PRIVACY-PRESERVING FOR SECURE VOLTE BASED ON COMPUTATIONAL INTELLIGENCE IN MOBILE COMPUTING

M.GopikaMurali, Department of CSE, Francis Xavier Engineering College, gopikamurali020@gmail.com

M.Irene Selena, Department of CSE, Francis Xavier Engineering College, irenesweetyims@gmail.com

Dr. C. Gopala Krishnan M.E.,Ph.D., Professor/CSE, Francis Xavier Engineering College, skywarekrish@gmail.com

Abstract: Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services a shared pool of configurable computing resources, without the burden of local data storage and maintenance. The low mobility communication are soon to be deployed on a broad basis with LTE-advance and IEEE802.16m as the two candidate system.

Keywords: — Local Data Storage,Physica Possession,Data Integrit

IINTRODUCTION

Voice over Internet Protocol (VoIP) is a technique to transmit voice data through Internet Protocol (IP) networks. Unlike fixed circuit switching telephony, voices are encapsulated into data packets and transmitted through the packet switching in VoIP. To setup a call, Session Initiation Protocol (SIP) is used as signaling protocol [1]. The existing VoIP services in 4G LTE (Long Term Evaluation) mobile network mainly include Over-The-Top (OTT), Voice over LTE (VoLTE) and Voice over Wi-Fi (VoWiFi). The differences among OTT, VoLTE and VoWiFi are elaborated as follows. OTT refers to the applications, which provide contents and services over the Internet but are independent of Internet Service Providers (ISP). Take voice call services for example, Skype, Facebook Messenger and LINE are some of the most popular OTT applications. However, network providers mainly promote VoLTE and VoWiFi. The former utilizes LTE and the latter utilizes Wi-Fi to connect to Evolved Packet Core (EPC), 4G core networks. VoWiFi is Promoted to strengthen the indoor coverage of VoLTE and slash international roaming expenses. In terms of billing mechanism, OTT service does not charge a calling fee, but the users may be charged for the data transmission volume by their network providers. Yet, both VoLTE and VoWiFi use the traditional time billing mechanism, which calculates calling fee based on the duration of the call. In respect of the Quality of Service (QoS), since voice packets of OTT are transmitted through the Internet, which OTT has no quality control over, the packet loss may be high when network congestion occurs. By contrast,VoLTE calls setup over QCI 5 (QoS Class Identifier) and can guarantee the packet loss rate within 1% since there is a specific bearer for voice data of VoLTE inside the LTE core network [2]. As for VoWiFi, WI-Fi Multimedia (WMM) can be adopted to increase the priority of voice in IEEE 802.11 networks [3]. Therefore, network congestion has larger impact on OTT than VoWiFi and VoLTE. Although VoLTE and VoWiFi are the official voice service provided by network operators, users still prefer to make a call via OTT services. The investigation report from National Development Council in Taiwan shows that 43.9% of mobile users said that the using time of traditional voice calling is less than 10% [4]. There are also 21.7% of subjects said that they make less calls after using instant messengers (OTT services) [5]. Compared to using the OTT with LTE, using the OTT with Wi-Fi is cheaper since most Wi-Fi is free. Moreover,the investigation from Big-Data Research also supports this perspective by showing that 71.8% VoIP users choose to make calls withWi-Fi connection. Besides, connecting to a Wi-Fi AP causes less power consumption than connecting to an eNodeB (eNB) when devices run multimedia applications . As a result, we infer that most users are willing to sacri_ceQoS in order to spend less money. As the popularity of heterogeneous networks, user equipment's (UEs) provide several radio access abilities. In this network architecture, OTT applications are no longer independent of networks, and should implement the selection between network

