ISSN: 0976-3104
SPECIAL ISSUE Emerging Technologies in Networking and Security (ETNS)
Menaka et al.

THE IIOAB JOURNAL

ARTICLE OPEN ACCESS

NEW APPROACH FOR TRACING STOLEN LAPTOP AND DATA PROTECTION

Menaka, Subashree, Narendran
Dept.of Computer Science and Engineering, SRM University, Chennai, INDIA

ABSTRACT

Aims: *Around the world everywhere, everyday many laptops are keep on stolen by strangers. It's been a critical issue since the laptops may have the confidential data, files or some personal info as well. Letting such information's to strangers will lead unexpected events. Tracing such laptops and the strangers is the big issue in the computing world. Many solutions provided by the many vendors but none of them really resolve this issue. Many of them require external intervention; require expensive additional hardware's like GPS, Hardware Lock, point-point sensors key servers etc.* ***Results:*** *This paper provides a new approach for Tracing the Stolen Laptops, suggesting a solution which does not need any additional resource.* ***Conclusion****: It is useful for tracing the location of the laptop, identity of stranger (captures image and video), protecting the content by locking the Laptop etc.*

Published on: 28th– August-2016

KEY WORDS

Laptop, Trace, GPS, IP address, MAC address, Hardware Lock, Sensors

***Corresponding author: Email:** menanand7@gmail.com

INTRODUCTION

As per FBI, in 2005 laptop theft causes $3.5 loss. The Computer Security Institute (CSI)/FBI Computer Crime & Security Survey, they found that the average theft of a laptop to cost a company $31,97[1]. The survey done by 325 private and public organizations which is published by Intel in 2010 says 10% of Employee laptops were before the laptops usefulness lifespan [2]. Average total negative economic impact of a due to laptop theft was $49,256 due to data stealing. The cost of laptops lost for the organization is $2.1 billion [3]. In US, 28% of $48bilion total lost in economy is due to data breaches in stolen laptops and other mobile devices[4].The NSW Bureau of Crime Statistics and Research prepared a report which states that laptop theft has been increased in last 10 years. The laptops were stolen for the cost initially, but now a day it has been stolen for accessing the data inside them. Most of the laptops are stolen during the travelling at train, hotels/motels, airports, taxi cars, and public gathering events.

It is necessary to protect laptops being stolen since it leads vulnerable effects. For the business people lose of laptop is lose of their business, since the business information's which is confidential shouldn't be leaked to others. For example, the information regarding the tenders, project business logics are highly confidential, those are not sharable or exposed to others. The private personal photos, videos are another secret set of things not sharable or exposed outside. So what is more important, tracing Laptop? Or protecting data in it? Most of the people will say both for this question.

Many solutions exist for protecting the laptop being stolen, protecting the data in them, tracing the laptop even it has been stolen by any. These solutions use various techniques like GPS, hardware locks, point-point tokens, inside data protection, centralization of data and WiFi based etc. Next section in this paper give brief about the techniques listed here.

RELATED WORKS

Many researches have been done for preventing laptop theft, protecting data inside and tracing the stolen laptop. Still many working on improvising the existing solutions and to develop a new solution. But very few among them really protects the laptop from thief, protects data and trace stolen laptop.

Basic Security

The security can be provided simply by using any of the following ways

THE IIOAB JOURNAL
ISSN: 0976-3104

- Pre-boot authentication

  Authenticating users of Laptop by asking username and password before the boot up, (i.e) verifying user even before Operating System launched[5]. This will be useful for completely protecting the Laptop data.

- Disk Encryption

  Encrypting the entire disk from un-authorized access is another solution for data protection [6]. Using this one can access the data in a disk only after the authentication.

- Locks
  Varieties of Laptop locks are available to protect it physically from strangers. These locks are available in market to lock the Laptop in a physical location to make it immovable.

