IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 10, October. 2019, Series -II, PP 69-73

Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing

Rama Krishna Sreerama[1], Dr. K. Venkata Rao[2]
[1]*M.Tech (CSE), Dept. of Computer Science and Systems Engineering,*
[2]*Professor, Dept. of Computer Science and Systems Engineering, Andhra University College of Engineering (A), Visakhapatnam, Andhra Pradesh, India.*
Corresponding Author: Rama Krishna Sreerama
Received 30 September 2019; Accepted 15 October 2019

Abstract: We are entering in a new era of computing technology i.e. Internet of Things (IoT). Data sharing is a significant idea in cloud computing for sharing data to open clients. Cloud gives various services to the clients for getting to data from cloud. Storage as a service, it enables the data proprietors to store and share their data to clients through cloud server. In this kind of service it is important to put cryptographically upgraded access control on the common data, named Identity-based encryption. When getting to data some client's approval is terminated, there ought to be a component that can expel him/her from the framework. Therefore, the repudiated client incapable to get to both the recently put away data. Subsequently, propose an idea called revocable-storage identity-based encryption. In this paper, we actualized and demonstrated that a repudiated client can ready to get to the past data utilizing secret key in Just cloud condition and same data to be shared to open clients.
Key Words: IoT, cloud computing, Future Internet, Secured data sharing, encryption.

I. INTRODUCTION

Internet of Things (IoT) term speaks to a general idea for the capacity of system gadgets to detect and gather data from around the globe, and after that offer that data over the Internet where it tends to be handled and used for different fascinating purposes. The IoT is contained shrewd machines cooperating and speaking with different machines, items, situations and foundations. Presently a day's each individual are associated with one another utilizing loads of correspondence way. Where most prevalent correspondence way is internet so in another word we can say internet which associate people groups. The fundamental thought of the Internet of Things (IoT) has been around for about two decades, and has pulled in numerous scientists and ventures in light of its incredible assessed sway in improving our day by day lives and society. At the point when things like family unit apparatuses are associated with a system, they can cooperate in collaboration to give the perfect service in general, not as a gathering of freely working devices. This is valuable for a large number of this present reality applications and services, and one would for instance apply it to manufacture a brilliant living arrangement; windows can be shut naturally when the forced air system is turned on, or can be opened for oxygen when the gas stove is turned on. The possibility of IoT is particularly profitable or people with handicaps, as IoT advancements can bolster human exercises at bigger scale like structure or society, as the gadgets can commonly coordinate to go about as an all-out framework. Correspondence capacity and remote manual control lead to the subsequent stage … how would I computerize things and, based on my settings and with advanced cloud-based handling, get things going without my intercession? That's a definitive objective of some IoT applications. What's more, for those applications to interface with and influence the Internet to accomplish this objective, they should initially progress toward becoming "brilliant" (fuse a MCU/installed processor with a related one of a kind ID) at that point associated and, at long last, controlled. Those capacities would then be able to empower another class of services that makes life simpler for their clients Cloud computing is a worldview that gives gigantic calculation limit and enormous memory space easily. It empowers clients to get planned services independent of time and area over numerous stages (e.g., cell phones, PCs), and in this way carries incredible comfort to cloud clients. Among various services given by cloud computing, cloud storage service, for example, Apple's iCloud, Microsoft's Azure and Amazon's S3, can offer a progressively adaptable and simple approach to share data over the Internet, which gives different advantages to our general public. A characteristic answer for overcome the previously mentioned issue is to utilize cryptographically authorized access control, for example, identity-based encryption (IBE). Besides, to conquer the above security dangers, such sort of identity-based access control set on the common data should meet the accompanying security objectives: Unauthorized clients ought to be kept from getting to the plaintext of the mutual data put away in the0cloud server. Moreover, the cloud server, which should be straightforward yet inquisitive, ought to likewise be stopped from knowing plaintext of the mutual data. Backward secret implies that, when a client's authorization0is terminated, or a client's secret key is0compromised, he/she ought to be kept from getting to the

plaintext of the in this way shared data that are still encoded under his/her identity. Forward secret implies that, when a client's position is terminated, or a client's secret0key is undermined, he/she ought to be kept from getting to the plaintext of the common data that can be recently gotten to by him/her.

