PROVIDING SECURITY FOR THE DATA IN CLOUD USING IBET

V.KESAVA KUMAR[1] POTHURAJU SWATHI[2] A.ANUSHA[3] M.SUJANI[4]
[1]ASSOC.PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[2] ASST. PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[3]ASST. PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[4]ASST.PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[1,2,3,4] SRI MITTAPALLI COLLEGE OF ENGINEERING

Abstract:
More and more organizations and individuals are using public cloud storage and data exchange services as cloud computing continues its meteoric rise in popularity. It is common practice for data owners to encrypt their sensitive data before putting it in the cloud. This ensures that only permitted users in the cloud may decipher the data. A major problem emerges when anyone other than the data owner's approved recipients needs access to encrypted material. Our proposed and officially documented identity-based encryption transformation (IBET) paradigm merges two popular encryption techniques—identity-based encryption (IBE) and identity-based broadcast encryption smoothly—to address this problem. In contrast to conventional secure distributed systems, which need cumbersome certificate management, IBET recognizes users and grants them access to data based on their recognizable identities. It's crucial to remember that IBET may transform an IBE ciphertext into an IBBE ciphertext, which means that people who weren't supposed to have access to the original material can actually access it. We construct an IBET scheme based on bilinear groups and show that it is safe against many complex attacks. The proposed approach is both very efficient and simple to execute, according to several theoretical and empirical investigations.

1. Introduction

Cloud computing offers powerful and flexible storage services to individuals and enterprises [1]. It reduces the local burden of storage administration and maintenance while bringing about a plethora of benefits from scattered data consumers exchanging data regionally. But another major problem limiting widespread usage of is the linked nature of personal data privacy and security. Cloud storage [2] has grown in popularity as a solution for data owners who no longer have physical control over their data. This involves outsourcing the burden of data storage to cloud servers, which are maintained by cloud service providers (CSPs). People in control of data who are worried about the exploitation of their personal information Access to it is granted to unauthorised individuals or malicious CSP. Cryptographic encryption is widely regarded as the gold standard for protecting data stored and processed on the cloud, and many individuals advocate for its usage. Before outsourcing to cloud-based servers, data owners encrypt their data using several ways. A ciphertext format is used to encrypt the data stored in the cloud, ensuring that only those with the proper decryption keys may access it. When people utilise free online cloud storage, different people might use different encryption techniques to communicate data. When a data owner wants to share sensitive information with others, they may encrypt it. This process involves creating a unique ciphertext that can only be read by the person using the device. Nevertheless, in order for data to be exchanged, The data owner will continue to share his information until there are major modifications. As the number of users increases, it becomes

important to update the ciphertext format so that it may be deciphered by different persons. There are several applications for crypttext transformation. This is an absolute need, as mentioned before. Consider that a customer-serving insurance plan is produced by a group of medical insurance firms. Consequently, it is the responsibility of every agent to gather client personal information from various sources, such as electronic health records, census data, job statistics, financial reports, and other databases. Some examples of such sources are hospitals, corporations, and tax organisations.