Laptop Tracking Software's

The methods specified above are used for protecting the data but they are not sufficient since many advanced security attacks will breach the data security. We need a solution need to protect the data as well as prevent the Laptop from stolen and track them even if it has been stolen.

This section describes some of the solutions for tracking the stolen Laptops.

- Tracking Laptop using Adeona

Adeona [7] is one of the Laptop Tracking solution for tracing the stolen laptop, it works on two step process. First the Tracking software needs to be installed later the recovery software. The tracker keep on send some data which used by the recovery software to analyse those data and predict its geo graphic location.

If at one point your laptop gets stolen and is connected to the internet, the Adeona will send you criminal's IP address. The IP address can then be retrieved using the Adeona Recovery Wizard. Knowing the IP address is enough in most cases to track the geographical location of the device.

Unlike similar commercial tools, Adeona is decentralized and doesn't store your password on its servers. It means no one besides the owner can use Adeona to track your laptop.

- Computrace Lojack for Laptop

It is another Laptop recovery tool brings back the lost or stolen laptop. It keeps working in background. When the laptop lost or stolen has to be reported to the Computrace team, they will trace it with the help of the tool installed in Laptop. Before reporting the lost or theft to the computrace it is mandatory to give a police complaint and the complaint copy is needed.

- MyLaptopGPS

Similar to above mentioned products it is used for protecting data as well as tracking it. It has an exclusive feature which allows us to re-encrypt the data with new encryption key in a Laptop even after lost. It is useful for encrypting even the USB devices, thump devices etc.

Other Related Works

Transient Authentication [8] force the user to use of wearable token that constantly attests to the user's presence. When the user departs, the token and device lose contact and the device secures itself. The small, lightweight nature of mobile devices, combined with their common usage environments (in public places, amid many un authenticated people) makes them an easy target for theft. More important than loss of hardware may be the cost of information exposure. To overcome problem using Wearable hardware token provides authentication and security using wireless communication.

A boot system that uses a U-Key [9] can help ensure the integrity of fairly static PC components. The U-Key approach is designed both to provide boot integrity and to enforce access control. The basic idea is that the host computer actually boots from a USB disk loaded with the operating system and the loader. Smart card is a secure way to store certificates and keys. Along with hardware tokens, smart cards deliver user benefits in four major areas: easy portability of user credentials, drastic simplification of platform, better protection of personal credentials and a higher level of personal privacy.

Role Based Access control in location based services (LBS) using the methodology GEO-RBAC [10]. a location based technique for with access control. These approaches are referred to as user-driven and event-driven respectively. Under the user-driven approach the position of the user is checked only upon an access request; conversely under the event-driven approach the position of the user is tracked so that the set of enabled roles can be changed dynamically and transparently with respect to the user. The conclusion of this project using this approach the access to certain features can be restricted based on current location. Computer vision applications for mobile phones are gaining increasing attention due to several practical needs resulting from the popularity of digital cameras in today's mobile phones. The face and eye detection [11]. modules are implemented and running quite well. For simplicity, they are trained using Haar-like features and AdaBoost.The main advantage of using Haar-like features is their low computational cost. However, the discriminative power of such simple features is limited.

THE IIOAB JOURNAL ISSN: 0976-3104

2D-Barcode Processing solution [12]. to support mobile applications and 2D Barcode Applications in M-Commerce, Using barcodes for providing mobile security. It is clearly understood that barcodes can be used to hide security information's which can be read only through bar code reader. The future work of this research includes two areas: a) to enhance the existing 2D barcode solution to deal with non-perfect 2D barcode images, and b) building a 2D barcode enabled mobile payment system. From the conclusion of this paper it is clearly understands that barcodes can be used to hide security information's which can be read only through bar code reader.

PCA & LDA based teeth-image personal identification method [13]. in this, the teeth image failed from the matching in the PCA & LDA based system is reconsidered by feeding back the image to eliminate the reflection and the rotation problems. In the experiments, 500 teeth images are tested with 200-teeth database. The results revealed that of the 10% errors caused by the two problems, 5% are correctly identified because of the proposed method. A method for improving a teeth image personal identification was proposed.