II. RELATED WORK

A. Shamir, "Identity-based cryptosystems and mark schemes [5]" The idea of identity-based encryption was presented by Shamir and advantageously instantiated by Boneh and Franklin. IBE wipes out the requirement for giving an open key framework (PKI). D. Boneh and M. Franklin, "Identity-based encryption from the Weil blending [6]" There ought to be a way to deal with deny clients from the framework when essential, e.g., the expert of some client is terminated or the secret key of some client is unveiled. In the conventional PKI setting, the issue of disavowal has been very much examined by S. Micali, W. Aiello, S. Lodha, and R. Ostrovsky, D. Naor, M. Naor, and J. Lotspiech, C. Nobility, V. Goyal, and a few methods are generally affirmed, for example, certi_cate renouncement list or adding legitimacy periods to declarations. In any case, there are just a couple of concentrates on renouncement in the setting of IBE. Boneh and Franklin proposed a characteristic denial path for IBE. They affixed the present timeframe to the ciphertext, and non-repudiated clients occasionally got private keys for each timespan from the key expert. Lamentably, such an answer isn't versatile, since it requires the key specialist to perform direct work in the quantity of non-renounced clients. What's more, a safe channel is basic for the key specialist and non-renounced clients to transmit new keys. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with e_cient repudiation "[7][8] To overcome this issue, Boldyreva, Goyal, and Kumar acquainted a novel methodology with accomplish proficient denial. They utilized a parallel tree to oversee identity with the end goal that their RIBE plan decreases the multifaceted nature of key disavowal to logarithmic (rather than straight) in the most extreme number of framework clients. In any case, this plan just accomplishes particular security. B. Libert and D. Vergnaud, "Versatile id secure revocable identity-based encryption "[9] The creator proposed an adaptively secure RIBE plan based on a variation of Water's IBE plot, Chen et al. developed a RIBE plot from grids. J. H. Web optimization and K. Emura, "Revocable identity-based encryption returned to: Security model and construction"[10] Recently, Seo and Emura proposed a productive RIBE conspire impervious to a reasonable danger called decoding key presentation, which implies that the divulgence of unscrambling key for current timeframe has no impact on the security of decoding keys for other timespans. 6. K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "A proficient cloud-based revocable identity-based intermediary re-encryption conspire for open clouds data sharing". Motivated by the work Liang presented a cloud-based revocable identity-based intermediary re-encryption that supports client denial and ciphertext update. To lessen the multifaceted nature of renouncement, they used a communicate encryption plan to scramble the ciphertext of the update key, which is autonomous of clients, with the end goal that solitary no repudiated clients can decode the update key. In any case, this sort of renouncement technique can't avoid the plot of disavowed clients and malevolent non-denied clients as pernicious non-repudiated clients can share the update key with those denied clients. Moreover, to refresh the ciphertext, the key specialist in their plan needs to keep up a table for every client to create the re-encryption key for each timespan, which fundamentally builds the key expert s outstanding burden.

III. Methodology

A. Outsourcing Data in Cloud

Outsourcing is a familiar method where the third party executes some function for the sake of the company, frequently for the IT department which do not have the resources to undertake. It is an important method for the global information sharing. One of the important services in outsourcing is the database outsourcing during this process the data must be secured from the hackers.

B. Cryptography

Cryptography is a method which is used for storing and transforming the data in the particular form so that only the intended users can read or process the data easily. Cryptography access control is a commonly used technique for the purpose of securing the data on the entrusted servers. Usually when we use this kind of servers then the sensitive data is encrypted before outsourcing the data and the decryption keys will be given only to the approved users and only by using these keys they can decrypt the data without these keys even the servers are not able to decrypt the data. Cryptography is usually classified into 3 different phase they are as follows:

A. Secrete key cryptography.
B. Public key cryptography.
C. Hash function cryptography.

A. Secrete Key Cryptography

A single key will be used by both the user and the receiver here the user contains a key for the data encryption then a similar key will be used by the receiver to decrypt the data hence both users share the same key for encryption and decryption.

B. Public Key Cryptography

In this it consists of two keys the one key will be used by the sender and the receiver to secure the data and other key between the receiver and the sender to insecure the provide data content.

C. Hash Function Cryptography

In this it does not contain any key pairs instead it uses the hash values which will be processed on the basis of the text message content. It is used to check whether the sent data is not altered by others and the data is not affected by the virus. In cryptography we have various methods:

• Substitution methods.
• Reciprocal methods.
• Symmetric methods.
•Asymmetric methods.

The security for the data can be most commonly done by using the Asymmetric method and this method is also called as the public-key method. In this method the key holder will be provided with two keys the public key and the private key content.

