International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 3 645 – 650

Development of Secure Mobile Cloud Computing Using Improved Identity Management Protocol

Pankaja A.Hadole
M.Tech,IV Sem , Dept. of Computer Sci & Engg TGPCET, Nagpur,India
pankajaahadole@gmail.com

Prof. Jayant Rohankar
Dept. of Computer Sci & Engg TGPCET, Nagpur,India
jayant_rohankar@gmail.com

Prof. Priyanka Ambatkar
Dept. of Computer Sci & Engg., DMIETR, Sawangi (M), Wardha, India
piyuambatkar@gmail.com

Prof.Arun Katara
Dept. of Electronics Engineering DMIETR, Sawangi (M), Wardha, India
arunkatara@gmail.com

Abstract — The convergence of Internet and mobile computing enables personalized access to online services anywhere and anytime. Entities (e.g., users, services) have to authenticate themselves to service providers in order to use their services. An entity provides personally identifiable information that uniquely identifies it to an SP.Due to the rapid spread of smart phones and social network service, the use of Interne applications has increased and their need for bandwidth has begun to exceed the capacity of 3G networks. This has caused a reduction in speed and service quality. The increase in mobile network users has caused identity management problems for mobile service providers. Therefore, in this paper, proposed system is designed to overcome this problem Improved Identity Management protocol is used to breaks up loads, which are allowed by the existing Identity Management 3G protocol's mutual authentication via mobile operator process, by sending some parts to an Internet application service provider to enhance mobile and ID management at the service provider and by reducing the network and process loads from information handling and packet transmission.

Index Terms—*Communication Protocol, Social Network, Message Encryption, User Identity management.*

*****

I. INTRODUCTION

Cloud Computing is a natural fit for mobile security[1]. Typical handsets have input constraints and practical computational and power limitations, which must be respected by mobile security technologies in order to be effective.

Cloud computing has brought new challenges and opportunities for authentication. There is increasing demand for usable authentication to access services and data for both enterprises and consumers. Identity management is one of the most critical factors that influence the success of Internet business applications. Identity management (denoted IdM hereafter) is about recognizing and verifying the correctness of Identities in Online environments.

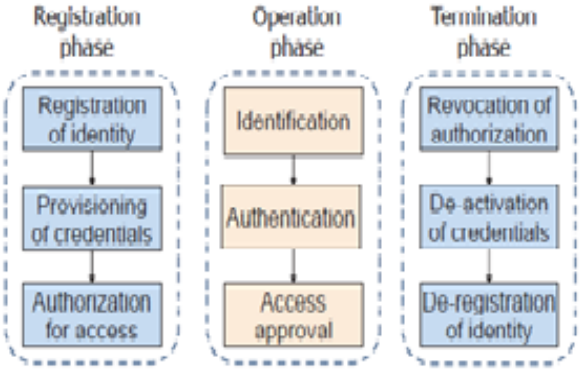

Fig.1 Phases of IDM and access control

Trust management becomes a component of IdM whenever different parties rely on each other for identity provision and authentication. IdM [2] and trust management therefore depend on each other in complex ways because the correctness of identity itself must be trusted for the quality and reliability of the corresponding entity to be trusted. IdM is also an essential concept when defining authorization policies in personalized services when talking about authentication; it is helpful to give some basic definitions regarding this matter.

The process of authentication [3], or also verification validates a claimed identity by matching it to a known set of identities. In contrast, identification has a different purpose. When identifying a person, that person does not his or her identity. Rather, the system has to find out itself that who is interacting, through matching certain characteristics of a client to models in the database. This is accomplished in a one-to-many matching process.

In the recent world, where the number of mobile users has raised to infinity, the network traffic overload and user identification found to be the main concern for service provider and mobile operators. As we can see, the heavily used social networks like face book and twitter also provide their mobile applications which cause heavy traffic management problem for mobile operators and network companies. It also causes the user identification problems to the service providers. To overcome all these limitations many communications protocols are being used by many mobile operators and service providers.

The widely used in recent time is IDM3G [4].We are proposing the improved version of this protocol .This protocol

 ISSN: 2321-8169
645 – 650

will minimize the traffic overload problems in mobile computing and will provide the unique user identification mechanism Our proposal minimizes degradation in MO and maintenance by constructing a trusted base with cross certification between service providers and MO.