Multimodal biometric authentication approach using teeth image and voice as biometric traits [14], this method is evaluated using 1000 teeth images and voices, in which these are collected by smart-phone, i.e., one mobile device for 50 subjects. In this paper, the Ada Boost algorithm is used based on Haar-like features for teeth region detection, and the EHMM algorithm with 2DDCT as feature vector is additionally accommodated in process of teeth authentication.The proposed multimodal biometric authentication system exhibits an EER of 2.13%. Thus confirm that the performance of the proposed system is better than the performance obtained using teeth or voice individually.

TrustVisor [15], a special-purpose hypervisor that provides code integrity as well as data integrity and secrecy for selected portions of an application.TrustVisor achieves a high level of security. The protection granularity in these systems is too coarse to provide strong security properties, because the entire application is in the TCB. Dynamic Root of Trust for Measurement (DRTM) mechanism provides memory protection from DMA accesses, and integrity measurement of the launched code before it executes. TrustVisor is a small hypervisor that enables isolated execution of Pieces of Application Logic (PAL) with a TCB containing only the TrustVisor runtime and the PAL itself. This system enforces code and execution integrity, data secrecy and integrity for PALs. TrustVisor supports unmodified legacy OSes and their applications.

“Mobile User Location-Specific Encryption (MULE): using your office as your password [16]. Data breaches due to stolen laptops are a major problem. The goal of this work is to provide encryption of sensitive data while requiring minimal administrative effort and zero user effort during common accesses and moderate effort otherwise. The proposed system allows access to restricted files only from specific location. This approach is to use information and services available only in a trusted location to assist in key derivation without user involvement and without authenticating the laptop to any outside service. In this paper, the Home Key Derivation and Corporate Key Derivation protocols are designed which allow a laptop to automatically derive the key needed to access sensitive files based on a location.

Keypad [17], an auditing file system for theft prone devices, such as laptops and USB sticks. This paper described Keypad, an auditing file system for loss- and theft-prone devices. Keypad provides users with evidence that sensitive data either was or was not accessed following the disappearance of a device. Keypad achieves its goals through the integration of encryption, remote key management, and auditing. It demonstrates the advantage of separating encryption and key management to enforce auditing for mobile device data. If data was accessed, Keypad gives the user an audit log showing which directories and files were touched, and also allow users to disable file access on lost devices, even if the device has been disconnected from the network or its disk has been removed.

Intelligent anti-theft and tracking system for automobiles [18]. a system for preventing the automobile theft since Vehicle theft is a serious issue around the entire earth. So an efficient solution is needed to track them. The vehicle owners use lot of approaches to safeguard their vehicles providing a lock, SMS alert when a vehicle start, alarm when a vehicle start apart from the owner etc., This paper provides a solution using GPS receiver, Google Earth and SMS. Using GPS device the current location of a vehicle can be obtained, which can be sent to the owner through the SMS and the using the co-ordinates the vehicle can be tracked using Google Earth.

BACKGROUND

The works described in previous sections having several shortfalls. This section will give a brief background about the new approach proposed in this paper.

Idea Behind

The solution proposed in this paper is to trace the stolen laptop using its current IP address and MAC address. It’s known to every one that the IP address is unique and using IP address we can trace the person using that IP address. The Internet Service Providers (ISP) providing internet services to any System using Mobile or Telephone lines. So it is clearly understand that every IP address is mapped on any of the Mobile number or Telephone number. So if we know the IP address, we can know the telephone or mobile number through which the system is connected. Using the telephone or mobile number we can know the person who is using the connection. This is the idea behind this solution. Apart from this identity, the photo of the person will help to trace him/her. Even If the photo is not clear the video will be useful. At least in a single frame the identity of a person can be found easily.

