International Journal of Engineering & Technology, 7 (2.7) (2018) 108-113

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

SAML based context aware IDM a fine-grained proxy re-encryption approach to improve the privacy of users identity data in cloud environment

T S Srinivasa Reddy Modugula[1]*, B. Vijaya Babu[2], Sunitha Pachala[3], Rupa Chiramdasu[4], L. Sumalatha[5]

[1]Department of Computer Science and Engineering, M.Tech Scholar,
Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India
[2]Department of Computer Science and Engineering, Professor,
Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India
[3]Department of Computer Science and Engineering, PhD Scholar, (JNTUK), Asst.Professor,
Dhanekula Institute of Engineering and Technology, Ganguru, Vijayawada, India
[4]Department of Computer Science and Engineering, Professor,
Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, India
[5]Department of Computer Science and Engineering, Professor,
Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh, India
*Email: *mtssreddyteja@gmail.com*

Abstract

Cloud computing has made tremendous changes in IT industry by offering various services ranging from Iaas, Saas, Paas, Daas, IDaas to Xaas i.e. everything as a service. Identity as a service is one of the popular service offered by cloud providers which is used for Identity and Access Management which reduces the burden of identity management to companies. As the Identity data of user's moves out of organizational boundaries to cloud servers, the control over identity data is lost thereby security and privacy issues arise. To address these issues many Identity management systems have been proposed but none of them provided privacy at the fine-grained level. In this paper, we propose a SAML based ContextawareIdM, a model for fine-grained privacy-preserving identity as a service which employs Identity-based conditional proxy re-encryption to maintain and operate identity data's privacy at a fine-grained level.

Keywords: *Cloud computing; Identity management; privacy-enhancing; cloud security; data protection; securing digital identities.*

1. Introduction

In Identity management systems the main role is to manage the identities of users of an organization, traditionally this identity and access management systems are on-premise i.e. within the organizational boundaries, which is an additional overhead to maintain and operate them, but nowadays with the widespread services of cloud computing, the identity as a service has evolved where organizations outsource the identity data of users to cloud provider that acts as identity provider which is responsible for managing the identity and access management processes. When a user wants to access a service offered by service provider then he need not register with it, he can get verified with pre-registered identity provider, this happens with the help of Identity management protocols like SAML, OPENID etc. where the service provider requests the identity provider to authenticate user and provide some SAML assertions about user and based on the SAML response of the identity provider the service provider provides the requested service to user ,this scenario reduces the burden of remembering a number of usernames and password credentials to users and reduces management overhead to organizations. As data moves to the cloud there may arise numerous problems like security breaches, the privacy of identities of users are at risk, and sometimes even the identity provider may share the identity data to others for gaining money or due to some legal regulations. To address these issues various identity management approaches were designed where the identity data is encrypted by the users or organization before transferred to identity providers so that the identity provider can neither understand nor use it for other purposes, some of the systems employed proxy re-encryption schemes to maintain privacy of identities of users where the identity provider with the help of reencryption key can transform the encrypted identity attributes to another form which can be decrypted by appropriate service provider there by identity provider and service provider cannot collude with each other in order to obtain any key related information and also privacy of identity data is maintained up to some extent but not at the fine grained level. So, in order to maintain privacy at fine-grained level in this paper we propose a ContextAwareIdM which offers a fine-grained privacy-preserving identity as a service where the identity attributes are encrypted with user’s identity and a context/tag and are outsourced to identity provider and those ciphered attributes satisfying specific context/tag can be re-encrypted by the identity provider which can be decrypted by appropriate service provider with its secret key.

