accessed through mobile phones;
    - Get notified about the trustworthiness of a website through web-safe-browser-extensions;
    - Use Incognito mode or Tor to allow private web activity.
    - Cover individual webcam with tape to avoid spying through camera;
    - Use RFID blocking wallets to prevent on-the-move attacks from RFID scanner;
    - Identify fake calls and SMS by setting up Truecaller in a mobile phone and turning on spam detection;
    - Delete traces from mobile phones while destroying old data during selling or exchange;
    - Protection of private data if mobile phones are stolen or lost; hidden lockers are essential for saved cards and private data; secure cryptographic storage is expected in mobile servers;
    - Mandatory reporting of m-commerce security breaches by service providers, consumers, corporate bodies, data centers and intermediaries to the government authorities under laws;
    - Be alert of telephobia and social anxiety disorder in the form of unintelligent phone calls.

Output: security intelligence of m-commerce service;

##

2.1 Cryptographic Protocol (P_c)

The basic building blocks of the cryptographic protocol in mobile commerce mechanism (MCM) are digital signature or signcryption, proofs of knowledge, commitments and secret sharing. Let us first analyze the role of **digital signature and signcryption** in the aforesaid mechanism**.** In case of secure communication, cryptography ensures privacy and secrecy of sensitive data through encryption method [18]. The sender (S) encrypts a message (m) with encryption key and sends the cipher text (c) to the receiver (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 [13]. 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. 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.

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 [14]. S informs his public key to R and owns a

private key. S signs a message with his 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. Blind signatures form the core of e-cash. A user (X) can get a signature from another agent (Y) on a value without revealing it to Y.

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. DPS 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 [19]. 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.

A **cryptographic commitment** is a piece of data which binds its creator to a unique value, yet appears random until it is decommitted. A commitment is the cryptographic equivalent of a sealed envelope. For example, a Pedersen commitment to w with randomness r is the group element $C_r(w) = g^w h^r$ and can be decommitted by revealing r and w [21]. Here, p is a large prime and q is a prime such that q divides [p-1]; $G = Z_p$ denotes the group of mod p integers; $g \in G$ and $h \in G$ be group elements of order q such that discrete log and $\log_g(h)$ are unknown. This commitment is computationally binding and unconditionally hiding. A zero **knowledge proof** of knowledge allows a prover to demonstrate knowledge of hidden values without actually revealing them. A proof of knowledge of a Pedersen committed integer w demonstrates knowledge of w and r such that $C_r(w) = g^w h^r$. One can also prove that a committed value w satisfies some condition $\phi(w)$ without revealing it. POK(w,r | $C = g^w h^r$, $\phi(w)$) denotes a zero knowledge proof of knowledge of (w,r) satisfying both $C = g^w h^r$ and the predicate $\phi(w)$. E-cash systems apply the concept of **secret sharing** such as arithmetic or Shamir's scheme [22] to identify double spenders. The user breaks her public key into n pieces of which at least two are required to recover her identity.

3. Complexity Analysis

The following section presents the complexity analysis of MCM in terms of security intelligence, computational and communication cost and also business intelligence.

3.1 Strategic Moves

Theorem 1 : The mechanism adopts a set of intelligent strategic moves for streamlined efficient transaction processing and improved security and privacy for mobile commerce service.

MCM outlines the construction of an efficient and secure digital payment mechanism. The 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 [31]. The agents involved in the mechanism are service consumer or user (C), mobile or internet service provider (P), merchant (M), bank (B). A user is an agent or an organization with computer, mobile phone, PDA, laptop or tablet connected to the web that consumes and pays online for products or services ordered to the merchants. The payer is the buying role of the customer. A merchant is an agent or an organization that offers products or services on the Internet and is being paid for those products. The payee is the selling role of the merchant. A bank is responsible for payment transaction processing. A payment gateway