New Approach in Tracing & Protecting

THE IIOAB JOURNAL
ISSN: 0976-3104

The new approach described in this paper is aimed at tracing the stolen laptop and restricting access to the files so that preventing data expose to others. In this, Laptop tracing is done with the help of IP Address and file protection is done using OTP (One Time Password).

IP addresses are the unique ID assigned to every system connected in a network which is used for communication between systems. If a system or laptop is connected in an Internet the IP address is assigned by the ISP. Usually the IP addresses are static or dynamic. The static IP addresses are fixed permanent IP assigned to a specific connection. i.e. Whenever the connection established between from the system through a specific connection always the same IP address will be assigned.

The next kind of IP addresses are dynamic IP address i.e. the IP address of a system connected using the specific line will change or not same for all sessions.

Globally region wise the IP addresses are allocated and managed by IANA (Internet Assigned Numbers Authority) which allocates IP addresses among following five Regional Internet Registries (RIR):

- African Network Information Centre (AfriNIC) for Africa
- American Registry for Internet Numbers (ARIN) for the United States, Canada, several parts of the Caribbean region, and Antarctica.
- Asia-Pacific Network Information Centre (APNIC) for Asia, Australia, New Zealand, and neighboring countries
- Latin America and Caribbean Network Information Centre (LACNIC) for Latin America and parts of the Caribbean region
- Réseaux IP Européens Network Coordination Centre (RIPE NCC) for Europe, Russia, the Middle East, and Central Asia

Each of the above RIR responsible for assigning and managing IP addresses in the specific region of the world. The next level allocation is done by these RIR's, these allocations include allocating IP for the ISP's in that regions, educational, government organization and large level private organizations.

PROPOSED WORK

The idea proposed in this paper is to trace the Laptop using its current IP address also protecting the data in it by making the laptop unusable once it is found missed or stolen. The proposed work having two main objectives, one is to find the IP address if it is stolen another is to protect the data.

Find IP address of a stolen Laptop

As specified in the previous section the IP address of the System no matter whether it is a Desktop PC or a Laptop is always unique one. So if the Laptop is missed the Tracer Located inside will fetch current IP address and check whether it is matched with the exiting stored IP address. If it is matched with the existing IP address it concludes that the Laptop is still with the Owner and is not missed. Whereas if the IP addresses doesn't match it is clearly indicates that the Laptop is moved to another network or location.

It is possible that the Laptop user/owner can use his Laptop anywhere wherever he/she goes. He may use it in his home, or in travel, in an office, in public gathering like malls, airports, railway stations etc. Everywhere he connects his laptop in different network using wireless (WiFi) or wired connection with different IP address.

So it is necessary to differentiate whether the Laptop has been stolen or it is used indifferent place with different IP address by the owner. In both the cases the tracer will fetch the current IP address, compare it with stored IP address. If the doesn't match sends the new IP address as a mail to the registered mail ID of the owner. This IP address is useful to trace the current location.

Apart from sending the IP address the photo image and video of the current user taken using web cam will also be send along with the IP in a mail as an attachment. This photo will be useful to trace the person who is using the Laptop right now. Even if the image is not clear the video may give us more information, regarding the person, his voice also his surrounding environment, these are all useful for finding the person hence the laptop.

So the IP address and the photograph and video will reveal the person who has stolen the Laptop. With these identities a complaint can be given in police to recover the Laptop and to catch the person. Instead of reporting in police that my Laptop is missing, a complaint can be given on specific person along with his photo, IP address with the mail copy. These two evidences will be useful for them to trace the person quickly **[Figure -1]**.

