Credit Card Counterfeit Recognition with Location Based Tracking System

Mrs. G. K. Sandhia
Assistant Professor
Department of Computer Science and Engineering
SRM University
Chennai, Tamil Nadu

Ms. P. Nandhini
Department of Computer Science and Engineering
SRM University
Chennai, Tamil Nadu

***Abstract*— Mobile networks are driven by the need to provide more advanced services to mobile or nomadic computing devices like security services requiring remote client authentication. The user's location might be used as authentication factor, in addition to the typical authentication factors. The location information itself is subject to forging attacks, additional mechanisms must be used to certify its integrity. Location Remote Authentication Protocol which is a novel protocol combining several authentication factors to securely authenticate a mobile user where the user's location can be determined and its correctness is certified by a third trusted party called Local Element. Location based verification scheme is implemented by comparing the user's credit card location with the user's mobile location through Global Positioning System which intimates to user mobile with automated specific key Short Message Service. It is very effective to identify the real user and resist the involvement of unauthorized attacks by fake user.**

Keywords—Local Element, Location Remote Authentication, Point of Sale, Location Detection

I. Introduction

Network securityconsists of the provisions and policies adopted by the network administrator to prevent and monitor the unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID (identification) and Password or other authenticating information that allows them access to information and programs within their authority.

Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises and other types of institutions for security and for more usage by the users with sequential information in it.Most RFID (Radio Frequency Identification) tags do notcontain any data after they are manufactured andthey are similar to a blank label waiting for information to be printed on them. To place information in the tag, an RFID encoder must be used. One of the most popular methods of encoding is with an RFID Capable Label Printer that has a built-in encoder and RFID Capable Barcode Label Software.

Class 0 - these RFID tags are similar to license plates in that they are read-only, and are encoded with data when they are manufactured. Class 1 - these RFID tags allow us to write the data in the tag and are usually one-time programmable (OTP). These are available in either HF (High Frequency) or UHF (Ultra High Frequency) versions and are known as GEN1. Class 1 GEN2 EPC (Electrically programmable code) - these RFID tags are the latest type of UHF tag and are most referred to in this document shown in table 1. They are also the tags required for mandates by various suppliers such as Wal-Mart and the US Department of Defense (DOD). In the automation identification industry, we refer to these tags simply as GEN2. These tags are 96 bits or larger and contain advanced features, such as lock after write and CRC (Cyclic Redundancy Code) read verification.

TABLE 1.RFID STANDARDS

STANDARDS	USAGE
ISO10536(ISOSC17/WG8)	Close coupled cards
ISO1444(ISOSC17/CG8)	Proximity cards
ISO15693(ISOSC17/WG8)	Vicinity cards
ISO10373(SC17/WG18)	Identification cards
ISO11785(ISO23/WG19)	Radio regulation stamps
ISO18001(SC31/WG4)	Application profiles

GPS (Global Positioning System) receiver calculates its position by precisely timing the signals sent by GPS satellites high above the Earth. Each satellite continually transmits messages that include the time the message was transmitted and the Satellite position at time of message transmission. The receiver uses the messages it receives to determine the transit time of each message and computes the distance to each satellite using the speed of light. Each of these distances and satellites locations defines a sphere. Each Global Positioning System satellite continuously broadcasts a navigation message on L1 C/A and L2 P/Y frequencies at a rate of 50 bits per second. Each complete message takes 750 seconds (12 1/2 minutes) to complete. The message structure has a basic format of a 1500-bit-long frame made up of five sub frames, each sub frame being 300 bits (6 seconds) long. Sub frames 4 and 5 are sub commutated 25 times each, so that a complete GPS message format requires the transmission of 25 full frames where each sub frames has separate sub frame descriptions in it.

Each sub frame consists of ten words, each 30 bits long. Thus, with 300 bits in a sub frame times 5 sub frames in a frame times 25 frames in a message, each message is 37,500 bits long. At a transmission rate of 50 bits, this gives 750 seconds to transmit an entire almanac message. Each 30-second frame begins precisely on the minute or half-minute as indicated by the atomic clock on each satellite ID products.

