International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 5, May - 2014

Privacy Preserving File Accessing System Using Location Proof and System Proof

John Berchmans
Department of Computer Science and Engineering
T.John Institute of Technology
Bangalore

Nagashree K. T
Assistant Professor
Department of Computer Science and Engineering
T.John Institute of Technology
Bangalore

***Abstract*— Today's location-based services are mainly based on user's mobile devices to determine the current location and send this location to the application. This may allows users to send false location and enable the user to access restricted resources. Here we present a privacy preserving file accessing system using location proof and system proof in which each mobile users having a mobile node such as a laptop can able to access files from a server. We also introduce system proof which is the IP and MAC address of the system to provide a high security application that allows confidential data access to its users. It can be implemented with Wi-Fi infrastructure and can be easily deployed with little computational cost.**

***Index Terms*—Location-based service, location proof, system proof**

I. INTRODUCTION

Location-based services use user's current location information and provide access to various resources and services. Today's location-based applications require users to provide their location proofs at a particular time. "Google latitude" and "Loopt" are the two examples of location-based services that help users to track their friend's location in real time. In all these applications location proof plays an important role to enable this kind of applications.

Location-based access control is a category of location-sensitive applications. For example, a hospital may allow doctors and nurses to access patient's information only when they are in a particular room of the hospital. Another application is in police investigation, in which detectives can able to finding out a person if he was at a murder scene at some time. Another kind of application is fraud detection on eBay in which location proof from the server can be used to identify that the sellers account has not been compromised by attackers. Location-based printing service is another kind of example. In this, client can able to print files in the nearest printer based on the location of the access point to which the client used to access the printing service.

This paper presents a privacy preserving file accessing system using location proof and system proof in which each user needs to submit their location to access the file from a server. The location proofs are uploaded to the server and verify the user location. In order to provide high security for the confidential data we also use system proof that is the IP and MAC address of the system. System proof is also send along with the location proof. Each user has a separate system allotted to them and users can access files only from their registered system, which provide high security for the confidential data.

The rest of the paper is organized as follows. In section II we introduce the location proof and system proof. We present the system architecture in section III. We discuss the related work in section IV, and conclude this paper in section V.

II. LOCATION PROOF AND SYSTEM PROOF

In this section we deals with the preliminaries of our system and our major concepts of location and system proof verification system.

A. Preliminaries

We focus on mobile nodes such as laptops where each device communicates with the server through Wi-Fi infrastructure. In our implementation each device produces their location proof to the server periodically. File access is possible only when the user is trusted based on the location proof and system proof.

Each client has their own public/private key pair. There exists a certification authority (CA) in the server. Each user needs to register with the certification authority and CA will assign one public/private key pair to the user. The public key is used as the pseudonym of the node. Also the private is used to digitally sign each messages so the verifier service can authenticates the node. Server can identify the client from which the location proof is send. Also when confidentiality is required, security mechanisms are used such as encryption, decryption, hash function etc.

B. Location Proof

A location proof is a piece of information that certifies a geographical location. We use the latitude and longitude coordinates to specify the geographical location. Each location proof contains the location of the node and the identities of the node, which is the public key of the node. The location proofs are submitted to the service which verifies the location and provide the service based on the verification. Location proofs are personal and non-transferable. Many identity schemes can be used for location proofs. The main requirement is that these schemes can verify that a public key embedded in a location proof is uniquely mapped to one single entity.

In mobile communication, cellular phones are capable of discovering their locations based on service provider or GPS. So cellular phones can generate location proof and submit to the application when they need it [1], [5]. But in the case of mobile nodes such as a laptop no GPS module is present. So we need to set the location manually or set the location of the Wi-Fi access point and use this location as the node's location, i.e. the location of the node is same as that of AP to which the node used to access the service.

C. System Proof

We introduce system proof to our system to improve the protection of confidential data stored in the system. System proof means the IP and MAC addresses of the system. User can access files only from their registered systems. This will provide high security to confidential file access. The system proof is verified along with the location proof and provides service based on the verification.

IP and MAC addresses are used uniquely identify each system. In a standard network the IP address of a system is fixed. But there is a chance of changing the IP address to another. So we also use MAC address. MAC address is manufacturer specific and is unique to each system. No one can modify MAC address. Combined use of IP and MAC will allow only registered users can access the service from their registered system.

III. SYSTEM ARCHITECTURE

In this section we introduce file accessing system architecture and the protocol used.

A. Architecture

In our system mobile nodes communicates through Wi-Fi. Each node plays different roles in our system. Based on this they are categorized as Prover, Witness, Proof Server. Proof Server consists of Certificate Authority and Verifier. The architecture and message flow is shown in fig. 1.