Examples of how video evidence has been used in the criminal justice process:

- Film evidence for using child soldiers by Lubanga: video clips were important to sparking an investigation, while not proving age of children
- Symptoms of Ghouta and Bhopal: video clip was used as lead evidence, but not linkage evidence
- Case in Darfur, Sudan: while the evidence did not link the attacks to the alleged attackers, the video and picture evidence was enough to move the case forward in court
- Footage of police torture of prisoners: despite authentication questions, footage was still used to call an investigation
- Footage of Al-Houlah Massacre in Syria: footage called attention to the massacre and led the UN to call for a special inquiry to conduct an investigation

THE IIOAB JOURNAL
ISSN: 0976-3104

- Video of General Ratko Mladic Speech: video speech of General Mladic's speech served as linkage evidence, as it linked Tolimir to the "inner command circle" of Mladic
- Case of Video Manipulation: Serbian journalist manipulated video evidence in order to protect himself from incrimination
- *Trust Alaska:* a story of how a young man named Nelson took a story he told in court with his Standing Declaration and made it into an influential video
- Videos on human rights abuses in Sri Lanka: videos used in the U.N High Commissioner for Human Rights in Geneva
- Solidary Uganda & oil company representatives: video was used to promote accountability in case representatives of oil companies went back on promises later
- Abuses of Uganda Wildlife Authority: video used to show abuses of the Wildlife Authority, but difficult to do with little artificial lighting
- Footage of the Mostar Bridge destruction: while there was footage, it was not established who did it, so the ICTY followed the bottom up strategy.

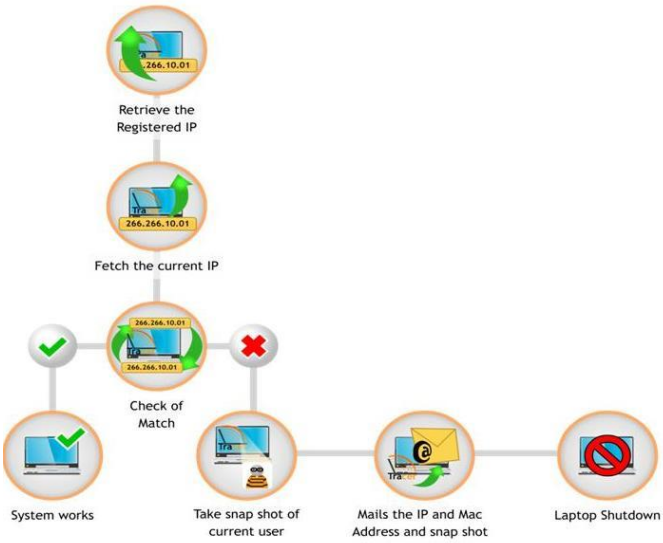

Fig: 1. Laptop Tracer

.....

Protecting Stolen Laptop data

Before the Laptop recovered from the robber it is highly important to protect the data in such Laptops. It is comparatively complex task. In Some earlier approach for protecting the data they used to provide a separate sever which have the key required to access the files in the Laptop. Normally this kind of servers is available in a concern need to protect their data. Every file access in such a environment need a encryption key without which the fie can't be accessed. Since the server is in office, if a person working in such office want to access any file from his home will be denied even the file exist in his laptop. So if such Laptop has been stolen by some strangers he is not able to access any of its content.

It seems to be a good idea but this approach having many drawbacks.

- It denies the file access even for a owner who is not in the office premises. In some emergency situation this approach gives a headache to the user.
- Need a dedicated server for maintaining file access keys.
- Slows down file access comparatively since every file access need a key from server and parallel request from others for the key causes heavy load at the key server.
- (iv)If the key server down or network down, none of the files from any laptop is accessible.

Keeping in mind the above limitations a simple solution for protecting the data is proposed in this paper.

When a Tracer finds that the laptop is in a suspicious location possibly with the stranger stolen it. Along with sending the IP address and photograph a One Time Password (OTP) will be send in a mail. Once the mail has been send the tracer will shutdown the Laptop.

If the Laptop restarted again the Tracer will be launched and this time it will prompt the user to enter the OTP to continue. If the Laptop is with the owner he knows the OTP since it has been delivered to his mail ID, so he could enter and continue to work in the Laptop. Also the current IP address will be stored in a Laptop.