II. ANALYSIS OF EXPRESS KEY IN CREDIT CARD VERIFICATION

Credit card fraud is the common existence problem due to less security against authentication for transactions.With an increase usage of credit cards for online purchases as well as regular purchases, causes a credit card fraud. In the mode of electronic payment system, fraud transactions are rising on the regular basis. The user's mobile number is used for providing security and authentication. Based upon the user's information a key is generated and sent to user's mobile for payments. Even though the intruders track the secret details of card and card holder, major security is provided.

Various methods with a variable degree of reliability are typically employed in credit cards using RFID tags [4] and GPS. In the proposed system by Location Remote Authentication Protocol, the user's location can be determined and its correctness is certified by a third trusted party, called Local Element. Location based Verification Scheme is implemented by comparing the User's Credit Card Location with the User's Mobile Location. The Proposed system is to generate an Encrypted Data to the Real User's Mobile Number along with the Decrypting Key as SMS (Short Message Service).

The proposed method ensures with the available additional security at the time of user transaction. It guides the reliable and trusted approach for the envelopment of secure transactions with the following services.

1. GPS services
2. One time tokens (Static Passwords)
3. Decrypted SMS (express key)

A. Structure of Key Elements

The GPS OPS (Operation Program System) represents a critical part of GPS modernization and provides significant information assurance improvements over the current GPS OPS program.

- OPS will have the ability to control and manage GPS legacy satellites as well as the next generation of GPS III satellites, while enabling the full array of military signals.
- Built on a flexible architecture that can rapidly adapt to the changing needs of today's and future GPS users allowing immediate access to GPS data and constellations status through secure, accurate and reliable information.
- Empowers the war fighter with more secure, actionable and predictive information to enhance situational awareness.
- Enables new modernized signals (L1C, L2C, and L5) and has M-code capability, which the legacy system is unable to do.
- Provides significant information assurance improvements over the current program including detecting and preventing cyber-attacks, while isolating, containing and operating during such attacks.
- Supports higher volume near real-time command and control capabilities and abilities.

The key elements are arranged with the message format of satellite sub frames. Each sub frames has its own numerical bits with their GPS and Satellite orbit sequences. The significant orbital sequences numbers are ordered based upon their sub frames with their perceptual functionalities are which is shown in table 2.

TABLE 2.GPS MESSAGE FORMAT

SUBFRAMES	DESCRIPTION
1	Satellite clock Time relationship
2-3	Ephemeris (precise satellite orbit)
4-5	Almanac component (Satellite network synopsis, error connection)

The ephemeris is updated every 2 hours and is generally valid for 4 hours, with provisions for updates every 6 hours or longer in non-nominal conditions. The almanac is updated typically every 24 hours. Additionally, data for a few weeks following is uploaded in case of transmission updates that delay data upload.Express key elements are those in which the encrypted and decrypted messages are modulated and RSA, DES (Data Encryption Standard) algorithm techniques are applied. It also includes the LRAP (Location Remote Authentication Protocol) and Location detection technologies in it.

III. ALGORITHM AND METHODOLOGY EMPOWERED FOR COUNTERFEIT RECOGNITION

A. Location Detection Algorithm

Location positioning using cellular broadcast towers can be used on cell phones with GPS modules. It is a location sensing prototype system that uses active RFID tags for locating objectsinside buildings. Also it proposes a user activity assistance system thatemploys a state sequence description scheme to describe the user's contexts. It depicts a navigation and location determination systemfor the blind using an RFID tag grid sensors [5]. It uses the basic parameters for processing location and detection issues which is explained in table 3.

TABLE 3.PARAMETER DESCRIPTION

PARAMETERS	**DESCRIPTION**
$event_i$	i^{th} access event
C_{id}	C_{id}=Card ID($event_i$)access Card ID of i^{th} access event
AP_i	AP_i=access point($event_i$)access point of i^{th} access event
Threshold	Normal maximum allowable with number of repeated access
Acc min	Normal minimum allowable duration for a sequence of repeated access

Let timestamp (AP_i, C_{id}) be the function which returns the timestamp of the ith detected access point of the person holding card C_{id}. Let location (AP_i)is the function which returns the location of the i^{th} access point, and let maxStay (loc, C_{id}) be the function which retrieves the predefined maximum duration that the person holding card C_{id} is allowed to stay at the location loc.