II. RELATED WORK

An issue in Mobile communication Side is Low Bandwidth. Bandwidth is one of the big issues in Mobile cloud computing since the radio resource for wireless networks is much scarce as compared with the traditional wired networks. Availability: Service availability becomes more important issue in Mobile cloud computing than that in the cloud computing with wired networks. Mobile users may not be able to connect to the cloud to obtain service due to traffic congestion, network failures, and the out-of-signal.

A. User Identity Management and Authentication

Identity management is one of the most critical factors that influences the success of Internet business applications
Whether an application runs on-premises or in the cloud, it typically needs to know something about its users. Toward this end, the application commonly demands that each user provides a digital identity, a set of bytes that describes that user. Based on what these bytes contain and how they're verified, the application can determine things such as who this user is and what they're allowed to do.

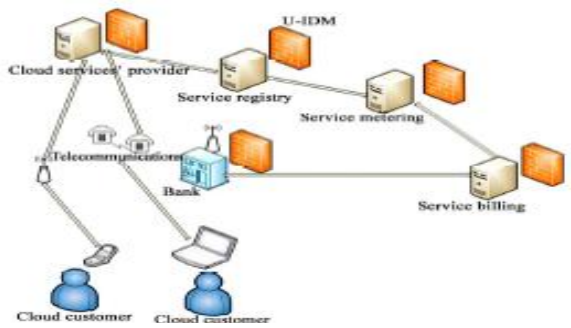

Fig 2. User Identity Management flow

Before authentication starts, the authentication consumer lists the access requests (e.g., a webpage access request or a payment request) that require authentication. The authentication consumer redirects the request to the authentication engine, along with request details. The authentication engine retrieves the policy for the access request, extracts the information that needs to be collected, and sends an inquiry to the client device and/or data aggregator.

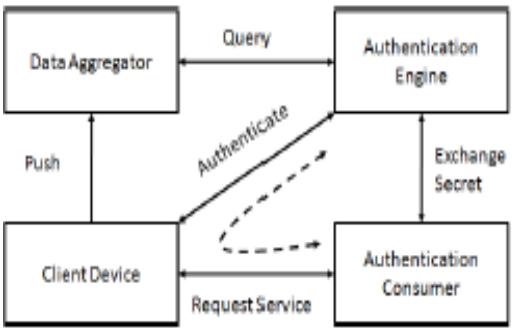

Fig 3: Participants in the general architecture And the relationships among them.

The authentication flow is as follows: Before authentication starts, the authentication consumer lists the access requests that require authentication [5]. For each request, the authentication consumer will register a policy with the authentication engine. The policy includes at least three parts: the access request, the information to be collected from client devices or data aggregator for this access request, and a rule to generate the authentication result. During normal operation, client devices periodically report to the data aggregator. This data will be used to track user behavior and support authentication requests.

The authentication flow starts when an access request is received by the authentication consumer. Upon receiving the request, the authentication consumer redirects the request to the authentication engine, along with request details. The authentication engine retrieves the policy for the access request, extracts the information that needs to be collected, and sends an inquiry to the client device and/or data aggregator. The client device and/or data aggregator receives the inquiry, generates a report, and sends it back to the authentication engine.

B. PGP Standard Protocol

Encryption of e-mails and any other forms of communication is vital for the security, confidentiality, and privacy of everyone. This is where PGP comes in and this is why PGP is so popular today. Pretty Good Privacy (PGP), developed by Phil Zimmermann. is a public-key cryptosystem. PGP works by creating a circle of trust among its users. In the circle of trust, users, starting with two, form a key ring of public key/name pairs kept by each user. Joining this "trust club" means trusting and using the keys on somebody's key ring. Unlike the standard PKI infrastructure, this circle of trust has a built-in weakness that can be penetrated by an intruder. However, since PGP can be used to sign messages, the presence of its digital signature is used to verify the authenticity of a document or file.

 ISSN: 2321-8169
645 – 650

This goes a long way in ensuring that an e-mail message or file just downloaded from the Internet is both secure and un-tampered with Improved Identity Management Protocol authenticate messages between SP and MO using key-pairing mechanism of PGP. MO issues paired public key before the beginning of services and generates corresponding private keys for each SP. Both generated keys are used for encrypting messages and verifying security associations between SP and MO.

