International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Generic Approach to Build Revocable Hierarchical Identity-Based Encryption

Shreya Heda[1],**Mahesh Gorde**[2],**Ruchita Kale**[3], **Vedant Londe**[4], **Zubiya Khan**[5]

[1]*Student, Computer Science & Engineering Department, PRMIT&R, Badnera*
[2]*Student, Computer Science & Engineering Department, PRMIT&R, Badnera.*
[3]*Assistant Professor, Computer Science & Engineering Department, PRMIT&R, Badnera.*

Abstract - This article introduces a cloud service that allows businesses to upload, distribute, and keep documents. The operation of documents/files stored on a cloud server/database is made simpler for the employees by this application. This article will offer methods for document uploading and downloading, document storage on a server, viewing documents shared by other users, and viewing file metadata that are stored on the server. A document will automatically be encrypted with the hybrid method when the user submits it.In heirarchical identity-based encryption (HIBE) technique developing an online secure document storage system in which the documents will be encrypted using identity key and access permission will be maintained in meta data file of document.Hierarchical identity-based encryption (HIBE) technique will reduce execution time required to revoke or grant access permission in existing identity based encryption. Identity encryption technique is used to encrypt uploaded documents. Hierarchical identity-based encryption (HIBE) model will generate two distinct identity keys one is public identity key and other is private identity key. Public identity key will be sent to the user on his registered email id whereas private identity key will be used to encrypt document. The two identity key concept will improve security of the system and reduce key leakage possibility.

Keywords: Revocable Encryption, Hierarchical Identity Based Encryption , Generic Construction

1. INTRODUCTION

Hierarchical identity based encryption technique is based on the identity of the user. Hierarchical identity-based encryption (HIBE)technique give precise definitions of their security and mention some applications. Hierarchical identity-based encryption(HIBE) Technology consists of a root private key generator (PKG), public key and users. Hierarchical identity based encryption technique is a extension of identity based encryption technique that uses the identity as a public key of a user. The identifier information of the user such as IP Address, email or mobile number instead of digital certificates can be accepted and used as public key for signature verification or encryption. previously identity based encryption technique consumes lot of time as well as storage space of system but Modified Hierarchical Identity Based Encryption Technique reduces time consumption and storage and increases security of documents. Because previously available technique like RSA is more complex because it requires two prime numbers with some conditions. This is difficult to find a couple of numbers as initiator of keys for millions of users. This complexity and difficulties of public key encryption is reduced, the output of this process is identity-based cryptography, which significantly reduces the system complexity and the cost for establishing and managing the public key authentication framework. This framework is known as Public Key Infrastructure (PKI).

There was a change in the conventional public key cryptography that, in place of a random couple of public key and secrete keys generation, the user could be choose his identity like his name, IP address as his public key.In the identity based system, any one is authorized to generate a public key from their known identity value. There is a third party in the environment to generate the corresponding private key this system is called as Private Key Generator, responsible to generate this key.First the master public key is published by the PKG and then the master private key is retained by the corresponding master private key. This master private key is referred as master key. ID is the unique identity of a user like his email ID.

For given master public key, any user, can compute a public key with reference to the identity ID by combining the identity value with the master public key.Now other user needs corresponding private key. So for obtaining this private key,this user recommends to use the identity ID and contact to PKG. The user is authorized to contact PKG. PKG uses the master private key to generate the private key for the identity ID. In Hierarchical identity based encryption technique, are using meta data file concept to reduce multiple key generation process and time consumption.While sending documents to a particular user meta data file will provide security by storing private key of that particular user and also provides authentication .Identity-based encryption (IBE) is a new type of public-key encryption (PKE) that solve the public-key management problem in PKE by using a user's identity as a public key. Since the first IBE scheme in bilinear maps was proposed by Boneh and Franklin,research on new types of cryptographic encryption such as IBE, hierarchical IBE (HIBE), attribute-based encryption (ABE), and predicate

encryption (PE) has been actively studied as an important research topic.