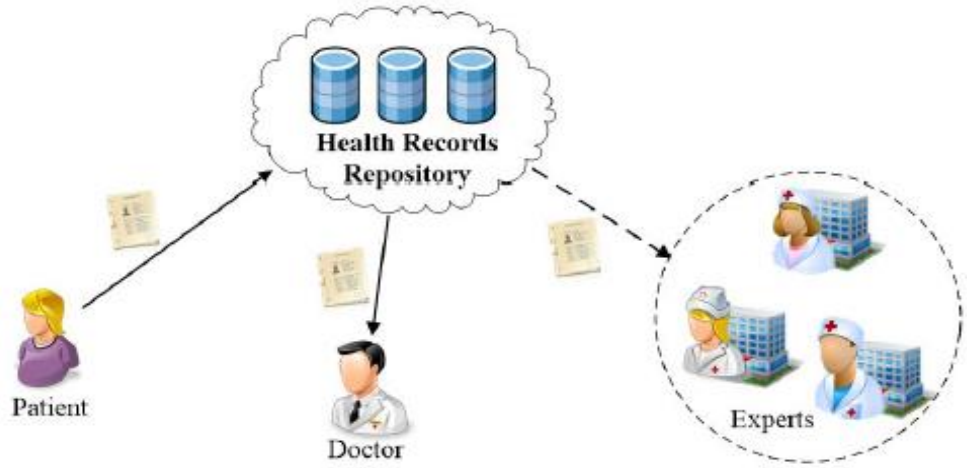


Fig. 1. Electronic Health Records Sharing with More Doctors

The data may be stored on remote cloud servers, which might use security measures like several layers of encryption. However, this raises serious concerns over the security of individuals' private information. The purpose of this piece is to provide a technical fix for that kind of problem. The government may change encryption algorithms without revealing the ciphertexts' decoding keys. One sort of encryption system that we consider is identity-based encryption, which involves a transformation mechanism that connects two widely-used encryption algorithms. based on the user's identity (IBBE) and encryption One of the main reasons for this is the fact that we deal with electronic health data exchanges. Imagine a world where medical records may be accessed by implanted devices or through the use of wearable sensors to gather personal physiological data. A mobile device is used to gather all of this data. Afterwards, the files were moved to a remote server. A patient's health records may be encrypted using specific methods to protect the confidentiality of his information. Thanks to IBE, an encryption technology, no one other than his doctor can access his medical records and arrive at an accurate diagnosis. In the end, the patient's health presents a challenging issue, and the doctor decides to treat them. throughout the book, consult with a group of doctors from different hospitals who have a thorough understanding of the patient's condition. In order to begin, review the patient's medical history (see Fig. 1). because doctors have a hard time deciphering encrypted records without the patient's knowledge and the patient's cryptographic password, which makes it tough for specialists to view the material directly. Consequently, experts are concerned about the following: "How are we going to read the patient's medical records in this new system?" so that I may advise on treatment options?" View Figure 1 to learn how to expand the number of providers who can access your electronic health information. One easy solution would be for the

physician to decrypt the communication, then encrypt all the data before sending it out. We provide detailed information to each consultant in plaintext, not encrypted. But, the daily transfer of enormous quantities of health data can end up costing a lot of time and energy, making its implementation challenging for the doctor. Furthermore, utilizing plaintext to send data has the additional risk of disclosing private information.

2. Related Work

When it comes to cloud computing, cryptographic encoding methods have a long history of use in securing outsourced data. To keep a close eye on who may access other systems, public-key encryption is a tried-and-true method. four, five, six All users may reap the benefits of IBE [6] as a future untrusted certificate elimination cryptography solution for safe communications. While working together on a mobile device, researchers Wei and colleagues [7] used IBE to secure data. While collaborating with colleagues, he developed an IBE-based healthcare handshake system that use a social networking site to ensure the security of patient data [8]. Also, identity-based broadcast encryption (IBBE) allows users to encrypt a message once and transmit it to all the recipients they select, in addition to IBE, which enables encryption for multiple receivers. With this useful feature in mind, Deng et al. [10] used IBBE to provide cloud storage solutions that let many authorised users access and utilise the same material stored elsewhere. Eliminating a few recipients The original receiver list for the IBBE ciphertext was used to randomly choose a number of receivers. As a method of dealing with changes to plaintext inside a cryptographic system, Blaze et al. (15) proxy re-encryption is being used for the first time. Consider this case in point The user has the option to modify the ciphertext generated by PRE. Make the ciphertext that was created using Bob's public key and Alice's public key unintelligible. To simplify things, Ateniese et al. [16] classified PRE as either single-hop or multi-hop. Pre-production might be interactive or non-interactive, and it can be bidirectional or unidirectional. There have been several efforts to enhance the safety and effectiveness of PRE, with the majority of these efforts focussing on PRE in a one-way fashion. Vergnaud [17] showed the first unidirectional PRE system that he had constructed. Cao et al. proposed the autonomous path as a way for users to choose a preferred route for authorised visitors to see their outsourced information. Responsibility for detecting the re-encryption key abuser proxy in a unidirectional PRE was first disclosed by Guo et al. [19].

