International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 12, Issue 10 (October 2016), PP.67-05-72

Contributory Broadcast Encryption on Group key Agreement For key Distribution Encryption & Decryption

S.Srinivas[1] Abhay Kumar[2]
[1]*M-Tech Dept Of CSE JB Institute Of Engineering And Technology, R.R. District, Hyderabad, TS.*
[2]*Associate Professor Dept Of CSE JB Institute Of Engineering And Technology, R.R. District, Hyderabad, TS.*

Abstract: Encryption is utilized in a communication system to secure information in the transmitted messages from anyone other than ye well aimed receiver. To execute the encryption plus decryption ye transmitter and receiver should have corresponding encryption plus decryption keys. For shipping precaution information to group needed broadcast encryption (BE). BE sanctions a sender to securely broadcast to any subset of members and require a trusted party to distribute decryption keys. Group key acquiescent (GKA) protocol sanctions a number of users to establish a mundane secret channel via open networks. Celebrating that a major destination of GKA for majority applications is to engender a confidential channel among group members, but a sender cannot omit any special member of decrypting ye cipher texts. By bridging BE and GKA notion with a hybrid primitive related to as contributive disseminate encryption (CBE). With these primitives, a group of members move through a mundane public encryption key while each member having there decryption key. A sender visually perceiving the public group encryption key can circumscribe the decryption to subset of members of sender‘s cull. A simple way to engender these keys is to utilize the public key distribution system invented by Daffier and Hellman. That organization, however, pass alone one match of communication stations to apportion a particular pair of encryption and decryption keys. Key distribution sets are acclimated to engender keys and Elliptic Curve Cryptography (ECC) is utilized for the encryption and decryption of documents; and this going to provide the security for the documents over group communication.

Keywords: Contributory Broadcast Encryption, Group Key Agreement, Key Distribution Set, Key Distribution Set, Encryption, Decryption.

I. INTRODUCTION

With the expeditious advance and pervasive deployment of communication technologies, there is an incrementing authoritative ordinance of multifarious cryptographic primitives to bulwark group communications and computation platforms. These incipient platforms include instant-messaging implements, collaborative computing, mobile ad hoc networks and convivial networks. These incipient applications call for cryptographic primitives sanctioning a sender to firmly encrypt to whatever set of ye users of the accommodations without relying on a planarity trusted dealer. Disseminate Encryption (BE) is a well-analyzed primitive aimed for assure group-oriented communications. It sanctions sender to securely broadcast to any subset of ye group members. However, a BE scheme hard depends on a planarity trusted key server who engenders mystery decryption keys for ye group members plus can read all the communications to any members. As a result of the incremented popularity with group-oriented applications and protocols, group communication occurs in many different settings of net layer multicasting to application layer. Regardless of the security accommodations, underlying environment are indispensable to provide communication privacy and integrity. While peer-to-peer security is a mature and well formulated field, ye assure group communication stays comparatively unexplored. Contrary to a prevalent initial impression, assure group communicating is not a uncomplicated propagation of secure two-party communication. There are two paramount differences. First, protocol efficiency is of more preponderant concern due to the number of participants and distances amongst them. Ye second divergence is imputable to group dynamic. Communication between two-parties can be viewed as a discrete phenomenon. It commences, lasts for a while, and ends. Group communication is more intricate. It commences and the group appendages give plus join ye group plus there may not be a well-defined end [3].

A group key accidence (GKA) is another well-realized cryptographic primitive to ensure group pointed communications. A conventional GKA sanctions a group of members to compose a mundane secret key via open networks. However, whenever a sender wants to send content to a group, his mustiness beginning join ye group and run a GKAs protocol to apportion a secret key with the intended members. More recently, and to surmount this constraint, Wu et al. introduced asymmetric group key accidence, in which only a prevalent group public key is negotiated and each group member holds there different decryption key. However, neither conventional symmetric group key acquiescent nor the incipiently introduced asymmetric GKA [4] sanction the sender to unilaterally omit any particular member from reading the plain text. Hence, it is essential to find more

flexible cryptographic primitives sanctioning dynamic broadcasts without a planarity trusted dealer. Contributory Broadcast Encryption (CBE) primitive, which is a intercrossed of GKA plus BE.
The model with the CBE primitive and formalize its security definitions. CBE incorporates the underlying conceptions of GKA and BE. A group of members interact via open networks to negotiate a world encryption central while for each one member holds a dissimilar secret decryption key. Utilizing the public encryption key, anybody from ye group can encrypt whatever message to any subset of the group members and only ye proposed recipients can decrypt. Unlike GKA, CBE sanctions the sender to omit some members from reading the cipher texts. Compared to BE, CBE does not require a planarity trusted third party to establish the systems. With formalize collusion resistance by defining an assailer who can planarity control all the members outside the intended receivers but cannot extract utilizable information from the cipher text.

II. RELATED WORK

Ankush V. Ajmire, Prof. Avinash P. Wadhe [1] has given the concept about possible way to bridge ye GKA plus BE notation in which group member can send the secure document to the other with some member to omit into it by introducing the CBE. So CBE model efficient and secure in the standard model.