2. Literature Survey

In 2011 C. Gentry proposed two efficient Identity-Based Encryption (IBE) systems admit selectiveidentity security reductions without random oracles in groups equipped with a bilinear map.Selective-identity secure IBE is a slightly weaker security model than the standard security model for IBE. In identity based encryption model the adversary must commit ahead of time to the identity that it intends to attack, whereas in an adaptive-identity attack the adversary is allowed to choose this identity adaptively. The first system—BB1—is based on the well studied decisional bilinear Diffie–Hellman assumption, and extends naturally to systems with hierarchical identities, or HIBE. Second system—BB2—is based on a stronger assumption which call the Bilinear Diffie–Hellman Inversion assumption and provides another approach to building IBE systems.[3]

In 2012 C. Gentry, C. Peikert, and V. Vaikuntanathan proposed The notion of aggregate signature has been motivated by applications and it enables any user to compress different signatures signed by different signers on different messages into a short signature.Sequential aggregate signature, in turn, a special kind of aggregate signature that only allows a signer to add his signature into an aggregate signature in sequential order. This latter scheme has applications in diversified settings such as in reducing bandwidth of certificate chains and in secure routing protocols. As an instructive example, obtain a translation of the Lewko-Waters composite order IBE scheme. This provides a close analog of the Boneh-Boyen IBE scheme that is proven fully secure from the decisional linear assumption. In the full version of this paper, also provide a translation of the Lewko-Waters unbounded HIBE scheme.[6]

In 2013 B. Waters proposed Revocable hierarchical identity-based encryption (RHIBE) is an extension of HIBE that supports the revocation of user's private keys to manage the dynamic credentials of users in a system. Many different RHIBE schemes were proposed previously, but they are not efficient in terms of the private key size and the update key size since the depth of a hierarchical identity is included as a multiplicative factor. In this paper, propose efficient RHIBE schemes with shorter private keys and update keys and small public parameters by removing this multiplicative factor. To achieve goals, first present a new HIBE scheme with the different generation of private keys such that a private key can be simply derived from a short intermediate private key. Next, show that two efficient RHIBE schemes can be built by combining HIBE scheme, an IBE scheme, and a tree based broadcast encryption scheme in a modular way.[4]

In 2013 A.B.Lewko and B.Waters, proposed Revocation and key evolving paradigms are central issues in cryptography, and in PKI in particular. A novel concern related to these areas was raised in the recent work of Sahai, Seyalioglu, and Waters who noticed that revoking past keys should at times (e.g., the scenario of cloud storage) be accompanied by revocation of past ciphertexts (to prevent unread ciphertexts from being read by revoked users) They introduced revocable-storage attribute-based encryption (RS-ABE) as a good access control mechanism for cloud storage. RS-ABE protects against the revoked users not only the future data by supporting key-revocation but also the past data by supporting ciphertext-update, through which a ciphertext at time T can be updated to a new ciphertext at time T +1 using only the public key. Motivated by this pioneering work, ask whether it is possible to have a modular approach, which includes a primitive for time managed ciphertext update as a primitive[9]

In 2014 A. Silverberg proposed Hierarchical identity-based encryption (RHIBE) is an extension of HIBE that supports the revocation of user's private keys to manage the dynamic credentials of users in a system. Many different RHIBE schemes were proposed previously, but they are not efficient in terms of the private key size. Revocable HIBE (RHIBE) is an HIBE scheme that can revoke a user's private key if his credential is expired or revealed. In this paper, first propose an unbounded HIBE scheme where the maximum hierarchy depth is not limited and prove its selective security under a q-type assumption. Next, propose an efficient unbounded RHIBE scheme by combining unbounded HIBE scheme and a binary tree structure, and then prove its selective security[5]

3.Modified Identity Based Encryption Technique

Nowadays data sharing through digital mode is very common but risk of hacking data is increasing ,so in this identity based encryption technique use normal encryption decryption technique while sending documents but this encypted data is also hacked by hackers using various technology.This process increases complexity ,requires more storage area and does not provide security so in this technique in this identity based encryption technique are creating an online secure document storage system which is based on revocable hierarchical identity based encryption technique.In revocable hierarchical identity based encyption technique data gets reencrypted while sending to the multiple users. When owner sends data to 'n' number of users 'nth' user will require 'n-1' number of keys to decrypt that encrypted document,this process increases security of data but it is a time consuming process.So to avoid time consumption process in this identity based encryption technique are using meta data file concept.

