HYBRID DATA SECURITY MECHANISM FOR CLOUD STORAGE SYSTEM

K. Selvamanigandan[1], S. Sasikumar[2], R. Sathishkumar[3], V. Sureka[4]
Computer Science and Engineering, S.A. Engineering College

Abstract

Hybrid data security mechanism for cloud storage system is used to improve a data security protection mechanism for cloud by using mobile application. Authentication and secret key (IMEI) are the two component to protect unauthorized third parties. A promising solution to offset the risk is to deploy encryption technology. There are many benefits to use cloud storage. The most notable is data accessibility. Data stored in the cloud can be accessed at any time from any place as there is network access. The security and efficiency analysis show that our system is not only secure but also practical.

Index Terms: Hybrid factor, factor revocability, security, cloud storage

I. INTRODUCTION

Cloud storage is the model of the network storage system where the data's are stored in huge collection which are generally hosted by third parties. There are many benefits to use cloud storage through android application. The most notable is data accessibility. Data stored in the cloud can be accessed 24*7 through mobile application as long as there is network access. Storage maintenance tasks, would be off loaded to the responsibility of a service provider. Here data's are kept so secured by using two way authentication process.

One way is using password and the next way is using IMEI number of a particular mobile, where only registered mobile can only access the data's that are stored in the cloud. Despiteit'sadvantages,outsourcing the storage of data also increases the attack on the surface area at the same time. For example, when data is distributed, the more locations it is stored the higher risk it contains for unauthorized physical access to the data.

What is Android?

Android is a most improving operating system developed by Google, based on the Linux kernel and designed primarily for touch screen mobile devices known as smart phones and tablets. Android has the largest usage base of all operating systems(os) of any kind. Android has been best sellingos on mobile phones and tablets since 2007and it is dominant by any metric. Android's source code is released by Google, under open source licenses. The success of android has made it a focus for patent litigation as part of "smartphones wars" between technology companies.

II. Related works

Vinodvaikuntanathan[1],Cryptography is highly secure against the memory attacks. A bit of secret key of a crypto system is measured by the key that is stored in a part of memory which would be accessed even after the power supply is stopped for some amount of time. These kinds of crypto attack rather accept the security of various crypto systems, including RSA and AES crypto systems. Public key encryption scheme and identity based encryption scheme are highly vigorous or strong against memory attack it can calculate the arbitrary function of the secret key can be calculated at the edge of the output key length. It is more highly done

without increasing the length of the secret key and without introducing any complication on it's natural encryption and decryption process.

Sattam.s[2],This paper makes the concept of certificatelesspublickey cryptography. This model of publickey cryptography mostly avoids originality based crypto system hence does not requires certificates for authentication of publickeys.Here it as been focused on (cl-pke),which is more secured and its related to bilinear problem

Man Ho Au[3],Group oriented signatures include signatures like ring signature where designer can continuously form a group and produce a signature that are verified and convinced, Here it is difficult to find who actually signed. In the ring signature no two signatures can be linked only if the same signature is signed by the user at different times. Only recent times ring signature has been formed. It is mostly underseen by security definition in ring signature. New model is highly strong than all the underlyinmg systems in literature, here they have proposed a short linkable ring signature and hence improved upon upcoming schemes.

Jing chen[4],In this systems they have proposed identity based system,where they have inherit key issues which is key generation center who always knows the secret key. KGC which is more vulnerable KGC starting the launching attacks which is known as type 2 attack only it is possible after the generation of master public key pair respectively. Here new security models has been proposed to overcome this this assumptions for the certificateless signature and the crypto system encryption schemes. Relatively shown that certificateless encryption schemes proposed are highly insecured.it still suffer escrow problem, they have given new proofs that they posses generic construction where certificateless signature and encryption are secured under new models.

Matt Blaze[5],The notation of divertibility has a protocol property where the language property has been omitted highly. Blind signature protocols is the one which is recently found one. In this atomic proxy cryptography, it convert the cipher text for the messages or signature that converts for another cipher text respectively. Proxy keys that are once generated can make use of the function that are applied to the untrusted environments. It is mainly focused on the discrete log based encryption methods where divertibility and proxy cryptosystems are mainly focused.