2. Literature Survey

2.1. Proxy re-encryption schemes

Blaze et al. [1] proposed an atomic proxy re-encryption scheme where a partly trusted proxy converts ciphertext for a user A in to cipher text for another user B without getting through the underlying plaintext, although it is easier to implement this scheme, it suffers from considerable security problems as this scheme is bidirectional, transitive and prone to collusion. Dodis et al. [2] presented a unidirectional proxy reencryption for RSA, ElGamal, and Identity-based encryption schemes by sharing user A's private key between two parties (proxy and another user B). This overcomes some of the problems of Blaze et al. [1] but it is not collusion safe and secret sharing is an extra overhead. Mambo et al. [3] have proposed a public key proxy cryptosystem that allows an original decryptor to transform its ciphertext to a ciphertext for a designated decryptor, proxy decryptor where the actual decryptor decrypts its ciphertext and re-encrypts an obtained plaintext under a designated proxy decryptor's public key. Then the designated proxy decryptor can read the plaintext. Ateniese et al. [4] presented an improved proxy reencryption scheme with applications to secure distributed storage, their scheme is extended on Dodis and Ivan's work, and this improved scheme is unidirectional and collusion safe and is useful for enforcing controlled access to SFS read-only file system. Green et al. [5] proposed an identity-based proxy reencryption where the ciphertexts of one identity (user A's) are transformed to ciphertext of another identity (user B's) and the proxy uses proxy keys, or re-encryption keys, to complete the translation without being able to learn the plaintext. Moreover, no information on the secret keys of user A and user B can be deduced from the proxy keys and this scheme supports multiple re-encryptions and its security is based on the standard assumption in random oracle model. Chu et al. [6] have proposed a basic unidirectional conditional proxy broadcast reencryption scheme which overcomes the problem of identity-based proxy reencryption where it is limited to a single receiver i.e. for multiple receivers IBPRE should be executed multiple times and in the chu's scheme, with the use of condition-based encryption, it allows a fine-grained decryption rights delegation and also allows giving decryption power to group of users at a time. And this scheme is proved secure against chosen ciphertext attack in the standard model. Ateniese et al. [7] proposed a key Private proxy reencryption scheme, which aims at providing key privacy where even the proxy who performs the transformations can't differentiate the identities of the participants and this scheme is proved to be chosen plaintext secure under simple Decisional Bilinear Diffie Hellman assumption and its key-privacy under the Decision Linear assumption in the standard model and it is applicable to applications like secure distributed file system. Tang et al. [8] have proposed a construction of type based proxy reencryption which provides selective delegation of decryption rights to delegatee by the delegator with only one key pair which allows the delegator to implement fine-grained access policies without any added trust on the proxy which differs from traditional pre-schemes where delegatee can decipher all ciphertext for the delegator after proxy has done reencryption. Tang has proposed two type-based proxy re-encryption schemes in which one is CPA secure with ciphertext privacy while the other is CCA secure without ciphertext privacy. Goyal et al. [9] have proposed an attribute-based proxy reencryption scheme which allows a partly trusted proxy to convert a ciphertext under a group of attributes to a new ciphertext under another group of attributes using some additional information. There are two types of attribute-based pre-schemes, one is key policy attribute-based encryption and other is ciphertext policy attribute-based encryption. In key policy attribute-based encryption scheme, every ciphertext is named with a set of attributes by the encryptor and every private key is bound with an access scheme that indicates which type of ciphertexts can be decrypted by it. Ciphertext policy ABE is apt for providing self-contained data protection by limiting the decryption power based on a few attributes of the receiver. In this way, both the attribute-based encryption schemes provide fine-grained access control over ciphered data. Sahai and Waters [10] introduced a new fuzzy identity-based encryption scheme which treats identity as a set of attributes and in this scheme a private key for an identity ID1 can be used to decrypt a ciphertext encrypted with an identity ID2, if and only if the identities ID1 and ID2 are near to each other as measured by the distance metric known as set overlap. This scheme is collusion safe and error tolerant thereby it can be easily applied to biometric identities which will have some noise. Emura et al. [11] presented a time release proxy reencryption scheme where the proxy can re-encrypt