Relationship tensions exist between Chu and Tzeng, but Green and Ateniese [20] succeeded in integrating PRE and IBE to propose identity-based PRE (IBPRE), an augmentation of PRE applicable to identity-based situations. Using short ciphertexts, [21] introduced IBPRE. Even though proxy servers and authorised users may cooperate together to launch collusion attacks on decryption keys, As pointed out by Liang et al., users pose a threat to the security of sensitive company information. Here we present the IBPRE cloud-based solution, which is revocable. Implementing the system as a transformational key generating authority requires collaboration between data owners and scheme developers; hence, efficiency may suffer. An IBBE-based PRE method may be developed, according to the idea made by researchers Xu and colleagues [23], who proposed incorporating IBBE into PRE. Consider other alternatives to IBPRE, such as attribute-based PRE [24, 25], time-based PRE [26], and functional PRE [27]. In contrast, ciphertext transformation is the main focus of these PRE proposals. This precludes the possibility of converting ciphertexts into any other data type or design. Encryption transition across domains

may be achieved in a few different ways. Matsuo The conversion of public-key encryption systems into IBE ciphertext using personal identification numbers (PINs) was a major component of traditional public-key cryptography.

Additionally, Mizuno and Doi [29] proposed unidirectional transmission. The PRE technique requires user participation and data storage for the reworking process, but it converts attribute-based ciphertexts into plaintext and IBE system ciphertexts. A recent study by Jiang's team [30] proposed a method to public-key encryption that combines the greatest features of Regardless, the system of public-key encryption certificates is necessary for identity-based encryption. This page is here to talk about how change happens in different fields. This is why an identity-based approach is more cost-effective for certificate management. Data may still be securely encrypted even after it has been shared with several people, thanks to the transformation offered by this piece of programming, which takes the IBE system (one-receiver) and uses it with the IBBE system (multi-receiver).

3. Proposed Model

An abstract picture of the system's design is the System design Model (SAM). Figure 2 shows the design of the IBET system. Within an IBET system, four types of entities may be found: Owners of data, people who utilise it, registration authorities, and others service provider for the internet of things (CSP). the individuals responsible for data management Users of the cloud might be either data creators or consumers. It's reasonable to assume that RA can be relied on by whoever is responsible for system setup and responding to requests for file parameter publishing and registration outsourcing. Here are the primary duties of CSP: delivering clients storage space and services for outsourced data The compute services provide clients the ability to change the stored files. A business or organisation may acquire a service provider in the real world. Compute and storage are provided via CSP. The responsibility of the RA type is with the organization's or company's IT centre. Consequently, all registered employees have the option to use processing and storage capabilities provided by the cloud. Data owners have the option to outsource their data to CSP. If data owners want to be extra cautious with their privacy while processing data, they may employ IBE encryption, which sends files containing encrypted data to CSPs. What if we were to say that the IBE technique had been used to encrypt data in a file? The data is accessible to only one user. What happens if the Furthermore, the data's rightful owner is keen on disseminating the details. As the number of data users increases, he generates an authorization and sends it to CSP. CSP may use the token to change an IBE ciphertext file into another IBBE ciphertext file format, allowing all intended users to decode it. Below that, you can see what's happening. Consequently, the data owner may decide how many individuals can access the IBE-encrypted data, which was previously accessible to only one data consumer.