connections on application layer to optimize data usage for users. Since heterogeneous networks use different interfaces and IP addresses, the OTT applications need to send Re-INVITE to renegotiate the sessions [9]. The term, application-based vertical handover, is used and abbreviated to handover in this paper to describe this process of changing session settings between different networks during the OTT call. Similar with the scenario between VoLTE and VoWiFi, OTT can connect to LTE, whose coverage ranges several kilometers, and Wi-Fi, whose coverage ranges hundreds of meters. However, when users move in the area where LTE and Wi-Fi provide similar QoS,OTT may frequently handover between LTE and Wi-Fi networks.From the OTT vendors' point of view, these unnecessary vertical handovers produce signal overload problem. From the users' point of view, the LTE usage and energy consumption increase without handover management. Some vertical handover algorithm (VHA) makes handover strategies. However, to the best of the authors' knowledge, no existing work focus on how OTT voice services deal with connection management in heterogeneous networks. Since OTT users are more tolerant to the delay and packet loss and more willing to use Wi-Fi than LTE, the OTT application is not necessary to renegotiate as soon as the status of network changes. The proposed a SIP-base disconnect tolerant session recovery mechanism, which records the speech in disconnected period and plays back the recording subsequently when connection resumes. To shorten the delay, the parts without voice are cut in the recording. Thus, we propose a Delay Handover Mechanism (DHM) to avoid frequent and unnecessary handover procedures by postponing the timing to switch connection from Wi-Fi to LTE. A Delay Timer is applied for the UE to wait for the next Wi-Fi connection rather than switch to LTE as soon as the UE leave the previous Wi-Fi coverage. If the UE reconnects to a Wi-Fi, two handover procedures are reduced. The trade-off between packet loss and the reduced ratio of handovers is discussed by mathematical analysis and simulations.

II EXISTING SYSTEM

Location management is the mechanism for locating the mobile node(MN) or a user in order to initiate and establish a connection TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user.the existing wireless access network and the model is quite straight forward

III PROPOSED SYSTEM

Many of the proposed changes to the telecommunications systems will drive additional modification.They need to work in concert with the other proposals in order to fully meet the expected requirements for VOLTE telecommunications.
To how the network is construct or functions in order for them to work. We also show how to extent our main scheme to support batch auditing for TPA upon delegations from multi-users.

IV SYSTEM ARCHITECTURE

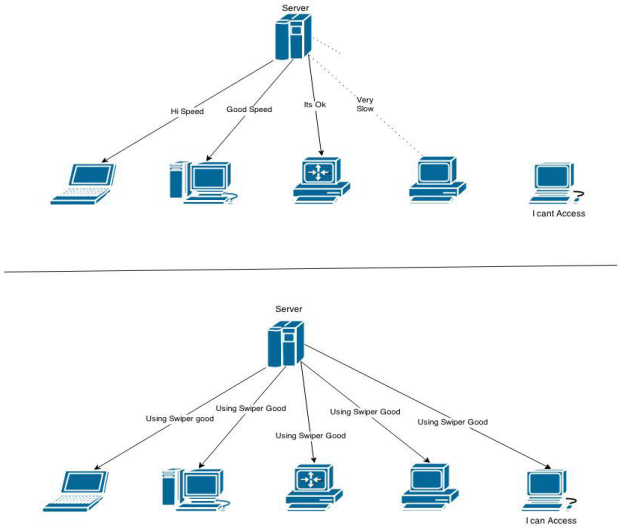

Fig 4.1:System architecture

V MODULES

1.Store and Create Packets.

2.Information Sends Random Wakers.

3.Luby Transform degree distribution.

4.Secure Coprocessor.

5.Trusted Database.

6.Roc Process.

7.Task Execution.

8.Data owner initialization.

9.Web Server identification.

Store and create packets

To create a new encoded packet, each storage node asks information to a randomly selected node of the network. The receiver answers to the caller sending its information that will be used by the caller to encode a new packet. A similar algorithm is proposed in where the coded packet formation mechanism is reversed; in this case, the node that stores the information sends random walkers containing the information.