a ciphertext with a release time under a public key to the one with the same release time under another public key by making use of a reencryption key provided by the delegator. This scheme is based on time-based proxy reencryption scheme. Saduqulla et al. [12] proposed a threshold proxy reencryption scheme which consists of distributed storage servers which perform their tasks independently and highly protected key servers for managing cryptographic keys by means of which the cloud storage system enables secure encryption, decryption with data confidentiality and secure data forwarding over encrypted messages. Praveen Chandar et al. [13] have proposed hierarchical attribute based proxy re-encryption that is extended using key policy attribute-based encryption technique for user revocation and securing data in the cloud. This scheme provides fine-grained access control where user's secret key operation is carried out by lazy reencryption and proxy reencryption. Fang et al. [14] introduced a hierarchical conditional proxy reencryption which is based on the hierarchical extension of conditional proxy reencryption in which condition is treated as a vector of keywords. They have provided a good model of hierarchical key derivative conditional proxy reencryption scheme in which length of the ciphertext is independent from the depth of the hierarchy and they have presented a generalized key delegation by making use of wildcard in keyword vector and this scheme is used in Personal Healthcare Records application and other applications. Weng et al. [15] have proposed a more efficient conditional proxy reencryption with chosen ciphertext security by studying the pros and cons of previous tang et al and Weng et al schemes and constructed this efficient scheme where the proxy uses only one key i.e. reencryption key for reencryption process and the user can act as delegator or delegatee for other users. They have also defined first level ciphertext security for conditional proxy reencryption and their scheme is communication wise and computation wise more efficient than Tang et al and Weng et al previous schemes. Seo et al. [16] proposed a proxy invisible type based proxy reencryption scheme which is chosen ciphertext attack secure in the standard model. This scheme is constructed based on the concept of libert et al. CCA secure unidirectional proxy reencryption scheme and gentry's anonymous identity based encryption scheme in order to achieve proxy invisibility and CCA security without random oracles in standard model. Shao et al. [17] have made an initial construction of identity based conditional proxy reencryption scheme which allows proxy to convert ciphertexts which satisfies a specific condition. This scheme is a combination of conditional and identity-based proxy reencryption schemes and it is suitable for an application like encrypted email forwarding and it is CCA secure and identity attack secure in random oracle model. Liang et al. [18] have proposed a new identity based conditional proxy reencryption scheme which is unidirectional and single hop. This scheme captures the properties of both identity based and conditional proxy reencryption schemes. It is proved to be adaptive condition secure and adaptive identity chosen ciphertext attack secure in the standard model. Ge et al. [19] have made a construction of Identity-based conditional proxy reencryption with the fine-grained policy which finds a solution to the problem left open by Liang et al to construct a CCA secure identity based conditional proxy reencryption scheme which supports OR gates on conditions. In their scheme Ge et al have labeled every ciphertext with a set of descriptive conditions and every reencryption key is linked with an access tree that specifies which type of ciphertexts can be re-encrypted by the proxy and this scheme is also proved secure against adaptive identity chosen ciphertext attack and adaptive access tree. Liang et al. [20] have proposed an efficient cloud-based revocable identity-based proxy reencryption scheme for public cloud data sharing scheme. This scheme not only support user revocation but also delegation of decryption rights. It makes no difference whether a user is revoked or not, at the end of given time period the cloud which acts as proxy re-encrypts all the ciphertexts of the user under the present time period to the next time period. If the user revocation occurs in the upcoming time period, the user can't decipher the ciphertexts using private key which is expired. This scheme is efficient in terms of computation and communication. Qiu et al. [21] have proposed an identity based conditional proxy reencryption scheme without random oracles which is based on Boneh-Boyen's Identity based encryption technique. This scheme provides the user with the capability of fine-grained delegation of decryption rights and is appropriate for different applications which require fine-grained property. Qiu's scheme is communication wise and computationally efficient than Shao et al. [17] identity based conditional proxy reencryption scheme.