June's Liu[6],This paper makes the certificateless public key cryptography(CL-PKC) a model for the use public key cryptography that avoids existing of the identity based cryptography this involves no certificate for authenticity of public keys. The existing lack of certificate problem and resists the access to master key and development of new security model. The main aim of paper is to provide certificateless public key encryption(CL-PKE) , it shows the concrete pairing based(CL-PKE)which provides essential security for the above mention related problems but it is pretty hard for Diffie- Hellman problems.

Guojunwang[7],Cloud computing is the most emerging and highly used storage services across all platforms. It enables users to remotely store the data. As it is highly used for the companies with limited budgets where, from hosting to deployment can be done effectively. Cloud service providers which are not the same trusted domain are known as enterprise users as it takes care of confidential data and the privacy issues are highly maintained. To keep the user data more sensitive and confidential against the CPRs, a natural way to apply cryptographic approaches respectively. As it provides high performance, delegation and the scalability and the best thing is data can be accessed anytime anywhere without any limitations. Here the goal is achieved by hierarchical identity based encryption systems.

FenghеWanga[8],An efficient identity based encryption scheme above lattice is proposed here.

Inorder to learn the strength of the errors that are to be noted is highly semantic secure against all odds of plain text attacks in the underlying model. In order to improve the efficiency of the lattice based IBE scheme, identity string is encoded in the matrix where several known constructions. With the help of this idea it is possible to extract the IBE scheme of the same lattice . Public key of the proposed scheme consists of n x m matrix and 1+1 vectors. Hence the public key size of this schemes is shorter than that of those known constructions.

Brent Waters[9],In this new methodology for realizing the policies of the cipher text that allows non-interactive cryptographic assumptions. For an efficient system size of the cipher text ,encryption and the decryption all factors matters the most. The previous models have limited proof for the generic model. There are three constructions which are present inside the framework . First system is more secure under the PBDHE method . Next two systems provide performance trade off.

RulyingDu1[10],In the past decade or so cloud has been the emerging and the most influential one in the It sector. Hence for its high popularity and high usability it is more and more vulnerable to the users. This system is highly and more selectively secure which is called as (PBDHE). And the next two systems provide a detailed information of the FEACS, where the4 comparison are made to be with the existing schemes as it is more effective for the cloud storage environment.

Alexandra Boldyreva[11],In this paper a fully fledgedidentity based encryption has been proposed. This method has chosen the message security in a continuous model of the oracle in the form of a elliptic curve variant of the working device. They are mainly based on the most common pairing known as Weil pairing, as it provides the precise information and the security identity depending encryption provides several applications for more and more utilizing systems. Here data are to be encrypted more and more likely to be highly used where the messages are kept so confidential. Alice and Bob are two famously known characters because of the cryptosystems that are highly used. In case of data theft scenarios where messages are possible to be hacked by the intruders who needs to get rid of the information that are to be passed. Hence here the datas are to be highly kept classified by using the third party vendors who provide such kind of multiple factor security for the data that are stored in the devices. It also formally capture security for the Pre schemes to the simulation based systems.

Ran Canetti[12],The most important thing that is taken into consideration is the proxy re-encryption steps. Here the proxy is allowed and given the necessary permissions and adaptations that to allow and convert the proxy address and the cipher text that are to be converted to another cipher text of the same message that are under the same private key. The main advantage of this is that the proxy cannot read any information that are converted into cipher text either under the key, it does not know about any kind of information about the message. Even if the intruder tries to take the proxy for being granted they are not allowed to know the data source that are stored as a unique addresses which are invisible to the intruders that provides high range of security that is what needed. Previous systems made had been known for the re-encryption schemes that is achieved only through the semantic security. More often it is taken to be noticed only for the particular cipher text attacks. It also captures the highly needed CCA security for the PRE schemes.