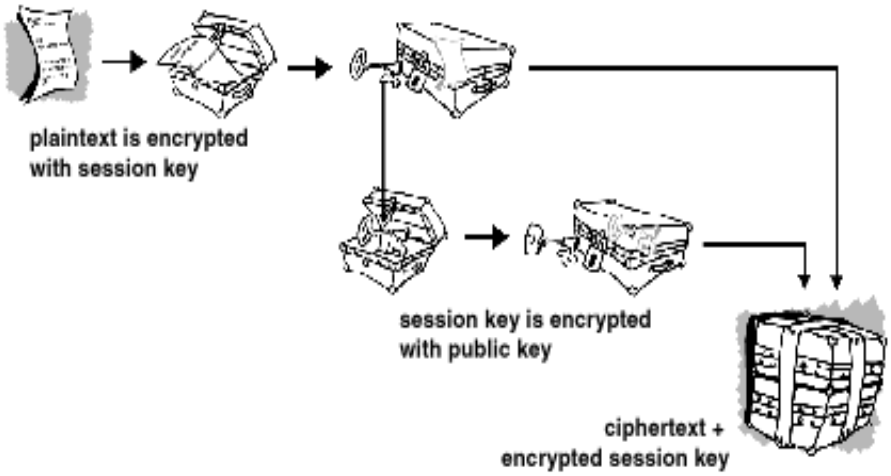

Fig 4.PGP Encryption work

C. UMTS-AKA

The UMTS-AKA (Authentication and Key Agreement) is a 3G mobile network technique designed for wireless networks. The Third Generation), a joint initiative of telecommunication standardization organizations from the United States, Europe, Japan and Korea, defined the UMTS Authentication and Key Agreement (UMTS-AKA) mechanism as their core element for entity authentication, user identity management, confidentiality and integrity). The UMTS-AKA mechanism [6] uses a pre-shared secure key (K) between the mobile operator (MO) and the UMTS subscriber identity module (USIM) of the mobile phone to perform authentication and key agreement. The USIM is a cryptography-enabled smart card identified by a unique 15-digit number, called international mobile subscriber identity (IMSI). The USIM and the mobile operator can perform mutual authentication by a challenge and response mechanism. The UMTS-AKA mechanism can achieve a mutual authentication between the mobile user and MO while preserving mobile user's identity privacy and location confidentiality.

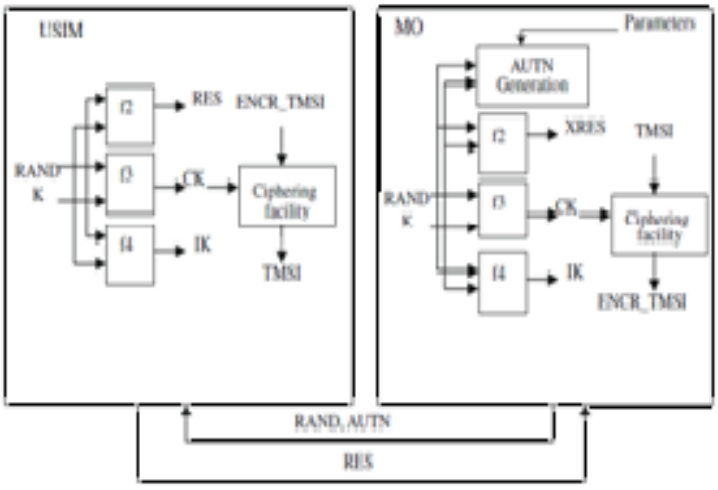

Fig.5. Simplified AKA-UMTS Mechanism

However, the UMTS-AKA mechanism cannot help a mobile device user and the user's service provider to authenticate each other In Improved Identity management protocol, this relationship exists between two independent individuals or between users and the service provider

D. IDM3G Protocol

IDM3G [7], based on a UTMS-AKA protocol on the 3G mobile network, focuses on cross-certification and administration between the service provider and users. Authentication and Key Agreement (UMTS-AKA) mechanism

 ISSN: 2321-8169
645 – 650

as their core element for entity authentication, user identity management, confidentiality and integrity The UMTS-AKA mechanism uses a pre-shared secure key (K) between the mobile operator (MO) and the UMTS subscriber identity module (USIM) of the mobile phone to perform authentication and key agreement. The USIM is a cryptography-enabled smart card identified by a unique 15-digit number, called an International mobile subscriber identity (IMSI)[8]. The USIM and the mobile operator can perform mutual authentication by a challenge and response mechanism.