2.2 Identity Management Systems

The identity management systems encompasses various technologies and processes for the purpose of digital identity creation, management, and usage. There are many identity management systems proposed as of now. In any Identity management system, there are three common entities, they are the user, the identity provider, and the service provider.

Isolated identity management model [22, 23] is a simple model in which the identity provider and service provider are combined in such a way that user identification and authentication are carried at the service provider itself and all the identity management activities are carried out by that service provider only. If the user wants to access the services offered by other service providers, then he needs to again register with their respective identity providers. This type of model is not feasible because the users have to remember more credentials for different identity providers. In a centralized model [25] the identity management system is deployed to a centralized identity provider by many service providers. The identity provider is responsible for storing identity data in its own repository and issuing credentials, authentication, and managing identities. In order to access a service offered by a service provider, the user needs to provide a token to the service provider which is given by identity provider after proper authentication. Since in this model identity data is placed in the identity provider in-house repository, the user loses control over his identity data and many privacy and trust issues arise. customer centric model [22, 23] is an alternative to centralized model in which the user's identity data is stored at his own domain instead of outsourcing to identity provider thereby user has full control over his identity data. Based on user consent only identity provider can transfer identity data to service provider thereby increasing user privacy.one example which uses his model is Microsoft CardSpace. In federated model [25], instead of capturing identity data in a centralized repository, it is distributed across multiple identity/service providers. The distributed identity data of a specific user is linked by the means of the common identifier. This model uses various approaches like SAML, WS-Federation, and Shibboleth. In this model all the participating service providers and identity providers form a common trust relationship with each other, thereby providing cross-domain access and single sign-on.

This Identity in the cloud model [26] is similar to isolated model and the cloud service provider which provides the service also acts as identity provider and stores, manages the identity data of users, whereby users have no control over their identity data, this is an advantage to the organizations which want to outsource identity management to cloud in order to reduce costs on one side but it leads to man security and privacy issues related to organizations outsourced data on the other side. Identity to the cloud model [26] is similar to the centralized model in which the service provider is cloud-based, and the identity provider is hosted by the organization itself. When the user wants to access a service, he should be authenticated at the identity provider and then identity provider transfers required data to the service provider with the help of some standard interfaces in order to provide requested service to the user. This model also uses SAML (Security Assertion Markup Language), Open-ID and Oauth for the interfaces. This model has advantages like limited data disclosure, use of the existing organization's identity management system but it also has some interoperability issues related to interfaces. Identity from the cloud model [26] is fully cloud-based where both the identity provider and service provider are hosted on the cloud, but these two entities are provided by different cloud providers i.e. is service provider is hosted by one cloud and the identity provider is hosted on another cloud. Since the identity data is offered as a service, this identity from the cloud model is also named as Identity as a Service model. This model offers the advantages of cloud computing on one side but also organization must trust the identity providers and service providers on the other side. Cloud identity broker model [26] is an extended concept of identity from the cloud model where the identity provider in cloud works as an identity broker. The identity broker works as a bridge between different identity providers and different service providers, thereby it reduces the interoperability issues faced by service providers and identity providers. The service provider just needs to implement a single interface that works for the identity broker. Identity broker handles the interface complexities and trust relationships of different identity providers and cloud service provider need to trust only the identity broker. Since identity broker model provides advantages on one side, it also has disadvantages on the other side like the user, service provider should have similar functionality as that of identity broker, and identity broker should also support the specific identity provider which the user is interested, if it doesn't support that identity provider then the user cannot get the service from service provider and the identity data in plain format is transferred from identity provider to service provider through identity broker a lot of privacy and security issues arises in this scenario. Federated cloud identity broker model [26] is proposed by merging the features of federated identity model and cloud identity broker model in order to overcome the limitations of previous cloud identity broker model where both the service provider and user must depend on common identity broker. In this new federated cloud identity broker model, the user and service provider can opt any identity broker of their choice and also user has an ability to choose an identity broker which supports all his required identity providers and also service provider has the ability to choose an identity broker which suits its communication interface but this model didn't solve the privacy issues related to transfer of identity data in plain format between identity providers, different brokers and service providers. Blind IDM [27] is a privacy-preserving identity management as a service proposed by Nunez et al. which is an extension to their previous work [28] which also focus on enhancing privacy in identity management systems by integrating OpenID with Proxy reencryption technique. In their Blind IDM scenario they have focused on SAML based attribute exchange and making the identity provider behave in a blind manner in order to provide privacy to users identity data i.e. the identity data of users is encrypted by host organization and then migrated to identity provider, since it is in encrypted format, the identity provider cannot go through it and when the user wants to access a specific service at the service provider, the service provider redirects the user for authentication and it also specifies required identity attributes of user, then the host organization generates a reencryption key related to service provider and then provides it to identity provider, then using that key identity provider re-encrypts the identity attributes with the help of proxy reencryption technique and provide to service provider and then the service provider decrypts them using its private key and provides requested service to user. In this manner, Blind IDM provides an interesting solution to the previous cloud identity management models as described above, which have limitations with respect to providing privacy to identity data. However Blind IDM provides a good opportunity for privacy-preserving Identity management, it is not suitable for those organizations which want to maintain and manage their user identity data at the fine-grained level.

