Anonymous Authentication Scheme in Smart Health to Secure Smart Health Records in Cloud

Miss. Sonali Khandu Satpute
Department of Computer Engineering
Amrutvahini College Of Engineering
Sangamner,India

Dr. Baisa L. Gunjal
Department of Information Technology
Amrutvahini College Of Engineering
Sangamner,India g

***Abstract*— As smart health care systems are providing cloud services to patients to store health records, security and privacy of data are crucial to its success while patients don't want to leak their identities. In protection of their identities, the authentication process normally includes disclosing users' personal data like username and password on authentication server. Patients privacy can be breached, in cases, if patient can be tracked or linked by malicious adversaries. Hence, in this paper, we have proposed a system that providing anonymity, security and privacy to the patient's of health care related sensitive data from the authentication server and adversaries. Our proposed scheme utilized rotating group signature scheme which is based on Elliptic Curve Cryptography (ECC) that provides anonymity to health records and to add an extra layer of protection at network layer ,we have used The Onion Router (TOR). The theoretical analysis evaluated schemes' performance, demonstrating that the scheme provides various security features as well as resistance to several attacks.**

***Keywords*— Smart Healthcare Systems, Anonymous Authentication, Rotating Group Signature, Anonymity**

I.INTRODUCTION

With growing popularity of cloud computing, many health care system adopting its services for various purpose. Because of many benefits cloud computing offering like scalability and cost saving ,the healthcare industries with massive amount of storage and computations are driving them to use cloud based servers. In recent past, many advances in embedded systems, biosensors and wireless network have great development of wearable sensors in the human body to gather all health records such as blood pressure level, heart rate. The hospitals have hosted their services on cloud servers where data from sensors sent here for data processing and data is analyzed to improve the level of healthcare. An example of smart cloud based healthcare system is shown in Fig. 1. Generally, patients want hospitals hosted with high efficiency without revealing their identities stored on cloud servers. Whereas, sharing data on un-trusted cloud servers can put patients privacy in danger as well as cloud computing may result in serious cloud specific. Privacy and security issues. Patients are always worried and hesitate to transfer their private or sensitive information to the cloud unless we provide complete security and privacy. To build a trustworthy and secure data storage or processing system in healthcare applications on the cloud, we must overcome some the challenges like losing physical control over data, multitanacy and privacy breach. We need to build mechanisms to protect users' privacy and protect their confidentiality and integrity to avoid risks associated with losing physical control over data as well as to get illegal access from malicious user to patients' data in virtualized environment. The traditional mechanisms to protect an individual's privacy may not be sufficient due to huge processing power. Users' online activities reveal a lot that cloud server or any eavesdropper analyze browsing habits and location footprints may be very risky. Our solution will provide an authentication scheme that discloses the identity of patient by using all healthcare services.

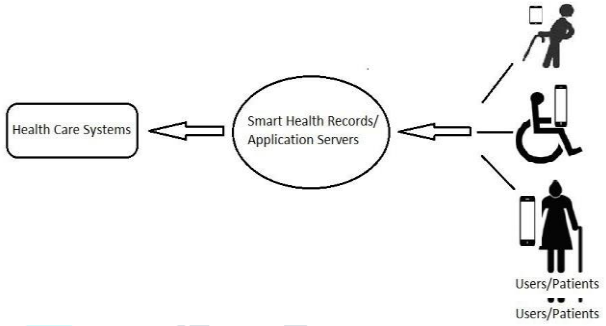

Figure 1. Smart Healthcare Systems

The operation of the proposed scheme is strong and attractive on cloud servers to store and hide the identities of patients giving priority to their privacy.