interconnects different agents. The basic objectives of the mechanism are efficient fast transaction processing, business intelligence, ease of doing business, monitoring of corruption, black money flow, fake currency and terror funding subject to budget constraints. The mechanism adopts a set of strategic moves: an intelligent mix of cash, e-payment and m-payment for flexible transaction processing options; intelligent threat analytics to assess and mitigate various risks and secure multi-party computation for improved fairness, correctness, transparency, accountability and also privacy.
The Digital Payment System (DPS) uses different types of payment option such as cash, micro-payment, e-wallet or prepaid card, debit card, post paid credit card and health card [30]. The communication and application schema support both e-payment and m-payment system. A micropayment system supports money transfers smaller than the minimal economically feasible credit card transaction [23,24]. It supports low value payments at low transaction costs and with a minimal delay and in exchange the products (e.g. digital content and services like online music, videos, games, economic and financial news, social networks and online brokerage) are instantly delivered.
The mechanism supports protocols P_1, P_2 and P_3. The cryptographic building blocks of e-cash set up and e-transactions include proofs of knowledge, commitments, blind signatures and secret sharing [25,26,27,28,29]. Each protocol is linked with a set of processes. It is required to generate a set of public and private keys for e-cash set up and bank key generation. Withdraw lets the user to extract e-cash from her bank account through proper authentication and authorization. Spend allows her giving the merchant a specific amount of e-cash. Deposit allows the merchant giving the bank the spent e-cash.
The mobile commerce mechanism adopts a set of intelligent moves a dominant strategies: (a) flexible use of *hybrid payment system* which supports cash, e-payment and m-payment, (b) *secure multi-party computation* to ensure information security and privacy and (c) call *intelligent analytics* to assess and mitigate possible threats on mobile communication system. 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. The mechanism is truthful if the agents report their strategic moves correctly. Truth telling may be a dominant strategy. The mechanism is strongly truthful if truth telling is the only dominant strategy. The basic objective of the mechanism is to find an acceptable distribution of cost among the agents. The 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 this mechanism is applicable in various domains such as policy making in corporate governance, supply chain finance, banking and financial services, logistics, utilities, travel and hospitality.

3.2 Security Intelligence

Theorem 2 : MCM verifies security intelligence of mobile commerce service collectively through rational threat analytics.

The security intelligence of the mobile commerce mechanism is a multi-dimensional parameter which is defined in terms of rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, reliability, consistency, commitment; safety, liveness, synchronization, reachability, deadlock freeness; authentication, authorization, correct identification, non-repudiation, integrity, audit and privacy. The mechanism 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, the DPS 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. The fundamental objectives of cryptography are to provide confidentiality, data integrity, authentication and non-repudiation.
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 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.

Test case 1 (Rubber hose attack) : The digital payment system associated with MCM may face miscellaneous types of threats. Generally, the service consumers or users are recommended that they should never share username and , password to the other agents; they should assign strong password and change the same on periodic basis; they should not keep common passwords across various sites associated with m-service. But there may be the risk of coercion i.e. rubber hose attack; ordinary passwords can be given away inappropriately. Innocent honest public can be physically coerced or threatened into revealing their passwords or forced to disclose them to the malicious adversaries. Where is the safety of e-cash or m-cash? Let us recall the basic security issues in e-transactions or m-transaction. In fact, user's password is always disclosed to the system administrator (e.g. cloud computing, web mail service). The message can be encrypted but the provider of encryption and decryption algorithms can crack the passwords efficiently. Suppose, a user is trying to protect a document file through single or multiple passwords. The software service provider can easily crack the encryption options or passwords. It is an open research agenda how to mitigate the risk of rubber hose attack through aforesaid threat analytics of the mobile commerce mechanism.

Test case 2 (Mobile internet security flaws): Let us also recall online security issues accessed through mobile phones. An web enabled payment system accessed through mobile phone may face different types of vulnerabilities such as hacking, virus attack, cross site scripting, injection flaws, malicious file execution, insecure data object reference, cross site request forgery, information leakage, improper error handling, broken authentication, session hijack, insecure cryptographic storage, insecure communication and failure to restrict URL access. How to solve these security problems in e-transactions? Natural disaster (e.g. flood, storm, snowfall, heavy rainfall, Tsunami) may cause denial of service due to communication link failure. There is also threat of traffic congestion in the communication channel. There is threat of power cut i.e. cascaded black out for very long duration.

The basic objective of the mechanism is to protect DPS from phishing attacks, privacy violations, identity theft, system compromise, data alternation, data destruction, financial and reputation loss. Cross site scripting (XSS) flaw allows an attacker to execute malicious code in the web browser of the user that can hijack user session, deface websites, possibly introduce worms or insert hostile content or conduct phishing attack and take over the browser of the victim through malware. The best protection of XSS is a combination of validation of all incoming data and appropriate encoding of all output data. Validation allows the detection of XSS attacks and encoding prevents injection of malicious script into the browser. Cross site request forgery (CSRF) forces the web browser of the logged on user to send a request to a vulnerable web application which forces the victim's browser to perform a hostile action. Web applications rely solely on automatically submitted credentials such as session cookies, basic authentication credentials, source IP address, SSL certificates or windows domain credentials. CSRF is applicable to any web application that has no authorization checks against vulnerable actions.

