**Think India Journal**

*ISSN: 0971-1260 Vol-22, Special Issue-21*

**National Conference on**

**Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020)** organised

by

**Department of Commerce, VEL TECH Ranga Sanku Arts College,**

Avadi, Chennai-62

Held on 4th January 2020

# Fingerprinting Protocol for P2P Digital information Distribution

V.Shalini [1],
Assistant Professor,
Department of CS,
Veltech Ranga Sanku Arts College, Chennai

N.Chamundeeswari [2],
Assistant Professor
Department of CS,
Veltech Ranga Sanku Arts College, Chennai.

**Abstract:**
The traitor tracing protocol is used to detect the illegal transaction. Here I used fingerprinting solution to avoid illegal redistribution of multimedia contents. However, most of the existing anonymous fingerprinting protocols are impractical for two main reasons: 1) the use of complex time-consuming protocols and/or homomorphic encryption of the content, and 2) a unicast approach for sharing that do not scale for a large number of buyers. In this project stems from a previous proposal of recombined fingerprints which overcomes some of these drawbacks. However, the recombined fingerprint approach requires a complex graph search for traitor tracing, which needs the contribution of other buyers, and honest proxies in its P2P distribution situation. In this project focuses on removing these disadvantages resulting in an efficient, scalable, privacy-preserving and P2P-based fingerprinting system.

**Keywords:** Anonymous fingerprinting, P2P Digital data Distribution, Homomorphic encryption, Traitor tracing protocol.

## 1. Introduction:

Computer security is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from

unplanned events and natural disasters. Otherwise, in the computer industry, the term security or the phrase computer security refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

**Think India Journal**
*ISSN: 0971-1260 Vol-22, Special Issue-21*
**National Conference on**
**Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020)** organised
by
**Department of Commerce, VEL TECH Ranga Sanku Arts College,**
Avadi, Chennai-62
Held on 4th January 2020

Fig 1: System Security

## 1.1 Working conditions and basic needs in the secure computing:

If you don't take basic steps to protect your work computer, you put it and all the information on it at risk. You can potentially compromise the operation of other computers on your organization's network, or even the functioning of the network as a whole.

## 1.2Physical security:

Technical measures like login passwords, anti-virus are essential. However, a secure physical space is the first and more important line of defense. Is the place you keep your workplace computer secure enough to prevent theft or access to it while you are away? While the Security Department provides coverage across the Medical center, it only takes seconds to steal a computer, particularly a portable device like a laptop or a PDA. A computer should be secured like any other valuable possession when you are not present. Human threats are not the only concern. Computers can be compromised by environmental mishaps or physical trauma. Make sure the physical location of your computer takes account of those risks as well.

## 1.3 Access passwords:

The University's networks and shared information systems are protected in part by login credentials (user-IDs and passwords). Access passwords are also an essential protection for personal computers in most circumstances. Offices are usually open and shared spaces, so physical access to computers cannot be completely controlled.

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) organised
by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

To protect your computer, you should consider setting passwords for particularly sensitive applications resident on the computer (e.g., data analysis software), if the software provides that capability.

## 1.4 Prying eye protection:

Because we deal with all facets of clinical, research, educational and administrative data here on the medical campus, it is important to do everything possible to minimize exposure of data to unauthorized individuals.

## Anti-virus software:

Up-to-date, properly configured anti-virus software is essential. While we have server-side anti-virus software on our network computers, you still need it on the client side.

## Firewalls:

Anti-virus products inspect files on your computer and in email. Firewall software and hardware monitor communications between your computer and the outside world. That is essential for any networked computer.

## Software updates:

It is critical to keep software up to date, especially the operating system, anti-virus and anti-spyware, email and browser software. The newest versions will contain fixes for discovered vulnerabilities.

Almost all anti-virus have automatic update features (including SAV). Keeping the "signatures" (digital patterns) of malicious software detectors up-to-date is essential for these products to be effective.

## Keep secure backups:

Even if you take all these security steps, bad things can still happen. Be prepared for the worst by making backup copies of critical data, and keeping those backup copies in a separate, secure

**Think India Journal**
*ISSN: 0971-1260 Vol-22, Special Issue-21*
**National Conference on**
**Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020)** organised
by
**Department of Commerce, VEL TECH Ranga Sanku Arts College,**
Avadi, Chennai-62
Held on 4th January 2020

location. For example, use supplemental hard drives, CDs/DVDs, or flash drives to store critical, hard-to-replace data.

## Report problems:

If you believe that your computer or any data on it has been compromised, your should make a information security incident report. That is required by University policy for all data on our systems, and legally required for health, education, financial and any other kind of record containing identifiable personal information.