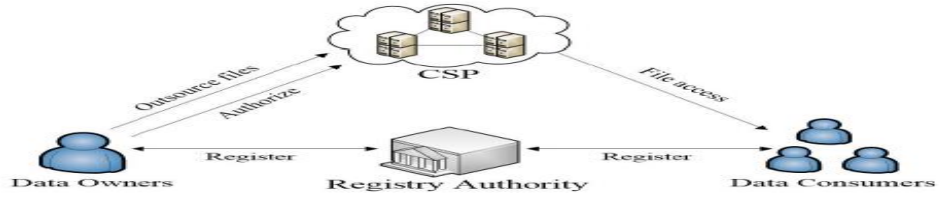


Fig. 2. System Architecture

An IBET system has to handle three different types of active attacks. One potential threat is that cloud customers may impersonate legitimate users in order to get access to outsourced data. For example, a dishonest employee may use a coworker's social media account or device to connect to a cloud service provider (CSP). Secondly, cloud servers may be utilised by malicious third-party service providers or hackers to search for and steal owner data. a third potential outcome is that CSP will abuse the authorisation tokens possessed by data owners to decrypt data beyond of their authorised geographic region. In light of these realistic attacks, we anticipate a secure IBET system that satisfies our minimum criteria. following these safety goals Data encryption is one method of data security protection; nevertheless, only authorised customers with the necessary information may get the decryption keys. Verified customers are the only ones who can decipher the CSP-encrypted data. Due to insufficient encryption key(s), you will only be able to modify the chosen files so that you have control over the authorisation token that the data owner receives. There is a transformational impact of CSP. Clients like CSP and others can't work together to provide an appropriate authorisation token, nor can they detect or change files with unclear or sensitive content.

IBET Preview

It's not easy to build a system that can change a file's permissions from allowing just one authorised visitor to allowing several visitors simultaneously. At first glance, it seems like an authorised user might encrypt their private key using IBBE and share it with all the people who need it. This way, everyone could get their hands on the encrypted file and decode it just like the original authorised user. On the other hand, unauthorised individuals may access outsourced data if the visitor's secret key was made public. To achieve encryption transformation while keeping private keys secret, we suggest adding a privacy-preserving authorisation mechanism to IBET's architecture. When the data owner creates an authorisation token, CSP uses it to convert files and receives a modified file that is the outcome of plaintext blinded by a random factor. The random factor used to encrypt the converted file is only accessible to permitted data users. This appropriately secures the data owner's private key. To reduce the size of the public parameters, Boneh and Boyen's identity-based encryption approach has one of its components reduced [31]. We also use Delerabl'ee's identity-based broadcast encryption technique [9] to accommodate a large number of listeners. Producing the authorisation token follows the application of IBBE encryption and the file's conversion to Delerabl'ee's IBBE-type ciphertext format. Here we display our IBET structure, which is built on bilinear groupings. throughout Table 1 you can see all the notes that are used throughout the article. Assume, for the sake of argument, that G and GT are two prime order cyclic groups of multiplicative function. Here are few features that define G G GT as a bilinear map: In this equation, you may find two features: For any g, h, and Zp, the integral of e(g, h) is equal to e(g, h)ab, indicating bilinearity. Additionally, e(g, h) is smaller than 1, indicating non-degeneracy. A bilinear group G is one in which both group operations in G and the bilinear map E: G G > GT may be efficiently calculated. We will base our IBET design on the following complexity assumptions.

TABLE 1
Notations

Symbol	Meaning
$\mathbb{G}, \mathbb{G}_T$	Cyclic groups with bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
p	The large prime order of groups $\mathbb{G}$ and $\mathbb{G}_T$
g	A generator of $\mathbb{G}$
PP	The system public parameters
MSK	The system master secret key
H_0, H_1	Two cryptographic hash functions
ID	An identity of a user, e.g., an email address
S	A set of different identities, i.e., $S = \{ID_i\}$
SK_{ID}	A private key for the user with identity ID
CT_{ID}	An IBE ciphertext in an original file
CT_S	An IBBE ciphertext in a transformed file
s, t, r	Random values in $\mathbb{Z}_p^*$
u, h	Random values in $\mathbb{G}$
m	the maximum number of data consumers who can access the same data
n	the number of data consumers specified by a data owner