Injection flaws allow the attacker to create, read, update or delete any arbitrary data available to the application. Even, it may compromise the web application completely bypassing firewalled protection. SQL injection occurs when the data input of the user is sent to an interpreter as part of a command and query. The hostile data of the attack forces the interpreter to change the data or execute unintended command. The common protection measures are to use strong and safe interpreters, do input validation, use strongly typed parameterized query APIs, enforce least privileges, avoid detailed error messages, use stored procedures, do not use dynamic query interfaces and do not use simple escaping functions.

Web application developers often trust input files improperly and the data is checked insufficiently. Arbitrary, remote and hostile content may be processed or invoked by the web server. It allows an attacker to perform execution of malicious code, installation of tool kit and system compromises remotely. Flawless design is required during the construction of system architecture, design and software testing. The application developers should use indirect object reference map, check errors, validate user's input and implement firewall rules appropriately. Another critical problem is insecure direct object reference; a direct object reference occurs when a reference is exposed to a file, directory, database records or key as a URL or form parameter. A malicious agent can manipulate these references to access other objects without authorization. The web application should avoid exposing direct object reference to the users by using an index, indirect reference map or other indirect validated method that is easy to validate.

An web application can unintentionally leak information about their configuration, internal state or violate privacy through error messages and it can launch dangerous attacks. The application should get support from a standard exception handling mechanism to prevent the leakage of unwanted information; detailed error handling should be limited; errors should be properly checked and should not be exploited by the intruders. Broken authentication and session management is caused due to the failure of protection of credentials and session tokens. It can hijack user's or administration's accounts, undermine authorization and accountability controls and cause privacy violations. The common protective measures are the adoption of efficient authentication mechanisms, secure communication and credential storage, use of efficient session management mechanisms; invalid session identifiers should be rejected.

Insecure cryptographic storage is caused due to the failure in encrypting sensitive data; it leads to disclosure of sensitive data and compliance violation. It is required to avoid inefficient weak cryptographic algorithms and check whether sensitive data are encrypted properly. An web application may fail to encrypt network traffic to protect sensitive communications. The adversary can sniff traffic from the communication network and access sensitive data, credentials, authentication or session token. The application should properly encrypt critical data. The only protection for a URL is that links to a page are not presented to unauthorized users. The adversary may get access to these pages and view private data. All URLs and business functions should be protected by an effective access control mechanism. Web security is a very broad topic; some common critical issues have been discussed above very briefly. There are several open issues in the design of service oriented computing schema. It is an interesting option to interview Internet experts, web developers and programmers and analyze the complexities and challenges in web programming issues.

Test case 3 (Denial of Service) : Next, let us analyze the threat of denial of service (DoS) which is common at retail outlets or restaurants. A digital card may be damaged or card reader may malfunction. For instance, Bob went to a restaurant with his family and ordered a grand dinner. After the dinner, he found that his credit card was not functioning or there was a problem of card reader which was unable to access his smart phone properly. He was not carrying any cash; He should have multiple flexible payment options such as cash or digital payment to avoid the surprise. The user may commit errors : he or she may forget password and / or pin number; may forget that the valid timeline of the card may expire. Lack of knowledge, skill and education of the users is a critical failure factor. The user may also face different types of threats from the digital payment service provider such as error in credit card statement (e.g. swap or mixing of data; incorrect computation, delay or stopping posting to destroy proof, malfunctioning of mobile SMS message and electronic mail system). A digital payment service provider often changes business rules without proper communication to the user. The user may also face various threats of fraudulent transaction in terms of hacking the privacy of a user's personal data like credit card number, pin and signature. There is also risk of communication link failure, coremelt attack and traffic congestion.

Test case 4 (M-commerce corruptions) : Now the question is the objectives and motivation of digital payment system: what are the economic benefits? who is doing the cost-benefit analysis? How can it mitigate the risks of black money, fake or counterfeit currencies, terrorism, corruption and ease of doing business? Let us first consider the issue of ***black money*** control. How do you define black money models? How do you define black money? Black money may be generated even through digital system if it is captured by a corrupted agent. Black money is a flow, the avenues should be blocked. For instance, selective disclosure to near and dear ones before note ban or demonetization move may not recover a significant part of total black money. Even possible black money models may exist in digital economy in forms of non-performing assets (NPA, debt not recovered by a bank), exchange of bribe or gifts in B2B, B2C or corporate governance through multiple labels, deposit of commission in foreign bank accounts received from various deals such as high valued procurement of arms and weapons, aircraft, choppers, helicopters and submarines, investment in unknown real estates, jewelleries, stock market, foreign currency and machines, high spending on healthcare (e.g. surgical operations, organ transplantation) and high capitation fees taken for admission at technical, management and medical institutes. Is it possible to restrict black money in a digital economy through better transparency and real-time monitoring?