B. Methodologies applied

A sequential change of points in detection procedure is aiming to detect changes of specific metrics in two ways such as Provide simple threshold values and TLD framework.

$$L\ (threshold) = \sum (p(x, z)\ |\ threshold)\ p\ (threshold)$$

Wherex, z - node parameters, p – position, L-location.

C. LRAP – Location based Remote Authentication Protocol

LRAP is a secure location-based remote authentication protocol which can be used to authenticate the remote users in mobile environments. LRAP is based on the use of “classical” authentication methods (like the static passwords and the one time passwords) combined with user location information at one time. To verify the integrity of the location data, LRAP exploits a dedicated component, named Local Element (LE). They implemented an LRAP-based service involving payment with the mobile devices at the gas stations. Fully compliant with ISO7816-4 and support T=0 protocol, fully compliant with Java code 2.2, Global Platform 2.1.1 EEPROM on card: 36K bytes, RSA algorithms: 512bits/1024bits/2048bits, DES algorithms: include standard DES and Tri-DES algorithm, Hash algorithms: SHA1, Hardware Certification: EMVco, CC EAL5+ high.

D. ODK (Open Data Kit) GPS Hybrid Systems

Hybrid positioning systems use a combination of network-based and handset-based technologies for location determination. One example would be some modes of Assisted GPS, which can both use GPS and network information to compute the location. Both types of data are thus used by the telephone to make the location more accurate (i.e. A-GPS). Alternatively tracking with both systems can also occur by having the phone attain his GPS location [3] directly from the satellites, and then having the information sent via the network to the person that is trying to locate the telephone. The technology of locating is based on measuring power levels and antenna patterns [10] and uses the concept that a mobile phone always communicates wirelessly with one of the closest base stations, so knowledge of the location of the base station implies the cell phone is nearby.

IV. OVERVIEW OF RECOGNITION

The basic architecture establishes the basic structure of the computer system, defining the essential core design features and elements that provide the framework for all that follows, and are the hardest to change later. The systems architect provides definition of the user vision for what the system needs to be and do, and the paths along which it must be able to evolve, and strives to maintain the integrity of that vision as it evolves during detailed design and implementation.

User provides Login User Name and Password once the card is swiped. Organization requests server for details. LE (Local Element) gives Transaction time, location information of mobile and card to Service provider. After verification SP (Service Provider) send this encrypted and decrypted code as SMS to the client. In the same way it sends decrypted key to organization.The client receives one time encrypted code in his/her mobile from service provider which is used for further secure transaction.

The secure novel approach for trusted transaction achieved with the GPS [4] enabled mobile and organization server where the transaction and the verification are done under sequential manner. Information retrieval with user data and location values of mobile with credit card of the user is transferred simultaneously to the user mobile and organization server for verification purposes.

Based on the need of requirement by server for user verification the service provider gets the user mobile location and card location value from a novel analyzer called Local Element is shown in Fig.1. Local element traces the location by using GPS (Global Positioning System) enabled service in user mobile and satellite communication system for card location.

Express key Architecture depicts the overall process of credit card counterfeit recognition using advanced features and it also employs the model of express key review for transactional behavior

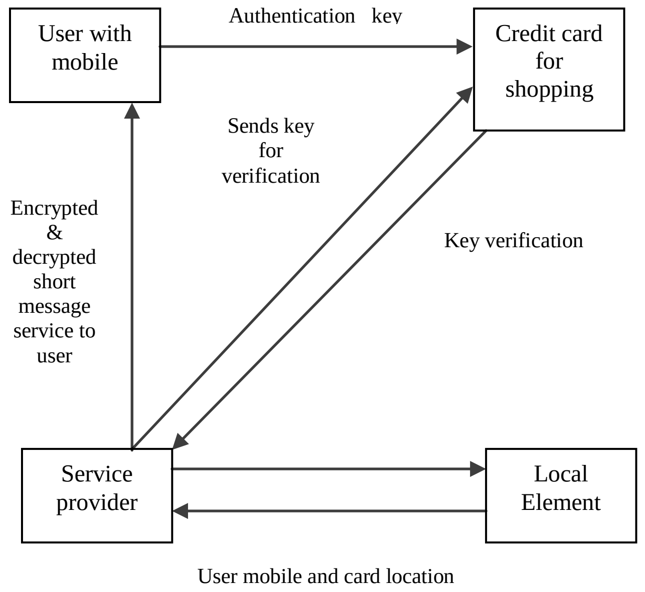
User with mobile
Authentication key
Credit card for shopping
Sends key for verification
Encrypted & decrypted short message service to user
Key verification
Service provider
Local Element
User mobile and card location