2.3 Abbreviations

SAML-Security Assertion Markup Language, OAuth-Open Authentication, IDM-Identity Management, IBPRE-Identity Based Proxy Re-encryption, CPA-Chosen Plaintext Attack, CCA-Chosen Ciphertext Attack, ABE-Attribute Based Encryption, SP-Service Provider, IdP-Identity Provider.

3. Proposed Model

3.1. Description of ContextAwareIdM

Our model is extended based on BlindIdM [27] where all the Identity attributes requested by the service provider are re-encrypted by the identity provider in such a way that they can only be decrypted by the service provider. In our model, we provide identity management at the fine-grained level. In our model, all the identity data of host organization users is encrypted by the host organization using its own identity and then the encrypted identity data is outsourced to cloud identity provider and the identity attributes consist of some context/tag field which has value like critical, simple in their metadata. Here we are using only two context /tag values like critical and simple for easier implementation. This encrypted identity data can only be decrypted by host organization using its own private key. The Identity provider cannot understand or do anything with the identity data as it is in encrypted form. So when a user of organization wants to access a particular service offered by a specific cloud service provider, then the service provider redirects the user to identity provider with which he/she is registered with for authentication and requests some attributes in the form of SAML assertions in order to provide the requested service, now the identity provider verifies the user validity and then it checks the context/tag of service provider whether it provides a critical services like banking where almost all the PII i.e. Personal Identifiable Information of user is required in order to provide the service or it provides a simple services like calculator, train ticket booking etc. where only few identity attributes of users are required. So, if the context/tag of the service provider is critical then a reencryption key with the condition critical is generated by the host organization using service provider identity or the public key of service provider and host organizations private key and then sent to Identity Provider. And using the reencryption key the identity provider checks those attributes with context/tag as critical are re-encrypted and then sent to service provider in the form of SAML assertions which can only be decrypted by service provider which requested those attributes, this is possible because of the reencryption key which is framed for that particular service provider only. After receiving the re-encrypted attributes, the service provider decrypts them using its own private key and then according to those attributes it provides the requested service to the user. So, if the service provider provides simple applications or services, then those attributes which contain the context/tag field as simple are only re-encrypted by the identity provider, our model uses identity-based conditional proxy reencryption technique in order to provide fine-grained access. So, in this way, our model context-aware IDM provides fine-grained privacy-preserving identity as a service.

3.2. Context Aware fine-grained proxy reencryption technique

This Context-aware fine-grained proxy reencryption technique consists of the following algorithms.

Setup: This algorithm takes a security parameter I^k as input and generates global public parameters which are distributed to users and master private key MPK.

KeyGen (MPK, ID): This algorithm takes Master Private Key and Users Identity ID as input and generates a private key SID corresponding to the Identity ID.

RencKeyGen (SID, C, ID2): This algorithm takes a private key SID, a Context C, and user2(service provider) identity ID2 as an input and outputs the reencryption key rk $_{1\text{--}}{}^{c}{}_{\text{-- >2}}$.

Encrypt (ID, C, M): This algorithm takes a user's identity ID, a context c, and a message M which has attributes and outputs a second order ciphertext CT associated with context c under identity ID.

ReEncrypt (CT1, rk$_{1\text{--}}{}^{c}{}_{\text{->2}}$): This algorithm is executed by Identity Provider which takes the second level ciphered text CT1 associated with c under Identity ID1 and a Re-encryption key and generates a first order ciphered text CT2 under Identity of service provider ID2.

Decrypt (CT, SID): This algorithm takes a private key SID related to Identity ID and a cipher text CT as input and outputs a decrypted message i.e. original text, in our model identity attributes.CT2 under Identity of service provider ID2.

3.3. Working process of our model

Step1: Initially all the identity data of users or employees of organization is encrypted based on the context using its public key or identity and then transferred to identity provider, here the encrypted identity data can be decrypted by only the host organization using its private key and the identity provider can’t do anything with encrypted data.