Next, let us consider ***corruption***. Money is not black. White money becomes black when possessed by corrupted agents and used for evil purposes. Let us look at some puzzles. Can e-payment or m-payment solve the following puzzles? Money is earned by peasants or laborers through hard work but not disclosed through banking system; is it white or black money? In case of media, information and entertainment sector, money may be earned through fake news broadcast (e.g. surgical strike, fake terror attacks; salute and musical tribute to the dummy martyrs or false data injection); music and films promoting horrors and violence or idle time pass. However, the details of earning, salary and payment are disclosed through e-payment or m-payment system. Is it not black money? Is it possible to audit corporate funding to the political parties for election? can it be allocated through election commission. Is it possible to do all transactions of political events using digital payment system? Is it possible to audit balance sheet, P/L account and expenses reports of all the political parties on regular basis? Another instance may be bio-terrorism in healthcare sector: how to restrict the flow of fund in smuggling, illegal import and export, drugs, liquor and tobacco products; money earned in open market or retail stores by selling fast food and colored soft drinks which are tasty but injurious to the health of the children. What is the fate of rural cooperative banks which may not be supplied with new currencies on regular basis and exchange is not possible against banned notes? Many rural people may not be covered under legalized banking system. Scrapped cash may be flown to the tribal zone as the tribal people are not supposed to pay tax as per the exemptions allowed by income tax laws. How can digital economy solve this loophole? So, information disclosure may not be the only ground or criteria of defining black money. It is a multi-dimensional parameter.

Next, let us consider the risk of the circulation of ***fake notes or counterfeited currencies***. Generally, number of fake notes is very small in a large cash economy (say .028%). Fake new currency notes may

be printed by the malicious agents or through neighbor attack. Even, the reserve bank of a country may admit errors in printing of new notes due to rush or heavy load on the printing machines. Is there any risk of smuggling of fake notes from neighboring countries? Is there any technological support to verify and detect fake notes at each bank? Sometimes, fake notes may be circulated or exchanged through a bank by mistakes. Even, it may be an *instance of insider attack*. For instance, Alice is an honest lady; she had withdrawn Rs. 10000 from bank A through ten number of Rs. 1000 notes. One of ten notes was fake. She paid her income tax of Rs. 5000 at bank B. Bank B detected the fake note and forced Alice to burn the fake note. Alice could not take the risk boldly to lodge complain at police station for legal action against bank A. Apparently, digital payment system should be able to mitigate this risk of fake notes. But, is it possible to generate fake e-cash in a digital economy? Computationally, it may be a simple task for a corrupted m-commerce service provider to generate and destroy e-cash without the knowledge of a dull service consumer.

Is it possible to fight against ***terrorism*** through digital payment system: how to stop terror funding through electronic fund transfer or digital payment system? How to monitor the flow of fund and cut off that link? Digital payment system is a good option but not sufficient. This problem should be solved through multiple ways such as economic policy for growth and development, poverty control, resolving unemployment problems, malnutrition, smart policing and defense set up.

Now, let us consider the issue of ***ease of doing business*** through fast, efficient and correct transaction processing system. What are the economic benefits of digital economy? It promotes the growth of electronics and communication sector: card readers, mobile phones, smart phones and digital payment service. It restricts the growth of printing, paper and banking industry; may cause lay-off and downsizing. Banning of notes may be a political move as a part of vote bank politics. But, lack of contingency plan and proper preparedness in demonetization may cause monumental mismanagement like recession, loss of revenue such as toll tax, loss of GDP (e.g. trade, agriculture, production); negative impact on export (garment, leather, logistics; wastage of perishable goods (e.g. food, flower, fruit, vegetable). Another critical issue is how to recover the cost of recycling banned notes (cost of paper, printing and labor); it may promote organized loot and legalized plundering. The public are scared of loss of economic freedom and privacy against the regulatory actions of reverse bank..