THE IIOAB JOURNAL
ISSN: 0976-3104

Otherwise if the correct OTP is not entered the tracer will again send the new OTP with IP and photo of the user. This will continue for three time after third attempt the Tracer will not allow the System to boot to protect the data from the strangers.
The following **[Figure -2]** above shows the working of data protection module.

The current IP address, mail id's, OTP code and stolen status every thing will be kept in a system registry in a encrypted format. The encryption key and password to access or modify the settings like changing IP, mail ids are also stored in registry.

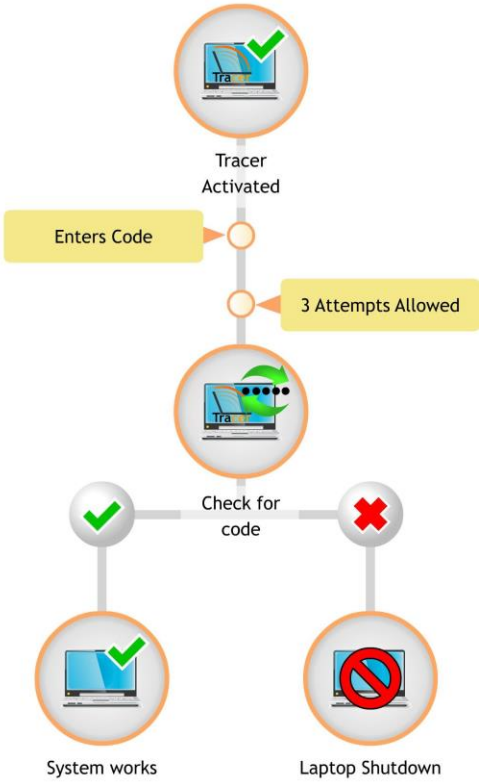

Fig:2. Laptop data protection

The following [Figure -3] is the sample mail from the Tracer.

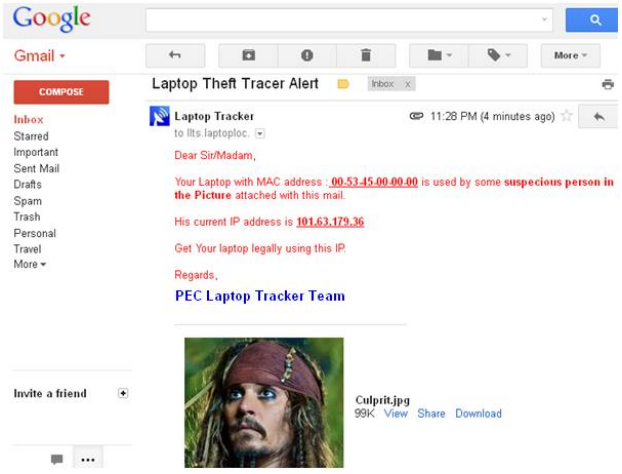

Fig: 3. Sample Alert Mail

THE IIOAB JOURNAL
ISSN: 0976-3104

The entire process of Laptop tracking shown in the following **[Figure -4]**.