Problem Statement

Many privacy preserving authentication schemes have been proposed in recent past. However, those are not efficient to protect users' private/sensitive data over cloud servrs. There are some threats that can put it to danger while using services online. In healthcare systems, patient don't want to disclose their identity when using cloud services. Patients don't trust such applications until system commits full privacy and security to them. The stored data may be sensitive. Hence, the scheme should be trustworthy and secure. The identity privacy of a patient can be breached by revealing personal information such as username, history biometric features etc., used during the authentication process as well as extracting the information from the hidden patterns like patient's preferences or analyzing the internet traffic. The following lists we aim to achieve in our scheme:

- Patient get authenticate to authentication server anonymously without revealing any personal details.
- Multiple requests from same patient should not be able to link by authentication server and eavesdropper, for instance, patient may get identified.
- System should able to resists attacks like man in the middle, replay attacks, eavesdropping etc.
- Receiver should be able to verify the transmitting messages.

II.LITERATURE SURVEY

A. In group signature, without revealing the member identity, any valid group member allow to sign any number of messages on behalf of the group. Whereas, group manager have rights to reveal the identity of the signer when misbehaved .Most of the group signatures are based on traditional cryptography like ECC, RSA, and discrete logarithm. If quantum computers emerge, these schemes would be easily broken. In 2012, S. Kuzhalvaimozhi and Dr. G. Raghavendra Rao worked on new identity based group signature which based on bilinear maps with some security properties. In this scheme, the length of signatures are independent and the size of the group pubic key on the size of the group. The scheme was well suited for large groups where the group member can sign many messages using the same key pair.

This scheme have drawbacks. The identity based authentication systems suffer from the key escrow problem. The key needed to encrypt or decrypt is held in escrow so that under certain circumstances, an authorized party may gain access to the key. As the escrow agent holding all the cryptographic keys, the key escrow systems are considered as a security risk and may leak information or single failure point. Also, once a user's private key is compromised, it becomes very hard to revoke the user[2].

B. In 2009,Lin et al., worked on pseudonyms based schemes. The e-Health system is envisioned with a promising approach to improving health care through information technology, where security as well as privacy are crucial for and large scale deployment and its success. This paper addressed on a strong privacy preserving Scheme Against Global Eavesdropping, named SAGE, for eHealth systems. The proposed SAGE can achieve the content oriented privacy also the contextual privacy against a strong global adversary. The SAGE has been demonstrated efficient in terms of transmission delay.This scheme had major drawback that it was impractical due to heavy computational overhead when directly applied to the distributed healthcare systems. The scheme could not bear the heavy computations[3].

C. In 2016, Djellalbia et al. proposed anonymous authentication scheme in cloud environment for s-health. The adoption of an e-Health Cloud has different benefits especially sharing, storing, allowing and exchanging information between various medical institutions, reducing cost , availability of information, reducing costs, fast services etc. Besides, preserving identity privacy is a significant challenge of security in all environments as well as constitutes particularly a very serious concern in cloud environments. It puts to the first priority of user while using services. Indeed, an important barrier to the adoption or usage of cloud user is fear of privacy loss in the cloud server, particularly in an e-Health cloud where users are patient with sensitive data or information. Users/ patients may don't want to disclose their identities to the Cloud Service Provider when using its services. A way to protect them is making them anonymous over the servers . This paper proposed an adaptive and flexible approach of patients' identity privacy to protect in an e-Health Cloud through an anonymous authentication scheme. This scheme is based on blind signatures which allow patients to consume cloud services anonymously over the world. The system lagged to provide any details about user registration and revocation. Discussion details about security analysis not provided [4].

D. Li et al. researched on application oriented scheme about Wireless body area networks (WBANs).That are widely used in telemedicine, which can be utilized for home health-care and in real-time patients monitoring . In WBANs, the sensor nodes gathers the client's physiological data. Transmit it to the medical center ,the clients' transmit it to the medical center ,the clients' personal data / information is sensitive and there are much security threats in the extrabody communication. Hence, the privacy and security of client's physiological data need to be protect and ensure first. Many existing authentication protocols for WBANs failed to consider the key update phase. This paper propose proposed an efficient authenticated key agreement scheme for WBANs plus to add the key update phase in enhancing the security of the scheme. In authentication phase, to reduce the computation cost , session keys are generated during the registration phase and kept those secretly. The scheme was more efficient based on bilinear pairings but the revocation process was not clearly defined in case of dispute[5].