The digital payment system is expected to be a resilient system. The **resiliency** measures the ability to and the speed at which DPS can return to normal performance level following a disruption. Real-time security management involves high cost of computation and communication. The vulnerability of DPS to a disruptive event should be viewed as a combination of likelihood of a disruption and its potential severity. The administrator of m-commerce services 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? A DPS 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.

3.3 Computational Cost

Theorem 3: The cost of computation depends on the complexity of proofs of knowledge, commitments, secret sharing and digital signature or signcryption algorithms

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, Elgamal's and Paillier's cryptosystem.
Secure communication is a critical issue of mobile commerce mechanism. The basic objective is to provide confidentiality, data integrity, authentication and non-repudiation in the communication of sensitive data. *Signcryption* can ensure efficient secure communication. 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 [20].
MCM demands the support of intelligent verification options to locate errors and find faults in the digital payment system. 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.
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? The computational cost of MCM also depends on the complexity of threat analytics in terms of features and data visualization outcome.

3.4 Communication Cost

Theorem 4: The cost of communication is O(n) where n is number of m-transaction. The efficiency of MCM depends on the business intelligence and communication cost of m-commerce models significantly.

The cost of communication of the mechanism depends on several factors such as number of m-transaction, number of agents and the complexity of secure communication protocol. The business intelligence and communication cost of various m-commerce models have significant impact on the efficiency of the mechanism. In spite of the great promise, there are doubts in the business world : how long will it take to become reality from its rich potential? Is it just a hype in communication industry? Can it be a profitable business model? The current reality may have some hard edges before an efficient m-commerce mechanism [15,16].

The mobile commerce users often consider fixed line Internet experience as benchmark with m-payment applications in terms of mobile telecommunications standards, standard pricing structures and competitive intelligence. Many micro-payment systems had failed due to lack of trustworthiness, very low coverage and lack of funding until they reached a critical payment volume, inconvenient usage, lack of appropriate security mechanisms and lack of anonymity. Another constraint is high start-up and operating cost. Cost of infrastructure deployment and maintenance of infrastructure is a critical barrier against the adoption of mobile commerce service in a vast country. Many service consumers are not satisfied with speed, ease of typing in text and ease of navigation. They would like to communicate more effectively and save time. They are also worried with privacy and security concerns. High upfront investments are required to secure licenses and upgrade networks for 4G, 5G and smart phones. Lack of a clear definition of efficient business model is a major hardle for m-commerce. Mobile payment structure often complicates m-commerce marketing strategy. M-commerce market often suffers from seriously poor wireless coverage; some key factors are large land mass, low population density and low urbanization. Another important constraint is consumer's behavior - many of them are about the hype of wireless web; initial impressions are important. Fraudulent SMS messages of various advertising campaigns often create lot of confusions among the users.

However, the mobile communication technology is evolving. Mobile subscribers and service providers are now enjoying various types of facilities. Ubiquity is a critical issue, a mobile terminal in the form of a smart phone or a communicator can fulfill the need both for real-time information and for communication anywhere independent of the location of the users. Another important benefit is reachability: with a mobile terminal a user can be contacted anywhere anytime. Mobile security technology is getting sophisticated. Convenience is also important; it is an attribute that characterizes a mobile terminal. Today, the mobile devices store data, always at hand and are increasingly easy to use. Localization of services and applications can add significant value to mobile devices in terms of improved service offerings and increased revenues. Instant Connectivity to the Internet from a mobile phone is becoming a reality. Personalization is already available today. However, the emerging need for intelligent payment mechanisms combined with availability of personalized information and transaction feeds via mobile portals will move customization to new levels.

4. Conclusion

What are the top ten technology trends in the new millennium? knowledge management, customer relationship management through data mining, collaborative real time supply chain automation, content management through web mining, peer-to-peer networking, optical computing, bioinformatics, business process integration, enterprise performance management (EPM) and mobile commerce. What are the pros and cons of today's m-commerce business? Three major factors are acting behind the growth of global m-commerce business models: (a) the sharp rise in the number of mobile phone subscribers, (b) the evolution of mobile communication technology and (c) the rapid development of mobile devices. The rapid advancement of mobile communication technology and mobile devices is the key driver for the increasing sophistication of the mobile market. Our society needs a mix of intelligent options such as cash, e-payment and m-payment systems. The common people should be able to use various options flexibly to meet their needs. This work finds a set of interesting research agenda for future : (a) explore new cryptographic concerns in m-commerce 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, (e) how to quantify and code miscellaneous security intelligence parameters? (f) Are the strategic moves considered in the mechanism are enough to ensure robust

security and stability of m-commerce services? (g) Is it possible to improve the cost of computation and communication of the cryptographic protocols? (h) It is interesting to develop efficient financial cryptographic tools for the mobile commerce mechanism to resist corruptions, black money and fake or counterfeit currencies apart from ease of doing business by ensuring accountability and transparency.