General Decision-Making Hypothesis: GDDHE The Exponent of Diffie-Hellman Put otherwise, assume that g0,h0 G is a cyclic group of order p. In this scenario, consider two polynomials P and Q that are coprime and have two distinct orders of pairwise unique roots. Given the inputs (g0, g 0,..., gq1 0, gP() 0, gsP() 0), the GDDHE assumption states that any probabilistic polynomial-time (PPT) algorithm A has an insignificant chance of identifying whether T is equal to or a random value of GT. According to the GDDHE hypothesis The q-SDH theory from a new angle [32]. This provides a natural variation on the q-Strong-Diffie-Hellman (q-SDH) assumption. In this case, we will act as if G is a p-order ordered cyclic group. Based on the variation of the q-SDH assumption, there is a low probability that any PPT algorithm A would calculate g1/(x+c) given a tuple of components (g, gx, gx2,..., gxq) Gq+1 and a fixed value c Zp. While c is freely selectable in the standard q-SDH assumption, it is fixed in this variation of the assumption [32].
We show (in Appendix A) that this q-SDH assumption variation is true in all groups where the q-SDH assumption is valid, as previously reported by Boneh et al., just to be thorough.

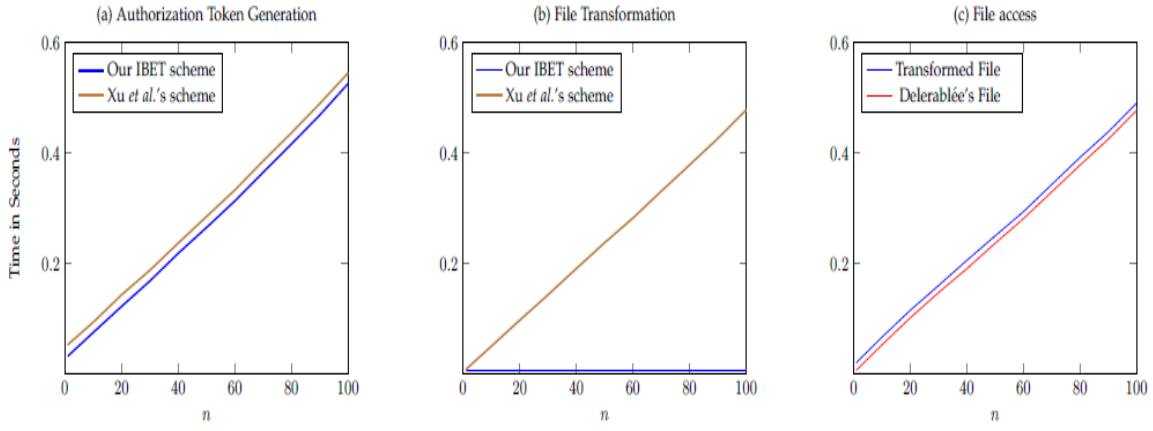
4. Result Analysis

At the entity level, we've summarised the computation overhead of each method in Table 2.

TABLE 2
Computation complexity of each algorithm in the IBET scheme

Algorithms	Computations	Entity
Setup	$(m+2)t_e + 1t_p$	RA
Register	$1t_e$	RA
Encrypt	$2t_e$ (case 1) or $4t_e$ (case 2)	Data owner
Authorize	$(n+4)t_e$	Data owner
Transform	$1t_p$	CSP
Decrypt	IBE: $1t_p$	Data consumer
	IBBE: $(n-1) \cdot t_e + 3t_p$	