The IDM3G protocol has two preceding phases as follows.

1. The user inputs a PIN to login in USIM according to the 3GPP specifications.
2. The USIM and MO finish mutual authentication according to the UMTS-AKA. During this period, the CK (for data encryption) and the IK (for integrity protection) are computed by both USIM and MO [9]. In addition,MO generates ENCR_TMSI by encrypting TMSI, and then sends ENCR_TMSI to USIM. The CK, IK, Auth, RAND and XRES compose a group of UMTS_AKA authentication elements called an authentication vector (AV), which is stored by MO during this connection. The IDM3G protocol is initiated when the user wants to connect to and to do so, they must authenticate with each other.

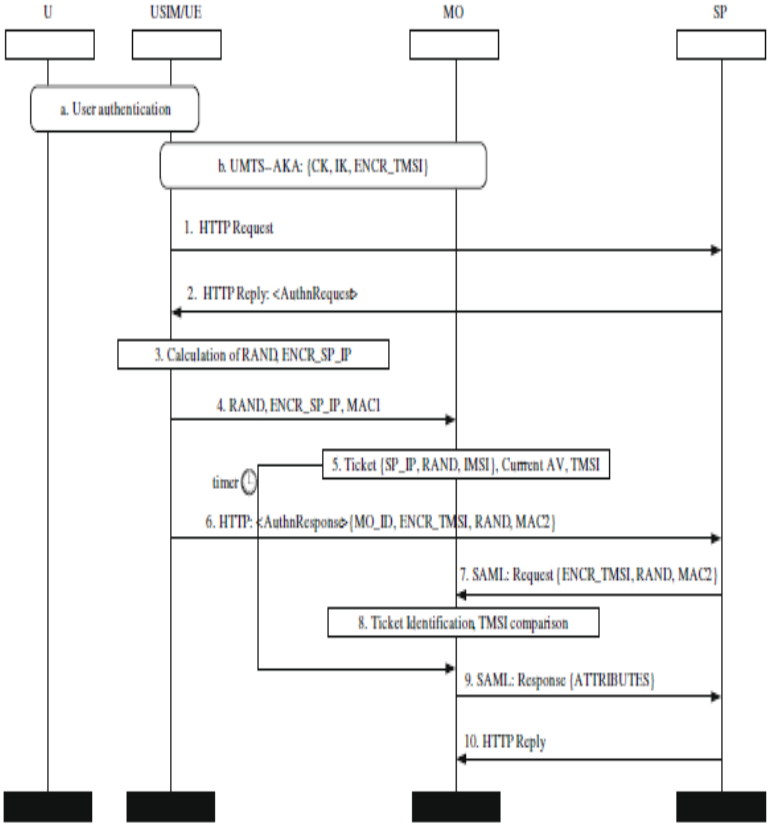

Fig.5. IDM3G Protocol Flowchart

In IDM3G the computation cost contains one random number generation, two message integrity checks, and six message exchanges, as well as ten computations for symmetric en/decryption. Our scheme integrates IDM3G to handle digital rights management over 3G networks [10]. In Table lists the number of computations and transmission rounds in our proposed scheme with IDM3G incorporated.

As showing the following table, in the online registration stage and login and access service stage. As well as, the number of symmetric key en/decryptions in the online registration stage and login and access service stage of our scheme is six times more than IDM3G.

Table 1: Number of exchanged messages

Protocol	Number of messages exchanged with the user client	Number of total messages
Liberty artefact profile for SSO	8	10
Liberty browser POST profile for SSO	8	8

Liberty-enabled client and proxy profile for SSO	6	12
Microsoft .Net Passport	8	8
IDM3G	5	7

III. PROPOSED METHOD

We are proposing the Improved Identity Management Protocol [11]for mobile cloud computing which has several advantages over the existing IDM3G Protocol [12],[13]. The proposed method builds the point of contact between service provider and mobile operator and thus allows them to keep log of user authentication and their access. Also this method minimizes the number of requests between user, service provider and mobile operator.