Tabulation

The following table shows the different technologies used in every paper has been analyzed

Reference Tiltle	Authentication	secret	Applied in real world
Simultaneous hardcore bits andcryptography	Yes	No	No
Certificateless public key cryptography. In ASIACRYPT	Yes	Yes	Yes
Certificate based (linkable) ring signature	Yes	No	partially
Malicious kgc attacks in certificateless cryptography	Yes	No	Yes
Divertible protocols and atomic proxy cryptography	Yes	Yes	No
Identity- based encryption with efficient revocation	Yes	Yes	No
Identity- based encryption efficient	Yes	No	No
Identity-based encryption from the weil pairing	Yes	Yes	Partially
Fine-grained control of security capabilities	Yes	No	No
A networkcoding-based storage system in a cloud-ofclouds	Yes	Yes	No
Key- aggregate cryptosystem for scalable data sharing in cloud storage	Yes	Yes	Yes

III. EXISTING SYSTEM

In this system it has two factors those two factors are 1. Authentication and the other is riddle key. Authentication is nothing but making the system more secure and making sure that it is not being accessed easily by any unknown users or the intruders. During the authentication process the user is provided with a user name and the password where the user name must be so specific where it should not be repeated for any other user hence that is maintained and the other one is password where passwords are kept so confidential, in order to maintain intrusion free source. Riddle key is also known as secret key. Where the sender and the receiver only knows the key that has been made. Here symmetric algorithm had been used. This system has some disadvantages hence it can be improved with more security features, that is what enhanced in this project.

IV. CONCLUSION

This paper has been focused on the data privacy and authentication security issues. In this hybrid authentication mechanism is used which provides a belief for better authentication than the password based system. Since the password has been stored in the hash format, it is not possible to hack and get the password as it is stored in the format that is not understandable by the attacker. As the data are uploaded to the cloud storage it is encrypted and stored where it is not possible to get the data at any instincts. It is safe from the attacker and the csp. Only the authenticated mobile with the IMEI can access the data from the cloud. It is not possible to access the data by the same user with different mobile, since it's IMEI is entirely different it does not log on to the cloud and it also alerts the user with a warning message to the registered mobile number. Successful implementation will provide the user it's assurance about the data security and the authentication.

REFERENCE

[1]A.Akavia, S.GolgWasser and VinodVaikuntanathan. " Simultaneous hardcore bits and cryptography". In TCC, volume 5444 of Lecture Notes in Computer Science, pages 474-495. Springer, 2010

[2] S.Sattam S. Al-Riyami and Kenneth G. Paterson. "Certificateless public keycryptography. In ASIACRYPT", volume 2894 of Lecture Notes in Computer Science, pages 452-473. Springer, 2011.

[3] Man Ho Au, Sherman S.M. Chow, Willy Susilo, and Patrick P. Tsang. Certificate based (linkable) ring signature. In ISPEC, volume 4464 of Lecture Notes in Computer Science, pages 79-92. Springer, 2012

[4] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang. Malicious kgc attacks in certificateless cryptography. In ASIACCS, pages 302-311. ACM, 2013.

[5] M. Blaze,G. GerritBleumer, and M. Martin Strauss. Divertible protocols and atomic proxy cryptography. In K. Nyberg, editor, EUROCRYPT, volume 1403 of LNCS, pages 127-144. Springer, 2009.

[6] A. Boldyreva, V. Goyal, and V. Kumar. Identity- based encryption with efficient revocation. In P. Ning, P. F. Syverson, and S. Jha, editors, ACM Conference on Computer and Communication Security, pages 417-426. ACM, 2009.

[7] D. Boneh, X. Ding, and G. Tsudik. Fine-grained control of security capabilities. ACM Trans. Internet Techn., 4(1):60-82,2004.

[8] D.Boneh and M. Franklin. Identity-based encryption from the weil pairing. In CRYPTO '01, volume 2139 of LNCS, pages 213-229, Springer, 2010.

[9] R. Canetti and S. Hohenberger. Chosen-cipher text secure proxy re-encryption. In P. Ning, S. D. C. diVimercatti, and P. F. syverson, editors, ACM conference on Computer and Communication Security, pages 185-194. ACM, 2007.

[10] H. C. H. Chen, Y. Hu, P. P. C. Lee, and Y. Tang. Nccloud. A network-coding-based storage system in a cloud-of-clouds. IEEE Trans. Computer, 63(1):31-44,2014.

[11] S. S. M. chow, W. G. Boyd. Nieto Security-mediated certificateless cryptography. In Public Key Cryptography, volume 3958 of Lecture Notes in Computer Science, pages 508-524, Springer, 2013.

[12] C. K. Chu, S. S. M. Chow, W. G. Tzeng. Key- aggregate cryptosystem for scalable data sharing in cloud storage. IEEE Trans. Parallel Distrub. Syst.,25(2):468-477,2014