E. In the additional work for Wireless Body Area Network(WBAN) Chhajed et al.proposed an authentication scheme .WBAN is a service which is efficiently used in today's time For providing efficient and secured healthcare services. This paper included Certificateless over wireless network scheme for the security purpose. Additionally, a pair of security protocols are been used in both end user and service provider. This scheme was propose to implement anonymous light-weight authentication protocol. A WBAN user can easily access the telemedicine system through this protocal. Using WBAN services, the physician receive updates and the real-time information of the patient. The Certificateless Signature (CLS) scheme is almost used to uniquely meet the security preserving demands in WBAN by certificateless encryption also designed to eliminate the drawbacks of the PKI based scheme and it does not require identity based encryption and digital certificate, i.e., no key escrow problem. CLS assigned the security by providing private keys to the patient because of that it is impossible for the third party or the attacker to access the private information of particular session happened during authentication process. The scheme also gave big drawback of revocation procedure detailing improperly[6].

F. Sudarsono et al. proposed an anonymous authentication scheme for wireless networks using Verifier Local Revocation (VLR) group signature scheme. In the advancement of data centric technologies and the Internet of Thing in collecting and distributing sensory data, security and privacy becomes most important and desirable priorities. This concern is because of sensory data are commonly transmitted on wireless networks toward data center which are easily or generally observed for the target l of network traffic analysis. Beside, the collected data in data center can be easily accessed by other users, hackers as well if the system does not deal with any proper security mechanism. In this proposed anonymous authentication system of pairing-based verifier-local revocation group signature scheme, that authenticates wireless nodes (i.e., sensor nodes) of a particular privilege group to the gateway node in transmitting data. An additional achievement is anonymous authentication for accessing data to the data centre . Where the scheme vulnerable to replay attacks also a malicious Group Manager can impersonate a user[7].

Keywords	Long Forms
ECC	Elliptic Curve Cryptography
TOR	The Onion Router
RS	Registration Server
s-Health	Smart Health
CSP	Cloud Service Provider
RSA	Rivest, Adi, Shamir

Table 1. Keywords and Long Forms

III.PROPOSED METHODOLOGY

The proposed anonymous authentication scheme utilized a rotating group signature scheme based on ECC , that provides anonymous authentication in smart cloud based healthcare applications to prevent users from untrusted authentication server and against eavesdropping.

In case of a malicious activity, proposed scheme provides a mechanism for traceability with minimal compromise on privacy. Each group shares an expiration date to remind members renew their keys regularly and to minimize authentication time. Also the need to reveal a member's past authentications when their key is revoked. Besides, anonymous authentication systems are generally considered in isolation. Cloud service provider operating over the internet can link subsequent requests by IP address by connecting them to a physical location or an individual. Hence scheme used TOR that provides anonymity to users on the network level and minimize the information available to cloud service provider. By non anonymous fashion, TOR hidden service cannot be accessed. It complements anonymous authentication schemes good, leaving the service provider with little information to link subsequent connections. Instead of using a direct connection, internet users employ TOR network by connecting through a series of virtual tunnels that it protects against traffic analysis attacks which may be used over a public network to infer who is talking to whom.TOR connected by 3 relay nodes as middle relay nodes are used to transport traffic from the entry nodes to exit nodes also prevents the entry and exit node from knowing each other . However, exit nodes send traffic to the final destination intended by the client. Each node knows decryption key for encryption. In our scheme we have employed TOR at server side, has a program to run two hidden services, pointing to a program running on CSP's and RS's portions of the protocol. While at client side TOR can be used as a proxy application to encrypt the internet traffic. By bouncing through the series of computers it can hide around the world.