In meta data file concept when owner sends data to the multiple users two keys will get generates i.e private key and public key as well as one meta data file gets created.private key get stored in meta file under that particular user name and public key is send to that user through email address.When user wants to decrypt the data he/she has to put public key for authentication process which verifies whether the user is real or not during the session one internal private key gets generated which compare with the private key present in the meta data file and if it matches then meta data file will give access to that user. If the key will not match the user will be consider as a unauthorized users.In these RHIBE,user can send, receive,download data securely as process

4. Algorithm For HIBE

The Advanced Encryption Standard (AES) algorithm is one of the block cipher encryption algorithm that was published by National Institute of Standards and technology (NIST) in 2000. The main aims of this algorithm was to replace DES algorithm after appearing some vulnerable aspects of it. NIST invited experts who work on encryption and data security all over the world to introduce an innovative block cipher algorithm to encrypt and decrypt data with powerful and complex structure. From around the world many groups submitted their algorithm. NIST accepted five algorithms for evaluate. After performing various criteria and security parameters, they selected one of the five encryption algorithm that proposed by two Belgian cryptographers Joan Daeman and Vincent Rijmen.

The original name of AES algorithm is the Rijndel algorithm. However, this name has not become a popular name for this algorithm instead it is recognized as Advanced Encryption Standard (AES) algorithm around the world.Hardware and software implementation of the AES algorithm is one of the most important area to attractive researches to do a research on it. In recent years a number of research papers have been publishing on AES algorithm to provide much more complexity and comparing the performance between the popular encryption algorithms to encrypt and decrypt data. In Lu, etal proposed a new architecture method to reduce the complexity architecture of AES algorithm when it is implementing on the hardware such as mobile phone, PDAS and smart card etc. This method has consisted of integrating the AES encrypted and the AES decrypted to provide a perfect functional AES crypto-engine. To do that they focused on some important features of AES especially (Inv)SubBytes and (Inv)Mix column module.

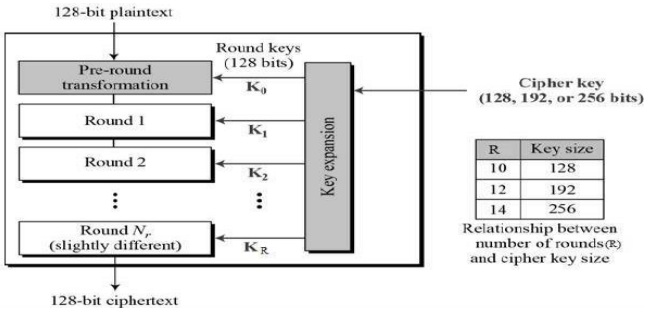

Fig -2: AES Algorithm

A study in has conducted on different secret key algorithms to identify which algorithm can be provided the best performance to encrypt and decrypt data.

CONCLUSION

Cryptography and cyber security are pivotal technology in the field of information technology, enabling users to access and store data and applications securely through the internet. However, as the amount of data stored in the cloud continues to grow exponentially, issues such as storage space management and data security have emerged as significant concerns.