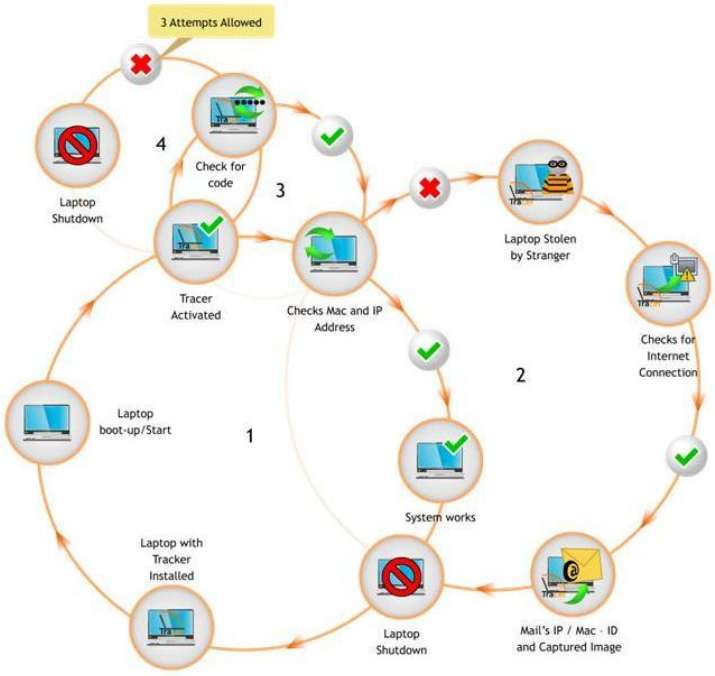

Fig: 4. The entire process of Laptop tracking

CONCLUSION

The proposed system of Laptop Tracking and Protection of data is cost effective and doesn't require any third party intervention in tracking them. Every operation can be done in Laptop itself and all operations are completely hidden from the user. It can be enhanced by including data encryption module based on the request from the user.

CONFLICT OF INTEREST

Authors declare no conflict of interest.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the technical support given by M.Narendran, Assistant Professor, Dept. of Computer Science and Engineering, SRM University, Chennai.

FINANCIAL DISCLOSURE

No financial support was received to carry out this project.

REFERENCES

[1] 2005 FBI Computer Crime & Security Survey

[2] "The Billion Dollar Lost Laptop Problem." Page 2 Intel. Ponemon Institute, 2009. Web. 13 Feb. 2013.

[3] "The Billion Dollar Lost Laptop Problem." Page 11. Intel. Ponemon Institute, 2009. Web. 13 Feb. 2013.

[4] "Security Breaches Are On The Rise But Preventable." Druva, 2012. Web. 15 August 2012.

[5] http://www.softexinc.com/pre_boot_authentication.asp

[6] https://www.lumension.com/data-protection/full-disk-encryption.aspx

[7] http://adeona.cs.washington.edu/

[8] Anthony J Nicholson, Mark D Corner, and Brian D Noble.[2006] Mobile Device Security Using Transient Authentication, *IEEE*.

[9] Peng Shaunghe.[2006] Enhancing PC Security with a U-Key, *IEEE* 4 (5)

[10] Maria Luisa Damiani,"'GEO-RBAC: A Spatially Aware RBAC",ACM 2006.

[11] A Hadid, JY Heikkil.[2007] Faces and eye detection for person authentication in mobile phones, *IEEE International Conference* 25-28

THE IIOAB JOURNAL
ISSN: 0976-3104

[12] Jerry Zeyu Gao, Lekshmi Prakash, and Rajini Jagatesan, "Understanding 2D-BarCode Technology and Applications in M-Commerce - Design and Implementation of A 2D Barcode Processing Solution, Published in Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International , 2

[13] Nadee C, Kumhom.P, Chamnongthai. K.[2005] Improved PCA-Based Personal Identification Method Using Invariance Moment,*ICISIP*

[14] Dong-Ju Kim, Kwang-Seok Hong.[2008] Multimodal biometric authentication using teeth image and voice in mobile environment, ,*IEEE Transactions* 54(4).

[15] McCune.JM, Yanlin Li, Ning Qu, Zongwei Zhou, Datta.A, Gligor.V, Perrig.A,[2010]TrustVisor: Efficient TCB Reduction and Attestation,*IEEE*.

[16] Ahren Studer, Adrian Perrig.[2010] Mobile user location-specific encryption (MULE): using your office as your password,ACM.

[17] Montaser N Ramadan, Mohammad A Al-Khedher, and Sharaf A Al-Kheder,[2012] Intelligent Anti-Theft and Tracking System for Automobiles, *Intl Journal of Machine Learning and Computing*, 2(1)

[18] Dong-Ju Kim, Kwang-Seok Hong. [2008]Multimodal biometric authentication using teeth image and voice in mobile environment, *IEEE Transactions on*, 54(4).