Step2: when a user wants to access a specific service offered by the service provider then the host organization generates a reencryption key using the private key of the host organization, context and public key or identity of the service provider.

Step3: Now the Identity Provider re-encrypts only those requested identity attributes which match the context associated with the reencryption key and send those re-encrypted attributes to the service provider thereby preserving privacy at the fine-grained level.

Step4: On receiving these attributes, service provider decrypts them using its own secret key and provide appropriate service requested by the user.

4. Figures

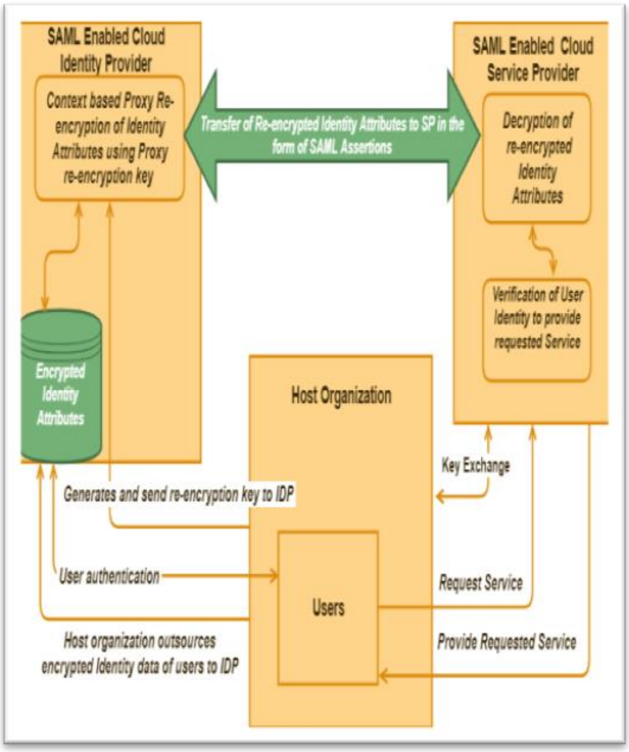
SAML Enabled Cloud Identity Provider
Context based Proxy Re-encryption of Identity Attributes using Proxy re-encryption key
Transfer of Re-encrypted Identity Attributes to SP in the form of SAML Assertions
SAML Enabled Cloud Service Provider
Decryption of re-encrypted Identity Attributes
Verification of User Identity to provide requested Service
Encrypted Identity Attributes
Host Organization
Key Exchange
Generates and send re-encryption key to IDP
User authentication
Users
Request Service
Provide Requested Service
Host organization outsources encrypted Identity data of users to IDP

Fig. 1: Schematic Representation of Proposed Model

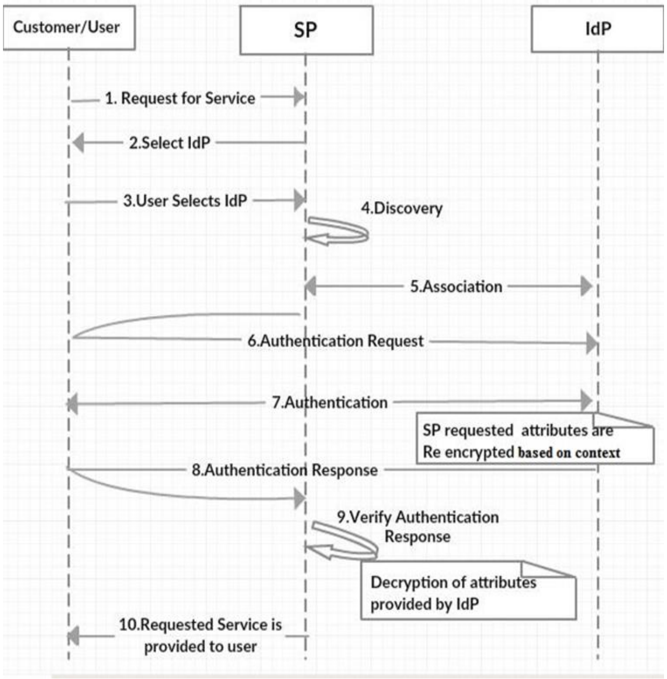
Customer/User
SP
IdP
1. Request for Service
2.Select IdP
3.User Selects IdP
4.Discovery
5.Association
6.Authentication Request
7.Authentication
SP requested attributes are Re encrypted based on context
8.Authentication Response
9.Verify Authentication Response
Decryption of attributes provided by IdP
10.Requested Service is provided to user