FIG. 1.SYSTEM ARCHITECTURE

A. key generation

- Mobile Client Authentication
- Locale Of Credit Rating
- Service Provider Value
- Location Detection
- Express Key Handover

Client provides Login User Name and Password. Then the card is swiped by the client. This starts one time encrypted code generation [8] process in service provider, where the location of the user is identified using Local Element. The code (encrypted key) is received by client mobile. The client enters key in credit institution to perform transaction. If new user uses his/her card should register with the essential data's to the server for future transactions and verifications.

The Place of purchasing a product and make payment through it. It receives Decrypted key of client from Service provider. Here the key is typed by client. By which further transaction is carried out only when key is valid for secured transaction. The card swiping and transaction verification is performed in order to achieve security under organization server.

Service Provider gets card number from client, user terminal position and their information using local element. Then generates one time encrypted code for that information and send SMS (Short Message Service) this code to the client. In the same way it sends decrypted key to organization for verification. Service provider requests for user information with mobile location from local element which in turn gets the location value obtained by different access patterns.

Local Element accesses to global navigation satellite system data, by dedicated connection to GPS (Global Positioning System) Reference Stations [4], and can exploit all the functions and data available in the mobile operator Network from the network database. The information is given to Service provider, since key generation in service provider needs Transaction time, location information.

The client receives one time encrypted and decrypted code in his/her mobile from service provider. The key is entered in organization. Only when the key is authenticated by organization server further transaction can be done.

V. TRACKING PRELIMINARIES FOR RECOGNITION

The development of a logical mathematical model to formulate a knowledge base of suspicious and irregular actions is implemented.Based on the model, a real-time suspicious access pattern detection prototype is proposed which allows rapid alert and reaction to irregular behavior. Given the lack of availability of secure access event data, an access event generator for physical environments has been developed. It defines the following four suspicious patterns:

i. Temporal pattern: an unusually long period of stay by a person in a given area.

ii. Repetitive access pattern: unusual repetitive accesses within a given period of time.

iii. Displacement pattern: consecutive accesses to distinct but distant neighbouring locations within an unusually short period of time.

iv. Out-of-sequence pattern: consecutive accesses in an undefined sequence.

A. Detection of Temporal Pattern

Let timestamp (AP_i C_{id}) be the function which returns the timestamp of the i^{th} detected access point of the person holding card C_{id}. Let location (AP_i) be the function which returns the location of the i^{th} access point, and let maxStay (loc,C_{id}) be the function which retrieves the predefined maximum duration that the person holding card C_{id} is allowed to stay at the location loc.

C. Detection of Repetitive Pattern

The detection of the repetitive pattern focuses on access events detected from a pair of access points (sensors) installed at two opposite sides of a GPS receiver module. In addition, two conditions must hold for a repetitive pattern:

- The total number of repeated accesses should be greater than the predefined threshold.
- The total time spent during the repeated accesses must be shorter than the minimum allowable duration for a sequence of normal repeated accesses. First, the system derives the total number of repeated accesses from the last detected access event.

Let timeSpent (APx;APy) be the function that returns the time spent by the person when accessing point *y* after accessing *x*. Therefore, the total time spent by the person for the previous access sequence can be denoted as timeSpent ($AP_i \leq 4$; AP_i). Based on these functions the algorithm for detecting repetitive access patterns as follows:

```
for all new detected event$_i$ do
if (repAccessCount($AP_i$) >= repThreshold) and
```

```
    (TimeSpent ($AP_i$;$AP_2$ (repAccessCount ($AP_i$))) <
repAccMinDuration) then
    pattern =”Repetitive"
    Else
    Pattern = “Normal"
    End if
    End for
```

D. Detection of Displacement Pattern

LetminMove (AP_i<1; AP_i) be the function which returns the minimum time required to travel from ($i \leq 1)^{th}$ access point to i^{th} access point.