In the field of computing, Mobile Cloud Computing has brought a new dimension to Networking Service. The main vision of this service is interconnected "Mobile Cloud" where application providers and enterprises will be able to access valuable network and billing capabilities across multiple networks, making it easy for them to enrich their services whether these applications run on a mobile device, in the web. In this paper, the data security issues considering on mobile cloud computing [14] and securing mobile cloud computing user's privacy. This method generates the secret key for particular user on mobile operator end and passes this key to service provider. So when user tries to login to the service providers account, it will be authenticate through this key as well. It will help to mobile operators to keep the user authentication log.

IV. CONCLUSION

This paper proposes a system which is designed to improve the communication protocol in mobile computing. By improving means just to overcome the limitations of existing protocols. The Improved identity management protocol will minimize the network overhead for network companies which ultimately maintain the balance between profit and investment for network companies.

In our proposed scheme, we successfully improve upon IDM3G to design a fair and secure digital rights management of multimedia over 3G networks, which makes our proposed scheme more practical and easy to implement in the future. It also provides strong SP management and ease of use. And strong SP management may be more secure for implementation of in cloud computing environments Mobile cloud computing is one of mobile technology trends in the future since it combines the Advantages of both mobile computing and cloud computing, thereby providing optimal services for mobile Users.

V. REFERENCES

[1] In-Shin Park, Yoon-Deock Lee, Jonpil Jeong., "Improved Identity Management Protocol for Secure Mobile Cloud Computing" 1530-1605/12 $26.00 © 2012 IEEEDOI 10.1109/HICSS.2013.262

[2] Mont M, Pearson S, and Bramhall P., "Towards accountable management of identity and privacy,"Proceedings of 14th international workshop on database and expert systems applications, 2003.

[3] Damiani E, De Capitani di Vimercati S, and Samarati P."Managing multiple and dependable identities," IEEE Internet Computing, Vol.7(6), pp.29-37, 2003.

[4] Christos K. Dimitriadis and Despina Polemi, "An identity management protocol for Internet applications over 3Gmobile networks," Computers & Security, vol.25, pp.45-51,February 2006.

[5] A. Josang and S. Pope. User Centric Identity Management,In Proc. AusCERT, Gold Coast, May 2005.

[6] Authentication in the Clouds: A Framework and its Application to Mobile Users by Richard Chow.

[7] Pfitzmann B and Waidner M, "Analysis of liberty single-sign-on with enabled clients," Internet Computing, IEEE, vol.7, Issue:6, pp.38-44, 2003.

[8] Fry M, Fischer M, Karaliopoulos M, smith P and Hutchison D, "Challenge identification for network resilience", Next Generation Internet(NGI), 2010 6th EURONF Conference on, pp.1-8, 2010

[9] G.J. Simmons. An introduction to the mathematics of trust in security protocols. In Proceedings of the 1993 Computer Security Foundations Workshop, pages 121–127. IEEE Computer Society Press, Los Alamitos, CA, USA, 1993.

[10] ES-ARP: An efficient and secure Address Resolution Protocol Ataullah, M. ; Chauhan, N. Publication Year:2012 ,Page(s):-1TO 5 IEEE conference publication.

[11] Khan, M. ; Ahmed, A. ; Cheema, A.R. Software Engineering, Artificial Intelligence, Networking, andParallel/Distributed Computing, 2008. SNPD '08. Ninth ACIS International Conference on Publication Year: 2008 , Page(s): 350 - 355 .

[12] Kaaranen, Ahtiainen, Laitinen, Naghian, Niemi: UMTS Networks – Architecture, Mobility and Services. 2nd edition, Wiley 2005

[13] Foroughi, A., Albin, M., & Gillard, S. (2002). Digital rights management: A delicate balance between protection and accessibility. Journal of Information Science, 28, 389–395

[14] Cox, I. J., Miller, M. L., & Bloom, J. A. (2002). Digital watermarking. Academic Press .Dimitriadis, C. K., & Polemi, D. (2006). Identity management protocol for internet applications over 3G mobile networks. Computers and Security, 25(1), 45–51.