C. Encryption and Decryption

For the purpose of securing the data in cloud we use the encryption and decryption methods. The security for the data can also be done using the following phases:

D. Generating the Keys and Authentication Method

Users are said to store their id secretly because it acts as a tool to verify the user every time when they login to the system. The valid users have some id/password combinations for the purpose of providing the security to their data. The authentication can be done through biometrics were we look into fingerprint, voice face, keyboard timings of the users. The authentication can also be done by cipher text content. The cipher text is an encrypted text where the data result will be obtained in an encrypted format. The data owner's identification, significance and the key (master/public) of the data owners attributes will be contained in the cipher class content.

E. Key Aggregation

When data is shared over the distributed cloud environment it can be secured by providing the aggregate key. For the particular data owners the aggregate key consists of some identity to find the perfect identifier along with the attribute based modules. This key is usually used to share the data between each other using some secret keys in between them. Key aggregation authorizes the users/data provider to share data with others in a confident way by using some small cipher text expansion, and this text can be provided to each authorized users by providing a single and small aggregate keys. These aggregate key can be sent to the authorized user through any means of communication mode secretly, the communication mode can be via email, SMS etc. This aggregate key helps the other user to decrypt the data.

Key Revocation Process

Revocation means recall. By public key infrastructure and Certificate Revocation List (CRL) therevocation operation can be done in cryptosystem. The CRL contains a list of certificate that is revoked. Firmly removing the compromised keys can be done by revocation process. Based on the data owners id the keys/data are revoked in cloud. When the master key content and the public key content are redefined then the revocation event will be called related to their variable attribute and later by using the master key the data will be re-encrypted.

Proxy re-encryption and Identity Based Encryption (IBE)

The secure communication can be done in the public key cryptography when both the sender and receiver tries to create an encryption and signature key pairs to the data content that has to be secured and then submit the certificate request to the Certificate Authority (CA) along with the proof of identity and then receive the CA-signed certificate which is used for validation and then later they exchange the encrypted message. This process was time consuming and to out come from this process the identity based encryption was introduced. This as the following advantage:

1. In IBE system we use strings such as email address or IP address are used for the public key to the user content instead of issuing certificate or revocation keys.
2. Users does not store any additional decryption key in proxy re-encryption, i.e only by using the users own secret keys the decryption process will be completed.

IV. IoT AND CLOUD COMPUTING FOR FUTURE INTERNET

The term of Future Internet is a collection of data communication network technologies in the future. The Internet of Things (IoT) is the most important concept of Future Internet for providing a common global IT Platform to combine seamless networks and networked things. In the future Internet, people will be connected Anytime, Anyplace, with anything and anyone, and appropriately utilizing any network and Any Service. In other words, the IoT addresses the Convergence, Content, Collections, Computing, Communication, and Connectivity between people and things [1]. On the other hand, Cloud Computing [2] is regarded as the backend solution for processing huge data streams and computations while facing the challenges of everything will be connected with seamless networks in the future. Cloud technologies can provide a virtual, scalable, efficient, and flexible data centre for context-aware computing and online service to enable IoT. Both the IoT and Cloud Computing are the trends of Future Internet. However, the developments of IoT technology are diversity and are not interoperable. That results the service providers and operators have no definite specification to follow. On the other hand, the cloud computing solutions are depended on service providers. Since many international organizations are devoted to work out their specifications for providing a common architecture of networks and software. Thus, we regard the IP Multimedia Subsystem (IMS) is the ideal solution for fulfilling the requirements. However, there are still many challenges for IMS being the network and software fabric between IoT and Cloud. In this paper, we discuss the open challenges and propose the possible solutions for Future Internet. Finally, we construct an early IoT bootstrap platform to provide the discussion of those open challenges and solutions for deploying IoT in Future Internet.Internet of Things (IoT) has immense potential to change many of our daily activities, routines and behaviors. The pervasive nature of the information sources means that a great amount of data pertaining to possibly every aspect of human activity, both public and private, will be produced, transmitted, collected, stored and processed. Consequently, integrity and confidentiality of transmitted data as well as the authentication of (and trust in) the services that offer the data is crucial. Hence, security is a critical functionality for the IoT. Enormous growth of mobile devices capability, critical automation of industry fields and the widespread of wireless communication cast need for seamless provision of mobile web services in the Internet of Things (IoT) environment. These are enriched by mobile cloud computing. However, it poses a challenge for its reliability, data authentication, power consumption and security issues. There is also a need for auto self-operated sensors for geo-sensing, agriculture, automatic cars, factories, roads, medicals application and more. IoT is still highly not reliable in points of integration between how its devices are connected, that is, there is poor utilization of the existing IP security protocols. In this chapter, we propose a deep penetration method for the IoT connected set of devices, along with the mobile cloud. An architecture and testing framework for providing mobile cloud computing in the IoT that is based on the object security, power utilization, and latency measures and packet loss rate is explained.