A. System Architecture

Module:

1. Trent Module
2. Cloud Service Provider Module
3. Registration Server Module
4. User Module

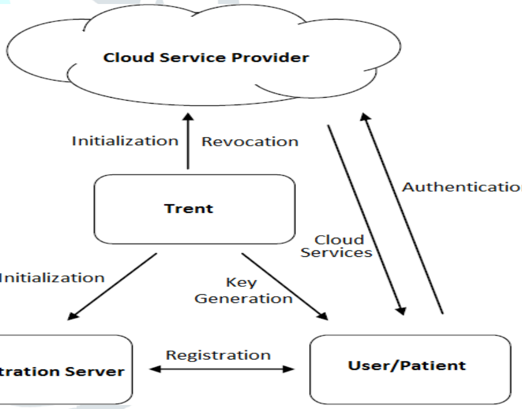

Figure 2. System Architecture

Module Description:

1. Trent Module : Trent presented as clinic ,is trusted party that outsourced its infrastructure to CSP. Responsible for initializaton, revocation, key generation and auditing.

2.Cloud Service Provider Module : CSP provides services to users by key exchanging. It is an un-trusted entity can gain much information of user during authentication process where information provided by Trent and RS. User may able to hide identity from CSP.

3.Registration Server Module : RS only does the registration process of user to initiate system entrance. It exchanges information to Trent and CSP as per requested.

4.User Module : User accesses the cloud services from CSP with autherised account to RS. User requests to CSP for services without disclosing their identity with exchanging some keys provided from Trent.

B. Design Details

Anonymous Authentication scheme includes 5 phases:

1. Initialization
2. Key Generation
3. Registration
4. Authentication
5. Revocation

Description :

1. Initialization : Trent generates private-public key pair and give public half to CSP and RS. With range of pairings users must use agreed pairings. Once Trent sets up the system, initialization is done.

2. Key Generation : Trent generates group key that valid for some time, master group key and from that derives public group key which is partially random and partially derived from group manager key. Trent generates a signed certificate containing information. Trent encrypts and sends that certificate to CSP and RS by using its public key.CSP and RS decrypt and verify that the certificate is actually from Trent with the help half public key given previous. Trent has to update group keys every time of same key generation process.

3. Registration : User registers to RS to get a key for the current group by joining and demonstrates identity to RS. RS verifies that user is authorized to use CSP's services of the current group, it shares bilinear pairing parameters from the initialization phase and signed from the key generation phase. User and RS generates random number. User sends parameter to the RS who derives variable from it and sends it back to user, who verify successful joining. This registration process leaves user with a member key and RS with a transcript that encrypted along with user's identity using encryption key and records it in registration log.

4. Authentication : User wishes to request a service to CSP and begins the authentication process. User connects to CSP over an anonymous network and sends the group key to authenticate. CSP verifies the group key matches a stored certificate sent by Trent and should not expired. CSP generates a random number and sends it to user. User and CSP perform a zero knowledge protocol. User generates signature and sends it and request to CSP. CSP continues to next step if the equality holds true/valid signature otherwise terminates the connection. CSP also checks that user didn't perform the protocol with the revoked key.CSP encrypts and performs the requested service with encryption key and save in the audit log that only Trent may read it.

5. Revocation : When Trent found that a user has been abusing the services, he revokes user's key. Key revocation necessary allows untrusted CSP who keeps an unencrypted log to link all of user's connections and should not be used primary not by terminating a client's service. Trent requests the registration log and audit log from RS and CSP respectively and decrypts it to get requests. Trent uses group signature master key and the list of transcript of process to extract which group member held signing key to signed the message and consumed which service. Trent tests for each record in registration log, if a match is found, Trent computes the corresponding parameter and adds it to revocation log. Trent shares the tracing information for user with CSP to revoke user's membership key. In order to allow CSP to get proofs of membership created by user and refuse giving services to him. RS removes user from list of acceptable clients when Trent sends user's identity to it.

C. Algorithm

ECC is public key cryptography algorithm applicable for key agreement. The equation of an elliptic curve is given as $y^2= x^3 + ax + b$

1) Key generation:

Public key and private key generated. The public key generation equation : $Q = d * P$

Where k and d is random number selected within the range of (1 to n-1),P is the point on the curve and Q public key and d is the private key.