Information sends random walkers:

This information and create encoded packets XORing some of the information they already received. At the end of the process, each storage node stores an encoded packet, and it is possible to retrieve the initial information querying any randomly chosen storage nodes.

Luby Transform degree distribution:

Each rate less packet performs a random walk across the network and novel information is combined only once every t hops; when new information is added the packet degree is reduced by one. When the degree becomes zero, the rate less packet performs t supplementary hops to hit the node that will store it. However, the focus of the paper is to increase data persistence; the time required for the distribution of the rate less packets.

Secure Coprocessor:

This module used to supplement the functions of the primary processor (Server).Operations performed by the coprocessor may be floating point arithmetic, graphics, signal processing, string processing, Decryption or I/O Interfacing with peripheral devices. This module used to decrypting user information and communicate with Admin.

Trusted database:

Database is to be secure because hackers do not hacking user information and they are using encryption and decryption both are used in secure purpose

Roc process:

The ROC family of Remote Operations Controller has established an industry benchmark for flexibility, robustness, ease of use and reliability. and the scalability, speed and control capability of a single device PLC. Fog computing brings the advantages and power of the cloud closer to where data is created and upon acted.

Task execution:

This can delay the execution of background tasks if you run the model with a relatively small sample time This value is an average of the measured CPU times, in seconds, to run the model equations and output post during each sample interval. Task execution time is nearly constant, with minor deviations due to cache, memory access, interrupt latency, and multirate execution module.

Data owner initialization:

This module is to register the new users and previously registered users can enter our project. The user only can enter into Proposed Process in our Project. The user can view Existing Of our Project. The data owner runs the Setup function to system the initiate. When the data owner wants to upload file to the cloud server, it first defines an access control for File Upload, and then determines the current time. Finally, it runs the Encrypt function to output the cipher text. When the data owner wants to grant a set of attributes in a period of time to data user, it runs the Gen Key function with attributes and effective times to generate keys.

Web server identification:

The available Peer List is obtained by entering the name workgroup. This peer list into active peer list and inactive peer list. The active peer list into long lived peer and short lived peer. The long lived peer list is selected and is used for process.

Proposed Technology

The public key based homomorphic authenticator and uniquely integrates it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. To efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate

signature to extend our main result into a setting multi user, where TPA perform multiple auditing tasks simultaneously. security and the proposed schemes are provably secure and highly high . We also show how to extent our main scheme to support batch auditing for TPA upon delegations from multi-users.

VI CONCLUSION AND FUTURE ENHANCEMENT:

Information sharing and state transition on the control plane have to be carefully crafted. Otherwise, they may lead to more severe attacks than the data-plane loopholes. A state change in the CS domain may impose unanticipated effect in the domain. The security implication is that CS can be exploited to degrade the performance of PS.

REFERENCES

[1] J. Rosenberg et al., SIP: Session Initiation Protocol,document RFC 3261-SIP, 2010.

[2] IEEE Standard for Information Technology_Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks_SpecificRequirements_Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Speci_cations, IEEE Standard 802.11e-2005, 2005.

[3] M. Yu, L. Jose, and R. Miao, “Software defined traffic measurement with open sketch,” in Proc. USENIX NSDI, 2013, pp. 29–42.

[4] B. Heller et al., “Leveraging SDN layering to systematically troubleshoot networks,” in Proc. ACM Hot SDN, 2013, pp. 37–42.

[5] H. Zhang et al., “Enabling layer 2 path let tracing through context encoding in software-defined networking,” in Proc. ACM Hot SDN, 2014,

pp. 169–174.

[6] K. Bu et al., “Is every flow on the right track Inspect SDN forwarding with rule scope,” in Proc. IEEE INFOCOM, Apr. 2016, pp. 1–9.

[7] P. Tam mana, R. Agarwal, and M. Lee, “Cherry Pick: Tracing packet trajectory in software-defined datacenter networks,” in Proc. ACM SOSR,

2015, pp. 23:1–23:7.