V. Proposed System

In our proposed, we introduce a notion called revocable storage identity-based encryption ABE for building a cost-effective data sharing system that fulfills the three security goals. More precisely, the following achievements are captured .We provide formal definitions for ABE and its corresponding security model. We present a concrete construction of ABE the proposed scheme can provide confidentiality and backward/forward2secrecy simultaneously. We prove the security of the proposed scheme in the standard model, under the decisional assumption. In addition, the proposed scheme can withstand decryption key exposure. The proposed scheme is efficient in the following ways: The procedure of cipher text update only needs public information.

We provide formal definitions for RS-IBE and its corresponding security model; we present a concrete construction of RS-IBE. The proposed scheme can provide confidentiality and backward/forward2 secrecy simultaneously. We prove the security of the proposed scheme in the standard model, under the decisional ℓ-Bilinear DiffieHellman Exponent (ℓ-BDHE) assumption. In addition, the proposed scheme can withstand decryption key exposure. The procedure of ciphertext update only needs public information. Note that no previous identity-based encryption schemes in the literature can provide this feature; The additional computation and storage complexity, which are brought in by the forward secrecy, is all upper bounded by O(log(T)2), where T is the total number of time periods.

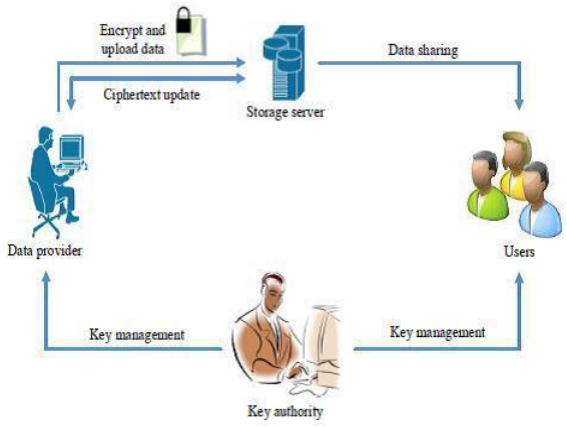

Fig. Proposed Architecture Diagram

VI. Conclusion

The IoT promises to deliver a step change in individuals‟ quality of life and enterprises‟ productivity. Through a widely distributed, locally intelligent network of smart devices, the IoT has the potential to enable extensions and enhancements to fundamental services in transportation, logistics, security, utilities, education, healthcare and other areas, while providing a new ecosystem for application development. A concerted effort is required to move the industry beyond the early stages of market development towards maturity, driven by common understanding of the distinct nature of the opportunity. This market has distinct characteristics in the areas of service distribution, business and charging models, capabilities required to deliver IoT services, and the differing demands these services will place on mobile networks.With The Cloud Computing, we can access our data anytime anywhere. In this paper, we are implementing a tool which will be of no high cost but It we will give better security, Its called Revocable storage identity based encryption, which will do both the things simultaneously which are identity revocation and ciphertext update, which will prevent user from accessing the shared data which is previously shared, as well as subsequently shared data.RS-IBE is better than others in the security in terms of efficiency and functionality, and RSIBE is more reliable. We also added the Fragment storage for this system. We can also save the Each Fragment on different Servers but that will be included in Future Scope.

References

[1]. L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud de_nition" ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50 55, 2008.
[2]. K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, Social cloud computing: A vision for socially motivated resource sharing, Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551 563, 2012.
[3]. C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, Privacypreserving public auditing for secure cloud storage, Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362 375, 2013.
[4]. G. Anthes, Security in the cloud, Communications of the ACM, vol. 53, no. 11, pp. 16 18, 2010.
[5]. A. Shamir, Identity-based cryptosystems, and signature schemes, in Advances in cryptology. Springer, 1985, pp. 47 53.
[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]. V. Goyal, Certi_cate revocation using _ne grained certi_cate space partitioning, in Financial Cryptography and Data Security. Springer, 2007, pp. 247 259.
[8]. A. Boldyreva, V. Goyal, and V. Kumar, Identity-based encryption with e_cient Revocation, in Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008, pp. 417 426.
[9]. B. Libert and D. Vergnaud, Adaptive-id secure revocable identity-based encryption, in Topics in Cryptology CT-RSA 2009. Springer, 2009, pp. 1 15.
[10]. J. H. Seo and K. Emura, Revocable identity-based encryption revisited: Security model and construction, in Public-Key Cryptography PKC 2013. Springer, 2013, pp. 216 234.

Rama Krishna Sreerama." Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing." IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 10, 2019, pp. 69-73.