## 2. System Architecture:

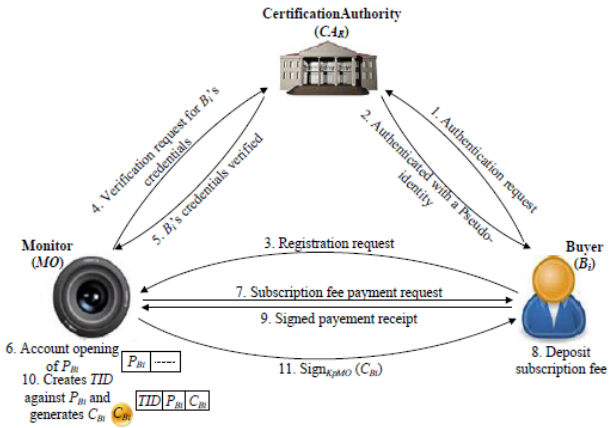


Fig 2: System Architecture Diagram

## 2.1 Merchant:

He distributes copies of the content legally to the seed buyers. Each fragment of the content contains a different segment of the fingerprint embedded into it. The segments have low pair-wise correlations.

## 2.2 Buyers' Privacy:

The identity of a buyer who has purchased a specific content could be revealed by a coalition of two parties: one of the proxies chosen by the buyer and the merchant or, similarly, the transaction monitor and the merchant. Better privacy could be achieved if, for example, the pseudonyms were encrypted by the proxies using the public key of the tracing authority.

**Think India Journal**
*ISSN: 0971-1260 Vol-22, Special Issue-21*
**National Conference on**
**Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020)** organised
by
**Department of Commerce, VEL TECH Ranga Sanku Arts College,**
Avadi, Chennai-62
Held on 4th January 2020

## 3.3 Transaction monitor:

It keeps a transaction register for each purchase carried out for each buyer. This transaction register includes an encrypted version of the embedded fingerprints. In case of illegal re-distribution, it participates in the tracing protocol that is used to
Identify the illegal re-distributor(s).

## 2.4 Database authentication attacks:

An attacker may try to obtain the fingerprint of a buyer that is stored in the transaction monitor's database. An attacker may try to intercept the traffic between a buyer and one or more of her proxies and keep a copy of all the fragments of the content.

## 3. System Frameworks:

Here the figure [4.1] is ensuring that the new Buyer and Merchant want to register through the registration form to get User id and Password. When we register the form we must fill up the mandatory fields, here innovative feature is available that is Bio-metric it will give secured authentication.

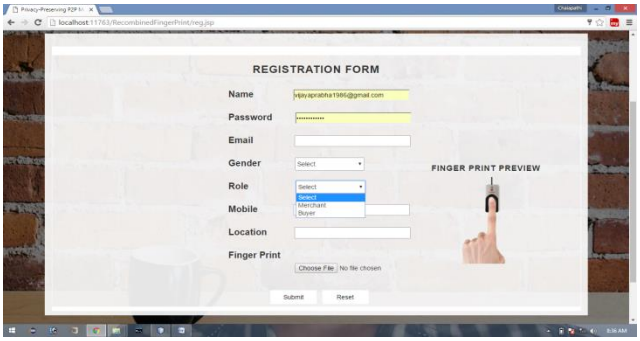


Fig 4.1: Registration Form

Now the figure[4.2] represents the seller must login through the merchant login form, by using user id and password then it checks whether authorized person or not.

**Think India Journal**
*ISSN: 0971-1260 Vol-22, Special Issue-21*
**National Conference on**
**Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020)** organised
by
**Department of Commerce, VEL TECH Ranga Sanku Arts College,**
Avadi, Chennai-62
Held on 4th January 2020

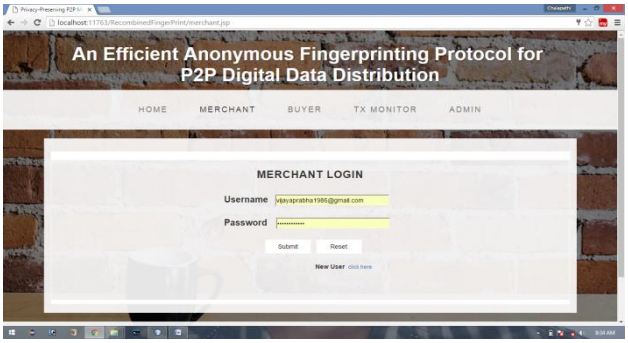

Fig 4.2: Merchant Login Form

Here the figure [4.3] stand for the buyer must login through the buyer login form, by using proper username and password then it ensure whether approved person or not.