The RHIBE Technique providing more security and authentication to the document. The RHIBE Technique overcome the drawbacks of Identity Based Encryption Technique. RHIBE saves more space of computer system. The purpose of RHIBE is confidentiality-concealing the content of the message by translating it into a code. The purpose of RHIBE is to provide integrity and authenticity-verifying the sender of a message and indicating that the content has not been changed. The implementation of this project has several benefits. First, it contributes to the field of security by addressing important issues related to documents management and data security. Online document storage system helps for maintaining integrity, confidentiality and promoting efficient data management. The use of cryptography enhances the security of data, safeguarding it from unauthorized access ,In summary, this project presents an innovative approach to address the challenges of data sharing and data security. The Online document storage system and cryptography approach contribute to the field by providing efficient robust data security and integrity of data.

ACKNOWLEDGEME

With great pleasurewe hereby acknowledge the help given to us by various individuals throughout the project. This Project itself is an acknowledgement to the inspiration, drive and technical assistance contributed by many individuals. This project would have never seen the light of this day without the

help and guidance we have received.We would like to express our profound thanks to Prof. Ruchita Kale for their guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project. We would also thank the faculties of the Department of Computer Science & Engineering, for their kind co-operation and encouragement which help us in completion of this project. We owe an incalculable debt toall staffs of the Department of Computer Science & Engineering for their direct and indirect help.

Our thanks and appreciations also go to our colleague in developing the project and people who have willingly helped us out with their abilities.We extend our heartfelt thanks to our parents, friends and well wishers for their supportand timely help. Last but not the least; we thank the God Almighty for guiding us in every step of the way.

REFERENCES

[1] D. Boneh and M. K. Franklin, ‘‘Identity-based encryption from the Weil pairing,’’ in Advances in Cryptology CRYPTO 2001, vol. 2139. Berlin, Germany: Springer, 2001, pp. 213–229.

[2] D. Boneh and X. Boyen, ‘‘Efficient selective-ID secure identity-based encryption without random oracles,’’ in Advances in Cryptology EUROCRYPT 2004, vol. 3027. Berlin, Germany: Springer, 2004,, pp. 223–238.

[3] C. Gentry, ‘‘Practical identity-based encryption without random oracles,’’ in Advances in Cryptology EUROCRYPT 2006, vol. 4004. Berlin, Germany: Springer, 2006, pp. 445–464.

[4] B. Waters, ‘‘Efficient identity-based encryption without random oracles,’’ in Advances in Cryptology EUROCRYPT 2005, vol. 3494. Berlin, Germany: Springer, 2005, pp. 114–127.

[5] C. C. Cocks, ‘‘An identity based encryption scheme based on quadratic residues,’’ in Cryptography and Coding, vol. 2260. Berlin, Germany: Springer, 2001, pp. 360–363.

[6] C. Gentry, C. Peikert, and V. Vaikuntanathan, ‘‘Trapdoors for hard lattices and new cryptographic constructions,’’ in Proc. 40th Annu. ACM Symp. Theory Comput., May 2008, pp. 197–206.

[7] D. Boneh, X. Boyen, and E.-J. Goh, ‘‘Hierarchical identity based encryption with constant size ciphertext,’’ in Advances in Cryptology EUROCRYPT 2005, vol. 3494. Berlin, Germany: Springer, 2005, pp. 440–456.

[8] B. Waters, ‘‘Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions,’’ in Advances in Cryptology CRYPTO 2009, vol. 5677. Berlin, Germany: Springer, 2009,, pp. 619–636.

[9] A. B. Lewko and B. Waters, ‘‘New techniques for dual system encryption and fully secure HIBE with short ciphertexts,’’ in Theory of Cryptography TCC 2010, vol. 5978. Berlin, Germany: Springer, 2010, pp. 455–479.

[10] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, ‘‘Bonsai trees, or how to delegate a lattice basis,’’ in Advances in Cryptology EUROCRYPT 2010, vol. 6110. Berlin, Germany: Springer, 2010, pp. 523–552.

[11]S. Agrawal, D. Boneh, and X. Boyen, ‘‘Efficient lattice (H)IBE in the standard model,’’ in Advances in Cryptology EUROCRYPT 2010, vol. 6110. Berlin, Germany: Springer, 2010, pp. 553–572.