Fig. 2 Communication between various entities in our model

5. Advantages of our model

In most of the identity management systems of this type, the service provider can decipher all the encrypted identity attributes after reencryption, thereby fine-grained privacy-preserving identity management is not possible, So our proposed model overcomes this problem by the context based proxy reencryption where the service provider can decipher only limited encrypted identity attributes which satisfies the context after reencryption by offering fine-grained privacy-preserving identity as a service**..**

6.Conclusion and Future Scope

Our model provides a trusted identity management solution to organizations which want to outsource their identity management module to cloud-based services in order to reduce management cost associated with it, but being afraid of migrating to cloud-based identity management systems as they lose control over the migrated personal identity data of organizations users. Context-aware IdM provides an efficient solution to organizations by securing and providing privacy retaining finely grained controlled access to identity data thereby it can be adopted by many organizations which require maintaining their identity data privacy at the fine-grained altitude. Robust Identity management systems which offers secure and privacy-preserving Identity as a service at fine-grained level must be built in order to rule the future of cloud-based identity as a service models which are highly secure and intelligent which provides a competitive advantage among cloud service providers to improve their business value by offering identity management services to organizations which want to outsource their identity management. As a future work, we want to extend our model to work in an intelligent manner by embedding AI (Artificial Intelligence) based modules to be more robust and secure.

References

[1] Blaze M, Bleumer G, Strauss M, 1998 Divertible Protocols and Atomic Proxy Cryptography in Proc. Int. Conf. Theory Appl. Cryptographic Techn: Adv.Cryptol: 127-144.

[2] Yevgeniy Dodis and Anca Ivan,2003 Proxy cryptography revisited. In Proceedings of the Tenth Network and Distributed System Security Symposium.

[3] Mambo M, Okamoto E,1997 Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts, IEICE Trans. Fundamentals of Electronics, Comm. and Computer Sciences, 80(1):54-63.

[4] Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger, 2005, Improved proxy re-encryption schemes with applications to secure distributed storage, In Proceedings of the 12th Annual Network and Distributed System Security Symposium:29-44.

[5] Green M., Ateniese G, 2007, Identity-Based Proxy Re-encryption. In: Katz J., Yung M. (eds) Applied Cryptography and Network Security. Lecture Notes in Computer Science, volume 4521:288-306. Springer, Berlin, Heidelberg.

[6] Chu CK., Weng J, Chow S.S.M, Zhou, Deng R.H, 2009, Conditional Proxy Broadcast Re-Encryption. In: Boyd C., Gonzalez Nieto J. (eds) Information Security and Privacy. Australasian Conference on Information Security and Privacy Lecture Notes in Computer Science, volume 5594: 327-342, Springer, Berlin, Heidelberg.

[7] Ateniese G, Benson K, Hohenberger S, 2009, Key-Private Proxy Re-encryption. In: Fischlin M. (eds) Topics in Cryptology – CT-RSA 2009. Lecture Notes in Computer Science, volume 5473: 279-294, Springer, Berlin, Heidelberg.

[8] Qiang Tang, 2008, Type-Based Proxy Re-Encryption and Its Construction, Proceeding INDOCRYPT, 08 Proceedings of the 9th International Conference on Cryptology in India: Progress in Cryptology:130–144, Springer-Verlag Berlin, Heidelberg.

[9] Goyal V, Pandey O, Sahai A, and Waters B,2006, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, Proceeding CCS '06 Proceedings of the 13th ACM conference on Computer and communications security: 89-98.

[10] Sahai A, Waters B, 2005, Fuzzy identity-based encryption, in Proc. EUROCRYPT 05, volume 3494 of Lecture Notes in Computer Science:457-473, Springer, Heidelberg.

[11] Emura K, Miyaji A, Omote K, 2011, A timed-release proxy re-encryption scheme IEICE Transactions on fundamentals of electronics, communications and computer sciences, E- 94-A (8):1682-1695.