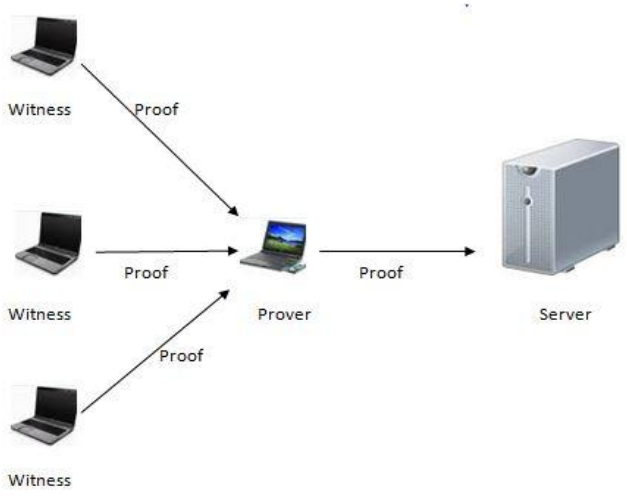

Fig. 1. System architecture and message flow

- **Prover**: one node from the entire nodes will act as the prover which is responsible for collecting the location proofs from other nodes and upload this to the proof server. Prover initiates the proof request and if no response is received, it submits a dummy proof.
- **Witness**: the node which registers with the server is the witnesses of the prover. Each witness node creates the location proof and sends it to the prover.
- **Proof Server**: it stores the location information of each node. The proof server is directly communicates with the prover node who submit the location proofs. The identity of each node is stored in the server. Also the files to which the client needs to be accessed is stored in the server. Each node should register with the server before accessing the files.
- **Certificate Authority**: every user must register with the certification authority before entering into the network. CA will provide separate public/private key pair to each node which is used in the communication to authenticate each node.
- **Verifier**: an application which is responsible for verify the location and system proof. Based on this verification the node is classified as trusted or untrusted. File access will allow only when the client is trusted.

The certificate authority and verifier service is implemented in the server. Whenever a client wants to register into the system, the certificate authority is responsible for registering the node. At the time of verification of proof, the verifier will do the things.

B. Protocol

When a location proof is required for the prover, it sends a request to the nodes. The protocol to be executed is shown in fig. 2.

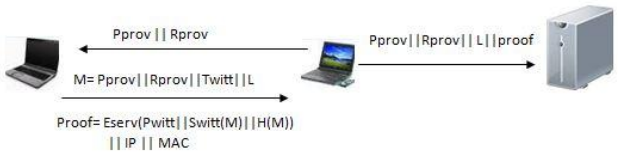

Fig. 2. Proof updating protocol

1. The prover broadcast the location proof request to its witness nodes periodically (at every 5 minutes). This request contains prover's current pseudonym Pprov and a random number Rprov.
2. After receiving the request from the prover, witness generates a location proof and sends back to the prover. This location proof contains prover's pseudonym Pprov, prover's random number Rprov, current time stamp of witness Twitt, witness pseudonym Pwitt, and the location of witness L. This proof is signed and hashed by the witness and then encrypt this message by using the server's public key. This will helps to authenticate the witness and avoids traffic monitoring or eavesdropping. The system proof is also send along with location proof.
3. After receiving the location proof from the witness, prover uploads this proof to proof server. This message also contains prover's pseudonym Pprov, prover's random number Rprov, and its location L. Also the IP and MAC address of the witness is submitted for verification.
4. The verifier in server is responsible for verify the location proof and System proof. First verify the system proof that

is check whether the IP and MAC address is belong to a registered system. Then it decrypts the message and verify the prover and verify the location of prover with the location of witness given in the encrypted message. If all these verifications are passed then the node is a trusted node.

IV. RELATED WORK

Many researchers proposed several systems that provide end users with the ability to prove that they are in a particular location. S. Saroiu and A. Wolman [2] presents "location proofs" which is a small piece of meta data issued by Wi-Fi infrastructure. But it relies on wide deployment of Wi-Fi infrastructure. In [3], the authors describe about spatial timestamp noting a system-verified time and location which is similar to geotagging. But it requires expensive trusted computing module to generate location proofs. Xu and Cai in[4] present a feeling based privacy model. In this each user can express his privacy requirement by specifying a public region which is reported as the location of the user.

There exist many works on location privacy in wireless networks. In [1], [5] Zhu and Cao present a location proof updating system. It also describes about colluding attacks in mobile phones which uses Bluetooth as a communication medium. Another work based on location discovery presents a location based printing service which uses the location of the access point as the mobile user location to locate the nearest printer. This is based on location discovery, in which the access point finds the printer near to its location for the printing service. In our system we protect the confidential file access by giving client's location proof and system proof. Use of IP and MAC address helps to identify the user as well as the system to which the user use to access files.

V. CONCLUSIONS

In this paper we present a privacy preserving file accessing system where mobile nodes such as laptop is used to access files from a server by giving the location proof of the client. To provide high security for the confidential file access we introduce system proof, the IP and MAC address of the system. Clients can access files by submitting location proof along with system proof that improves the secure confidential file access. Our system can be implemented with Wi-Fi infrastructure with little computational cost.

REFERENCES

[1] Zhichao Zhu and Guojong Cao, "Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System", IEEE TRANSACTIONS ON MOBILE COMPUTING. 2013.

[2] S. Saroiu and A. Wolman, "Enabling New Mobile Applications With Location Proofs", Proc. ACM 10th Workshop Mobile Computing Systems and Applications(HotMobile '09), 2009.

[3] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Location Based Trust for Mobile User-Generated Content: Applications, Challenges and Implementation", Proc. Ninth Workshop Mobile Computing Systems and Applications, 2008.

[4] T. Xu and Y. Cai, "Feeling-Based Location Privacy Protection for Location-Based Services", Proc. 16th ACM Conf. Computer Comm. Security (CCS), 2009.

[5] Z. Zhu and G Cao, "APPLAUS: A Privacy Preserving Location Proof Updating System For Location-Based Services", Proc. IEEE INFOCOM, 2011.