References

1. O.Goldreich. 2007. Foundations of Cryptography: Volume 1, Basic Tools. Cambridge University Press.
2. O.Goldreich. 1998. Secure multi-party computation.
3. W.Du and M. J. Atallah. 2001. Secure multi-party computation problems and their applications: a review and open problems. In 2001 workshop on new security paradigms (pp. 13 - 22). ACM Press.
4. Y. Lindell. 2003. Composition of secure multi-party protocols a comprehensive study. Springer.
5. 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.
6. Y. Dodis and T. Rabin. 2007. Cryptography and Game Theory. In Algorithmic Game Theory. Cambridge University Press.
7. G.Asharov, R.Cannetti and C.Hazay. 2014. Towards a game theoretic view of secure multiparty computation. Eurocrypt.
8. J. Katz. 2008. Bridging Game Theory and Cryptography: Recent Results and Future Directions. In 5th TCC, Springer-Verlag (LNCS 4948), pages 251-272.
9. G. Kol and M. Naor. 2008. Games for exchanging information. In 40th STOC, pages 423-432.
10. 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.
11. S.D.Gordon and J.Katz. 2005. Rational secret sharing revisited. ACM Electronic Commerce'05.
12. S.D.Gordon, K.Hazay, J.Katz and Y.Lindell. 2008. Complete fairness in secure two party computation. STOC'08.
13. J.Halpern and V.Teague. 2004. Rational secret sharing and multi-party computation : Extended abstract. STOC'04.
14. S. Chakraborty. 2001. Mobile commerce. Summer Project Report. Fellow Programme, Indian Institute of Management Calcutta. India.
15. Mobile commerce winning the on-air consumer. BCG report. November'2000. .
16. U. Varshney, R.J.Vetter and R. Kalakota. 2000. Mobile commerce: a new frontier.
17. 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.
18. D. R. Stinson. 2005. Cryptography: Theory and Practice. Chapman and Hall/CRC.
19. W.Mao.2003. Modern Cryptography : Theory and Practice. Prentice Hall.
20. Y.Zheng. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption). LNCS 1318, Springer-Verlag.
21. T.P.Pedersen. 1991. A threshold cryptosystem without a trusted party. In D.W.Davies, editor, Advances in cryptology – Eurocrypt'91, pp. 522-526, Berlin,LNCS volume 547, Springer-Verlag.
22. A. Shamir. 1979. How to share a secret. Communiation ACM, 22(11):612-613.
23. R. Párhonyi et al. 2005. Second generation micropayment systems: lessons learned. In Proceedings of the Fifth IFIP Conference on e-Commerce, e-Business, and e-Government. Poznan.
24. R. Párhonyi et al. 2006. The fall and rise of micropayment systems. In T. Lammer, editor, Handbuch E-Money, E-Payment & M-Payment. Physica-Verlag.
25. D.Chaum. 1988. Privacy Protected Payments: Unconditional Payer And/or Payee Untracability. Smartcard 2000, North Holland.
26. S. Brands. 1993. An efficient off-line electronic cash system based on the representation problem. Technical Report CS-R9323 1993, Centrum voor Wiskunde en Informatica.
27. J. Camenisch, S. Hohenberger and A. Lysyanskaya. 2005. Compact e-cash. In Advances in Cryptology: EUROCRYPT 2005, volume 3494, pages 302-321, Aarhus, Denmark. Springer-Verlag.
28. M.Belenkiy, M. Chase, M. Kohlweiss and A. Lysyanskaya. 2008. P-signatures and noninteractive anonymous credentials. In Theory of Cryptography, volume 4948, pages 356-374, New York. Springer-Verlag.
29. B.Schoenmaker. 1998. Security aspects of the ecash payment system. State of the Art in Applied Cryptography, 1528:338-352.
30. D. Abrazhevich. 2001. Classification and characterization of electronic payment systems. In K. Bauknecht et al., editors, Proceedings of Second International Conference on E-Commerce and Web Technologies, LNCS 2115. Springer-Verlag.
31. N. Nisan and A.Ronen. 1999. Algorithmic mechanism design. In 31st Annual ACM symposium on Theory of Computing (STOC), pp 129 -140.