We zero in on the most expensive cryptographic procedures, exponentiations and bilinear mappings. In the table, it takes time to assess an exponentiation operation in G as well as a bilinear pairing. The computational cost of RA's setup approach is linear in m if m data consumers have access to the same data. For RA to produce a private key, all it has to do upon registration is perform one exponentiation in G. There are two methods in which data owners may use the Encrypt algorithm. It takes two exponentiations for Case 1 ciphertext if the data owner only wants one person (like himself) to access the outsourced data; it takes just four exponentiations for Case 2 ciphertext if the data owner intends to share the data with other users in the future. When a data owner decides who may access their data and how much it will cost, they establish an authorisation token. To change a file's format, CSP has to establish a single connection with the Convert algorithms. The Decode method allows data consumers to decode an original file in a single bilinear pairing, whereas the decode algorithm allows them to decrypt a changed file in an endless number of ways. For your convenience, we have provided a comparison of our IBET scheme with other comparable schemes. This comparison covers several critical elements, such as the prices of token creation calculations, storage for clients and CSP servers, and more. In the table, the length of a value is represented by |Zp|, |G|, and |GT|, respectively, in Zp and G. One can see how computationally intensive the many algorithms that make up the IBET scheme are in Table 2. Computer Programs To begin an entity, add up all of its squares and you get: RA Register for the inaugural RA Ensure the security of your data by using robust encryption methods such as 228-bit or 256-bit encryption (case 2), or by obtaining the approval of the data's owner or controller. Convert one tp to another with CSP-based IBE decryption: tp Data usage by user IBBE: (n 1) te + 3tp and GT. The techniques proposed by Matsuo and Jiang et al. (cross-domain transformation) may convert files created by PKE to those generated by IBE; however, these approaches need the storing of public parameters, or keys, whose size is proportional to the number of expected data consumers (N). This efficiency challenge is solved by Xu et al. and our solutions using identity-based encryption. Compared to the methodology developed by Xu et al., our method achieves identity-based cross-domain translation with fewer client-side public parameters. The limitation of being able to convert in just one sort of encryption is removed by this functionality. If users want, they may encrypt data using an efficient identity-based encryption approach and then convert it to a format that another encryption system (IBBE) can decipher.



Execution time of Authorization token generation, File transformation and (transformed) File access

5. Conclusion

For this essay, we looked at methods for swiftly and securely encrypting and decrypting data stored in the cloud. One paradigm that has been developed to address this issue is identify-based encryption transformation (IBET), which combines the well-studied IBE and IBBE methods. By enabling data owners to safeguard outsourced data via identity-based access control, IBET eliminates the need for complicated cryptographic certificates for every user. Data owners may also take use of a transformation mechanism that lets cloud service providers (CSPs) convert files from one format to another; this way, only a limited set of authorised users will be able to decipher the files. We developed an extremely strong IBET system that is impervious to attacks of the highest sophistication. Results from several experiments confirm the system's efficacy and practicality.

REFERENCES

[1] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud data protection for the masses," Computer, vol. 45, no. 1, pp. 39–45, 2012.

[2] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1362–1375, 2016.

[3] H. Yin, Z. Qin, J. Zhang, L. Ou, and K. Li, "Achieving secure, universal, and fine-grained query results verification for secure search scheme over encrypted cloud data," IEEE Transactions on Cloud Computing, 2017.

[4] K. Li, W. Zhang, C. Yang, and N. Yu, "Security analysis on one-tomany order preserving encryption-based cloud data search," IEEE Transactions on Information Forensics and Security, vol. 10, no. 9, pp. 1918–1926, 2015.

[5] R. Zhang, R. Xue, and L. Liu, "Se archable encryption for healthcare clouds: a survey," IEEE Transactions on Services Computing, vol. 11, no. 6, pp. 978–996, 2018.

[6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586– 615, 2003.

[7] J. Wei, W. Liu, and X. Hu, "Secure data sharing in cloud computing using revocable-storage identity-based encryption," IEEE Transactions on Cloud Computing, 2016.

[8] D. He, N. Kumar, H. Wang, L. Wang, K.-K. R. Choo, and A. Vinel, "A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 633–645, 2018.

[9] C. Delerabl´ee, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2007, pp. 200–215.

[10] H. Deng, Q.Wu, B. Qin,W. Susilo, J. Liu, andW. Shi, "Asymmetric cross-cryptosystemre-encryption applicable to efficient and secure mobile access to outsourced data," in Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. ACM, 2015, pp. 393–404.