2) Encryption :

Input
1.string=message M(plain text)
2.public key=key
Literal types as Plain text, encrypted text
Output

1. START
2. Init = (ENCRYPT MODE, key)
3. Plaintext = Input message
4. EncryptedText - do Final (plaintext)
5. EncryptedString =cipher text
 cipher text 1 = k*P
 cipher text 2 = M +k*Q
6. Return encrypted String.

3) Decryption : Input
1.string=cipher text
2.private key=key
Literal types as Cipher text, decrypted text
Output

1. START
2. Init - (DECRYPT MODE, key)
3. Ciphertext – cipher text
4. DecryptedText - do Final(ciphertext)
5. DecryptedString –messageM(plaintext)
 M = cipher text 2 d * ciphertext1
6. Return decrypted String

D. Mathematical Model

Set Theory

Consider S be the whole system,
S ={I, P, O }

P=Process O=Output I = Input
Set I
I= {I0, I1, I2, I3, I4, I5, I6}
I0= Identity of User
I1= To Upload File on Cloud
I2= Total Group Members Numbers
I3= Public or Private Key
I4= Details of User
I5= Details of Cloud server
I6= Activities of Cloud User
Set P
P={ P0, P1, P2, P3, P4, P5, P6}
P0= Public/Private Keys Generate
P1= Registration Servers Login
P2= Certification Process
P3= Cloud Account Creation
P4= To CSP file Upload
P5=Activities of monitor User
P6= Revocation of User
Set O
O= {O0, O1}
O0= Anonymous Authentication of User
O1=Identity Hide

Venn Diagram:

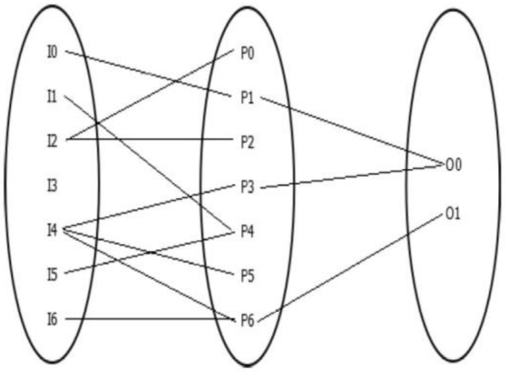

Figure 3 .Venn Diagram

E. Requirement Specification

1. Software Requirements
Microsoft Windows 7 and Above
Net Beans IDE 8.2
Java Development Kit (JDK)1. 7
Mysql 5.5 onwards
Application server Tomcat 5.0

2. Hardware Requirements
Processor above 1GHz
1 GB RAM
Speed : 1.1 GB(min) Hard Disk : 20 GB
Standard Key Board, Mouse, Monitor with Normal Resolution
LAN Connection

IV. EXPERIMENTAL RESULT

A. Result Analysis

By studying other techniques we got information that privacy preserving authentication schemes are lagging to ensure the privacy of patients' sensitive data by disclosing personal details while using services. If we are using this scheme in military, banking sectors, healthcare sectors, etc. our scheme is better to keep service provider unaware from the private information of users such as access tokens and access history, resistant to attacks, hiding identity.

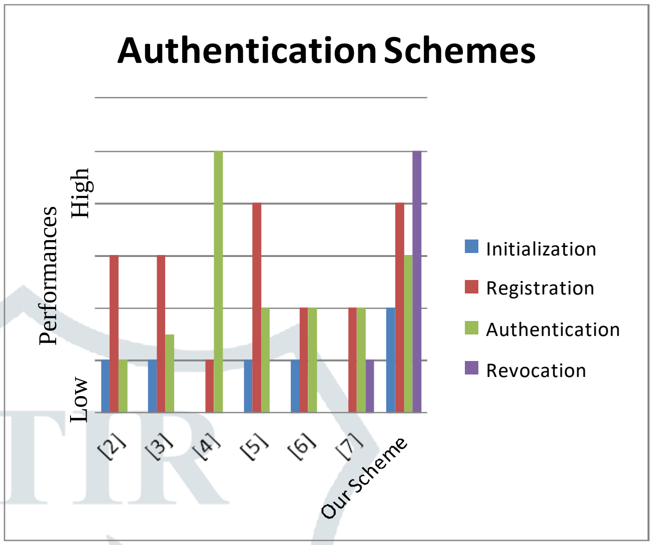

Figure 4. Comparison of phases performances between our scheme and existing schemes