[12] Gaj, K., & Chodowiec, P. (2011, April). Fast implementation and fair comparison of the final candidates for Advanced Encryption Standard using Field Programmable Gate Arrays. In Cryptographers’ Track at the RSA Conference (pp. 84-99). Springer Berlin Heidelberg.

[13] W. Diffie, and M. Hellman, “New directions in cryptography,” in IEEE Trans. Inf. Theor., vol. 22(6), pp. 644-654, 2012.

[14] Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications

[15] C. Gentry, and A. Silverberg, “Hierarchical ID-Based Cryptgraphy,” in Zheng Y. (eds) Advances in Cryptology - ASIACRYPT 2002, LNCS, vol. 2501. , pp. 548-566, Springer, Berlin, Heidelberg, 2014.

[16] V. Miller, “The Weil Pairing, and Its Effcient Calculation,” in Journal of Cryptology, vol. 17, pp. 235-261, 2015

[17] A. Joux, “A One Round Protocol for Tripartite Diffe-Hellman,” in Bosma W. (eds.) Algorithmic Number Theory - ANTS 2000, LNCS, vol. 1838, pp. 385-393, Springer, Berlin, Heidelberg, 2015

[18] S. Yamada, “Adaptively Secure Identity-Based Encryption from Lattices with Asymptotically Shorter Public Parameters,” in Fischlin M., Coron JS. (eds) Advances in Cryptology - EUROCRYPT 2016, LNCS, vol. 9666, pp. 32-62, Springer, Berlin, Heidelberg, 2016.

[19] D. Cash, D. Hofheinz, E. Kiltz, C. Peikert, “Bonsai Trees, or How To Delegate a Lattice Basis,” in Gilbert H. (eds) Advances in Cryptology - EUROCRYPT 2010. LNCS, vol. 6110, pp. 523-552, Springer, Berlin, Heidelberg, 2016.

[20] L. Ducas, V. Lyubashevsky, and T. Prest, “Efficient Identity-Based Encryption over NTRU Lattices,” in Sarkar P., Iwata T. (eds) Advances in Cryptology - ASIACRYPT 2014, LNCS, vol. 8874, pp. 22-41, Springer, Berlin, Heidelberg, 2017.

[21] L.K. Grover, “From Schrödinger's Equation To The Quantum Search Algorithm,” in Pramana - Journal of Physics, vol. 56, pp. 333-348, 2017

[22] C. P. Pfleeger, S. L. Pfleeger, and J. Margulies, Security in Computing. New Jersey: Prentice Hall, 2017.

[23] M. Mushtaq Faheem, S. Jamel, A. Hassan Disina, Z. A. Pindar, N. Shafinaz Ahmad Shakir, and M. Mat Deris, "A survey on the cryptographic encryption algorithms," Int. J. Adv. Comput. Sci. Appl., 8(11), 2017,

[24] W. Stallings, and M. P. Tahiliani, Cryptography and Network Security: Principles and Practice. London: Pearson, 2018.
[25] R. Kumar, and C. C. Ravindranath, "Analysis of Diffie Hellman Key Exchange Algorithm with proposed Key Exchange Algorithm," Int. J. Emerg. Trends Technol. Computer Sci., 4(1), 2018,
[26] S. Pavithra, "Performance evaluation of symmetric algorithms," J. Glob. Res. Comput. Sci., 3(8), 2018
[27] S. J. Aboud, "Secure e-exam scheme," International Journal of Science and Research, 3(9), 2014, pp. 2019.
[28] O. Zughoul, H. M. Jani, A. Shuib, and O. Almasri, "Privacy and security in online examination systems," IOSR J. Comput. Eng., 10(4), 2019,
[29] K. P. Karule and N. V Nagrale, "Comparative analysis of encryption algorithms for various types of data files for data security," International Journal of Scientific Engineering and Applied Science, 2(2), 2020
[30] Ionescu, V. M., & Diaconu, A. V. (2020, June). Rubik's cube principle based image encryption algorithm implementation on mobile devices.