[11] J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, "Anonymous identity-based broadcast encryption with revocation for file sharing," in Australasian Conference on Information Security and Privacy. Springer, 2016, pp. 223–239.
[12] J. Lai, Y. Mu, F. Guo, and R. Chen, "Fully privacy-preserving id-based broadcast encryption with authorization," The Computer Journal, vol. 60, no. 12, pp. 1809–1821, 2017.
[13] W. Susilo, R. Chen, F. Guo, G. Yang, Y. Mu, and Y.-W. Chow, "Recipient revocable identity-based broadcast encryption: how to revoke some recipients in ibbe without knowledge of the plaintext," in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016, pp. 201–210.
[14] J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, "Fully privacypreserving and revocable id-based broadcast encryption for data access control in smart city," Personal and Ubiquitous Computing, vol. 21, no. 5, pp. 855–868, 2017.
[15] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in EUROCRYPT 1998. Springer Berlin Heidelberg, 1998, pp. 127–144.
[16] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," Information and System Security (TISSEC), ACM Transactions on, vol. 9, no. 1, pp. 1–30, 2006.
[17] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," in PKC 2008. Springer Berlin Heidelberg, 2008, pp. 360–379.
[18] Z. Cao, H. Wang, and Y. Zhao, "Ap-pre: Autonomous path proxy re-encryption and its application," IEEE Transactions on Dependable and Secure Computing, 2017.
[19] H. Guo, Z. Zhang, J. Xu, N. An, and X. Lan, "Accountable proxy re-encryption for secure data sharing," IEEE Transactions on Dependable and Secure Computing, 2018.
[20] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in ACNS 2007. Springer Berlin Heidelberg, 2007, pp. 288–306.
[21] C. K. Chu and W. G. Tzeng, "Identity-based proxy re-encryption without random oracles," in ISC 2007. Springer Berlin Heidelberg, 2007, pp. 189–202.
[22] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloudbased revocable identity-based proxy re-encryption scheme for public clouds data sharing," in European Symposium on Research in Computer Security. Springer, 2014, pp. 257–272.
[23] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, "Conditional identitybased broadcast proxy re-encryption and its application to cloud email," IEEE Transactions on Computers, vol. 65, no. 1, pp. 66–79, 2016.
[24] K. Liang, M. H. Au, J. K. Liu,W. Susilo, D. S.Wong, G. Yang, Y. Yu, and A. Yang, "A secure and efficient ciphertext-policy attributebased proxy re-encryption for cloud data sharing," Future Generation Computer Systems, vol. 52, pp. 95–108, 2015.
[25] C. Ge, W. Susilo, L. Fang, J. Wang, and Y. Shi, "A cca-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system," Designs, Codes and Cryptography, pp. 1–17, 2018.

[26] Y. Yang andM.Ma, “Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for ehealth clouds,” IEEE Transactions Information Forensics and Security, vol. 11, no. 4, pp. 746–759, 2016.
[27] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X. Phuong, and Q. Xie, “A dfa-based functional proxy reencryption scheme for secure public cloud data sharing,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1667–1680, 2014.
[28] T. Matsuo, “Proxy re-encryption systems for identity-based encryption,” in Pairing 2007. Springer Berlin Heidelberg, 2007, pp. 247–267.
[29] T. Mizuno and H. Doi, “Hybrid proxy re-encryption scheme for attribute-based encryption,” in International Conference on Information Security and Cryptology. Springer, 2009, pp. 288–302.
[30] P. Jiang, J. Ning, K. Liang, C. Dong, J. Chen, And Z. Cao, “Encryption Switching Service: Securely Switch Your Encrypted Data To Another Format,” Ieee Transactions Services Computing, 2018.
[31] Lakshmi, Mannam Swarna, And Kale Masthan Rao. "Dynamic Audit Services For Cloud Outsourced Storages With Key Updates." (2017).

[32] Gupta, Dr K. Gurnadha. "A Productive Ibpre Model For Secure Data Sharing In Blockchain Technology Based Iot."