B. Comparison with Existing Scheme

The protocols selected for comparison are [2], [3], [4], [5], [6], [7]. Table 2 and figure 4 show comparison between existing selected schemes and our scheme. We can see from the table 2 that our scheme achieves all features anonymity, authentication, forward unlinkability, revocation, traceability, integrity, resistance to replay attack. Where other existing schemes not touches to all features. Also our scheme has high communication skills than other protocols. Figure 4 shows the performances of authentication schemes with low to high range. We can say that our anonymous authentication scheme performs best in all phases, initialization, registration, authentication and revocation. While other existing schemes lagging in every other phase to give better performance. Hence our scheme is the best technique among others.

V. Conclusion

Finally concluded to anonymous authentication scheme for smart cloud based healthcare applications by preserving the privacy of patients when they access the services hosted on the cloud.By utilizing ECC and TOR mechanism,we have proposed a practical system ensures that the patients can consume services without revealing their identity with security from an eavesdropper .

Features	[2]	[3]	[4]	[5]	[6]	[7]	Our Scheme
Anonymity	✓	✓	✓	✓	✓	✓	✓
Authentication	✗	✓	✓	✓	✓	✗	✓
Forward Unlinkability	✓	✗	✓	✗	✓	✓	✓
Revocation	✗	✓	✗	✓	✗	✓	✓
Traceability	✓	✓	✓	✓	✗	✓	✓
Integrity	✗	✓	✓	✓	✓	✓	✓
Resistance to Replay Attack	✗	✓	✓	✓	✓	✗	✓

Table 2. Comparison of features between our scheme and existing schemes

Acknowledgement

It gives me an immense pleasure to express my sincere and heartiest gratitude towards my guide **Dr. B. L. Gunjal** for her guidance, encouragement, moral support and affection during the course of my work. I am especially appreciative of her willingness to listen and guide me to find the best solution, regardless of the challenge. This work is also the outcome of the blessing guidance and support of my parents and family members and friends. I am also thankful to all who have contributed indirectly and materially in words and deeds for completion of this work.

References

[1] Abid Mehmood, Iynkaran Natgunanathan, Member, IEEE, Yong Xiang,Senior Member, IEEE, Howard Poston,and Yushu Zhang, Member, IEEE Anonymous Authentication Scheme for Smart Cloud Based Healthcare Applications IEEE Access, DOI 10.1109/ ACCESS.2018 . 2841972

[2] S. Kuzhalvaimozhi and G. R. Rao, "An efficient scheme for anonymous authentication using identity based group signature," IET, 2012.

[3] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: A strong privacy-preserving scheme against global eavesdropping for ehealth systems," IEEE J. on Selected Areas in Commun., vol. 27, no. 4, pp. 365–378, May 2009.

[4] A. Djellalbia, N. Badache, S. Benmeziane, and S. Bensimessaoud,"Anonymous authentication scheme in e-health cloud environment," in Proc. 11th Int. Conf. on Internet Technology and Secured Trans., Dec. 2016, pp. 47–52.

[5] T. Li, Y. Zheng, and T. Zhou, "Efficient anonymous authenticated key agreement scheme for wireless body area networks," Security and Commun. Networks, vol. 2017, Oct. 2017.

[6] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," IEEE Trans. on Parallel and Distributed Syst., vol. 25, no. 2, pp. 332–342, Feb. 2014.

[7] A. Sudarsono and M. U. H. Al Rasyid, "An anonymous authentication system in wireless networks using verifier local revocation group signature scheme," in Proc. Int. Seminar on Intelligent Technology and Its Applications, Jul. 2016, pp. 49–54.