[12] Saduqulla S and Karimulla S, 2013, Threshold Proxy Re-Encryption in Cloud Storage System, International Journal of Advanced Research in Computer Science and Software Engineering, Volume3, Issue 11.

[13] Praveen Chandar P, Muthuraman D, Rathinrai M, 2014, Hierarchical Attribute-Based Proxy Re-Encryption Access Control in Cloud Computing 2014 International Conference on Circuit, Power and Computing Technologies [ICCPCT].

[14] Liming Fang, Willy Susilo, Chunpeng Ge, Jiandong Wang, 2012, Hierarchical conditional proxy re-encryption, Elsevier, Computer Standards & Interfaces, Volume 34, Issue 4:380-389.

[15] Weng J, Yang Y, Tang Q, Deng R.H, Bao F, 2009, Efficient Conditional Proxy Re-encryption with Chosen-Ciphertext Security. In: Samarati P., Yung M., Martinelli F., Ardagna C.A. (eds) Information Security. ISC 2009. Lecture Notes in Computer Science, volume 5735:151-166 Springer, Berlin, Heidelberg.

[16] Jae Woo Seo, Dae Hyun Yum, Pil Joong Lee, 2013, Proxy-invisible CCA-secure type-based proxy re-encryption without random oracles, Theoretical Computer Science, Volume 491, 17 :83-93, Elsevier.

[17] Shao J, Wei G, Ling Y, Xie M, 2011, Identity-based Conditional Proxy Re-encryption. Proceedings of IEEE ICC 2011, Kyoto, Japan, 5-9 June:1-5. IEEE, USA.

[18] Kaitai Liang, Zhen Liu, Xiao Tan, Duncan S. Wong, Chunming Tang, 2013, A CCA-Secure Identity- Based Conditional Proxy Re-Encryption without Random Oracles. Proceedings of ICISC 2012, Seoul, Korea, 28-30 November:231-246, Springer-Verlag, Berlin.

[19] Chunpeng Ge, Willy Susilo, Jiandong Wang, Liming Fang, 2017, Identity-based conditional proxy re-encryption with fine grain policy, Computer Standards & Interfaces, Volume 52, May 2017:1–9, Elsevier.

[20] Kaitai Liang, Joseph K. Liu, Duncan S. Wong, Willy Susilo, 2014, An Efficient Cloud-Based Revocable Identity-Based Proxy Re-encryption Scheme for Public Clouds Data Sharing. In: Kutyłowski M., Vaidya J. (eds) Computer Security-ESORICS 2014.Lecture Notes in Computer Science, vol 8712, Springer.

[21] JunJie Qiu, YoungSil Lee, HoonJae Lee, 2014, Identity-based Conditional Proxy Re-Encryption Without Random Oracles, International Conference on Information and Communication Technology Convergence (ICTC), IEEE-2014.

[22] Josang A, Fabre J, Hay B, Dalziel J, and Pope S, 2005, Trust Requirements in Identity Management. Proceedings of the 2005 Australasian workshop on Grid computing and e-research: 99–108.

[23] Josang A and Pope S, 2005, User Centric Identity Management. AusCERT 2005.

[24] Josang A, Zomai M.A, and Suriadi S. 2007, Usability and privacy in identity management architectures. In Proceedings of the fifth Australasian Symposium on ACSW frontiers - Volume 68:143-152.

[25] Cao Y and Yang L ,2010, A survey of Identity Management technology. In IEEE ICITIS 2010:287– 293, IEEE.

[26] Bernd Zwattendorfer, Thomas Zefferer, Klaus Stranacher, 2014, An Overview of Cloud Identity Management-Models, 10th International Conference on Web Information Systems and Technologies (WEBIST):82-92.

[27] David Nunez, Isaac Agudo, 2014, BlindIdM: A privacy-preserving approach for identity management as a service, International Journal of Information Security Archive Volume 13, Issue 2:199-215, Springer-Verlag Berlin, Heidelberg.

[28] Nunez D, Agudo I, and Lopez J, 2012, Integrating OpenID with Proxy Re-Encryption to enhance privacy in cloud-based identity services, IEEE CloudCom 2012: 241 – 248.