E. Detection of Out-of-Sequence Pattern

A pattern is considered to be out-of-sequence when it is detected that a person attempts consecutive accesses to two distinct locations whereby the second location is unreachable from the first one. Let its Neighbor ($AP_i \leq 1$; AP_i) be a Boolean function which returns true if AP_i can be reached from $AP_i \leq 1$.

Using the above four detection algorithms, a security system may decide to detect the location when card access pattern is detected. However, in some situations a sequence of access events may not be considered suspicious as its degree of suspicion does not exceed pre-defined threshold values. For instance, the total number of repeated accesses by a person may not exceed the limit and hence the system may not find the access. In such cases, the system may not be able to detect cases minimum transaction. The prediction of future possible minimum cost access patterns would be a straightforward extension of location detection algorithms.

To detect these patterns in collected data, the detection algorithms can be used in an existing physical environment that has surveillance sensors installed.Data analysis and mining algorithms can be applied to this data to discover abnormal and suspicious activities among the considerable volume of data. Recent development of RFID technology [3] enables tiny contact-less tags for physical object tracing and re-tracking. Practical implementation of object movement identification and registration becomes feasible, simple and convenient.

VI .CONCLUSION

The concluded concepts portrays how the Credit Card Forgery Identification system with location based tracking using mobiles with GPS(global positioning system)works and avoids the unauthorized access of credit cards even if the user lost his/her credit card. The analysis shows that the work satisfies all security requirements and has several other practice-friendly features. The future work is to fully identify the practical threats on Credit Card Forgery Identification protocol and develop concrete five- factor authentication protocols with better performances.

REFERENCES

[1] Alexei Czeskis, Karl Koscher, Joshua Smith.R, Tadayoshi Kohno, **“**RFIDs and Secret Handshakes: Defending Against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications”, *CCS’08, Alexandria, Virginia, USA. ACM 978-1-59593-810-7/08/10, October 27–31, 2008(www.alhea.com/net basics of network attacks).*

[2] Di Ma, Nitesh Saxena, Tuo Xiang, and Yan Zhu,”Location-Aware and Safer Cards: Enhancing RFID Security and Privacy via Location Sensing*”, Proc. of Euro SSC 2007, LNCS 4793, pp. 93-109, March/April 2013.*

[3] Gerhard Hancke.P, Markus G. Kuhn**,** “An RFID distance bounding protocols”, *Proc. of ACM CCS 2006, pp. 168-178, Proceedings of IEEE/Create-Net SecureCom ,Athens, Greece, pp. 67–73. IEEE Computer Society Press, Los Alamitos,California, USA, ISBN 0-7695-2369-2, 5–9 September 2005.*

[4] Kwak.H.J, Son.K, Lee.W, Kim.S, and Won.D, “Confidence Value Based Multi Levels of Authentication for Ubiquitous Computing Environments*”, Proc. of ICCSA 2006, LNCS 3981, pp. 954-963.*

[5] http://www.cs.princeton.edu/bfactors/research.html (Two-Factor Authentication communication reference).

[6] Michael Buettner, Richa Prasad, Matthai Philipose, DavidWetherall,”Recognizing Daily Activities with RFID-Based Sensors”,*USP 6,466,200, issued by Innalabs, Inc., Potomac Falls, September 30-October 3, 2009.*

[7] http://www.privacies.com/products/index.html (Privacies and ID products reference).

[8] Selwyn Piramuthu, University of Florida, Gainesville, Florida 32611-7169,”HB and Related Lightweight Authentication Protocols for Secure RFID Tag/Reader Authentication”,*Collector Europe Conference, Basel, Switzerland, 9-10 June 2006.*

[9] Weister.M and ilex, “Protecting Privacy in Continuous Location-Tracking Applications*”, IEEE Security & Privacy Magazine, Vol. 2, Issue 2, pp.28–34,April 2004 (www.web4gps.co.uk/ org concepts of GPS).*

[10] Zheng.D and Ning.P, “Location-based pairwise key establishments for static sensor networks”, *Proc. of the 1st ACM workshop on Security of ad hoc and sensor networks, Fairfax, Virginia, pp. 72-82, 2003.*