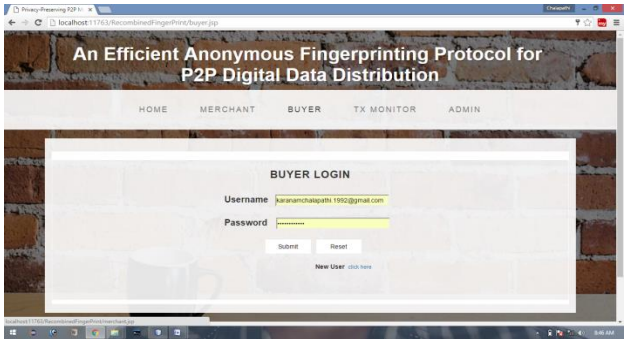

Fig 4.3: Buyer Login Form

Now the figure [4.4] shows that the transaction manager how to controls data traffic of merchant and buyer.

**Think India Journal**
*ISSN: 0971-1260 Vol-22, Special Issue-21*
**National Conference on**
**Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020)** organised
by
**Department of Commerce, VEL TECH Ranga Sanku Arts College,**
Avadi, Chennai-62
Held on 4th January 2020

Fig 4.4: Transaction Monitor Diagram

The figure [4.5] represent to download the data through the secured authentication by using fingerprint and public key. The public key is generated by the merchant and they send generated public key to the buyer through the e-mail.

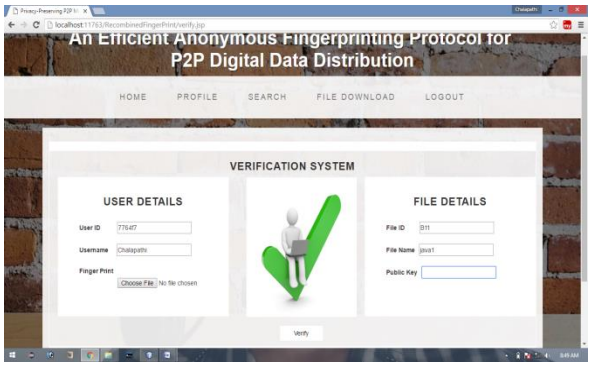


Fig 4.5: Public Key Verification

## 5. Conclusion:

In this we discussed about the implementation of the fingerprinting protocol based on public cryptosystems.Thehash message authentication code is used to construct binary code and that will be fingerprint of the content. The fingerprint is recombined and generates automatically from their parent and embedded with content distribution. The RSA algorithm is used to generate private and public key value and it is used to identify authorized users. This system will give more security to buyers and sellers who have distributed multimedia content through online.

## Reference:

[1] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," in Proc. 15th Ann. Int. Cryptology Conf. Adv. Cryptology, 1995, pp. 452–465.
[2] Y. Bo, L. Piyuan, and Z. Wenzheng, "An efficient anonymous fingerprinting protocol," in Proc. Int. Conf. Comput. Intell. Security, 2007, pp. 824–832.
[3] J. Camenisch, "Efficient anonymous fingerprinting with group signatures," in Proc. 6th Int. Conf. Theory Appl. Cryptology Inf. Security: Adv. Cryptology, 2000, pp. 415–428.
[4] C.-C. Chang, H.-C. Tsai, and Y.-P. Hsieh, "An efficient and fair buyer-seller fingerprinting scheme for large scale networks," Comput. Security, vol. 29, pp. 269–277, Mar. 2010.
[5] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Commun. ACM, vol. 24, pp. 84–90, Feb. 1981.

[6] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography. Burlington, MA, USA: Morgan Kaufmann, 2008.
[7] J. Domingo-Ferrer and D. Megıas, "Distributed multicast of fingerprinted content based on a rational peer-to-peer community," Comput. Commun., vol. 36, pp. 542–550, Mar. 2013.
[8] M. Fallahpour and D. Megıas, "Secure logarithmic audio watermarking scheme based on the human auditory system," Multimedia Syst., vol. 20, pp. 155–164, 2014.
[9] S. Katzenbeisser, A. Lemma, M. Celik, M. van der Veen, and M. Maas, "A buyer-seller watermarking protocol based on secure embedding," IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 783–786, Dec. 2008.
[10] M. Kuribayashi, "On the implementation of spread spectrum fingerprinting in asymmetric cryptographic protocol," EURASIP J. Inf. Security, vol. 2010, pp. 1:1–1:11, Jan. 2010.