C.K. Wong, M. Gouda and S. Lam[2] proposed to address the scalability quandary of group key management, author propose the utilization of key trees in which they looked into three rekeying schemes, key-oriented , group-oriented, user oriented, and designated join/leave protocols because them. Ye rekeying protocols plus strategies are enforced in a prototype key waiter author bear built. From the quantification results of a sizably voluminous number of experimentations, authors resolve that their group key server utilizing any of the three rekeying strategies is scalable to profoundly and immensely colossal groupings with patronize allows for and joins. In particular, the average server processing time per leave/join increases linearly with the logarithm of group size.

J.H. Park, H.J. Kim, M.H. Sung and D.H. Lee [3] have proposed two planarity collusion-resistant disseminate encryption systems for homeless recipients. The paramount way to construct their rudimental scheme has been to utilize the algebraic property of Vigorous Daffier-Hellman tulles. Next elongated the general scheme to obtain the culled cipher text security by applying the hash-predicated method. By coalescing general and rudimental schemes, authors were able to obtain a PKBE scheme for shorter transmissions while preserving utilizer storage cost. They proposed schemes had a retreat of commanding more than calculation cost in the decryption algorithm, but if they utilize set differences, this drawback can be scarcely alleviated.

Z. Yu and Y. Guan propose a key management scheme by utilizing deployment erudition for the wireless sensor networks. In author‘s scheme, neighbor nodes can utilize stored secret information more efficiently to engender pair wise keys. Author studied about network connectivity predicated on geometric desultory graph model and shows how to compute transmission range for achieving the desired connectivity. Simulation results show that author‘s strategy surpasses others in price of resiliency against node capture. Meanwhile, it achieves a higher property with a snippier transmitting range and a lower recollection requisite.

III. IMPLEMENTATION

3.1 key generation technique:

Key distribution sets (KDS) [6] are habituated to engender key in which there are variants of accumulation of character are taken from end utilizer at run time which is cognate to the document which utilizer are going to apportion on the intended group with group key acquiescent. Following are the few definitions of the KDS which giver consummate conception about who the sets are form and key is engendered by utilizing the definitions. Definition 1 = docid-S|!-docname-ddate-R|3419-username
Definition 2 = ddate-username-R|4444-docname-docid-S|% Definition 3 = docname-S|$-username-R|7424-docid-ddate
Docid: - which is the id of the document which is share among the group.
S| {! %,$,@,#} :- S denotes the special symbol in which we have taken any symbol from the sets of the five symbol.
Docname: - is the designation of the document at the time of sending taken given by the utilizer.
Ddate: - Date on which the document is going to apportion to the intended group.
R|3419:- R denotes the four digit arbitrary number engendered by the system in which system can engender any number from 0000 to 9999 at arbitrarily.

Username: - username of the sender which are going to apportion the document on a particular group or a single utilizer which store their document on server for security purport. Desultory numbers are astronomically subsidiary, for example, in engendering goes in a game or as test information for computer programs. If one is asked to "pick a number between one and a hundred", the task seems simple enough. But, if you require genuinely arbitrary numbers (each number is equipollent probable!), and if you optate to engender

them from a computer, the task is quite tricky as it turns out. Mathematicians have labored over this quandary, and have devised robust techniques to engender desultory numbers. However, computers are deterministic (all actions are prognostic able at some level!), and, so, engendering numbers that are "authentically" desultory is not possible. However, we can get fairly proximate. Algorithms that engender desultory numbers, admittedly, provide "pseudorandom" numbers. But, for most purposes this is adequate.

Key generation working:

KDS engender for the every branch of the registered customer. It will cull any one KDS set from the KDS set available utilizing arbitrary algorithm. Arbitrary algorithms again cull the any one algorithm from culled set of algorithm and engender key utilizing that algorithm which engender session secrete key plus Store session release key in Database in encrypted format [7].

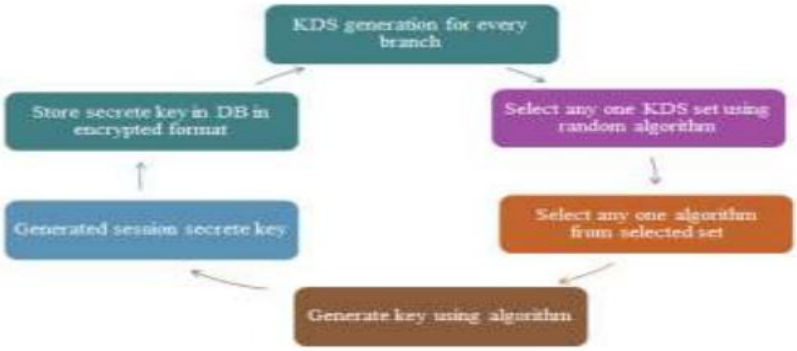

Figure 1 Key generation working.

Elliptic Curve Cryptography (ECC)

Elliptical curve cryptography (ECC) is a public key encryption technique predicated on elliptic curve theory that can be acclimated to engender minuter, more expeditious and more efficient cryptographic keys [8]. ECC engenders keys through the properties of the elliptic curve equation in lieu of the traditional method of generation as the multiplication of profoundly and astronomically immense prime numbers.

The primary benefit promised by ECC is reducing storage, a more minuscule key size and transmission requisites, i.e. that an elliptic curve group could provide the same level of security Afforded by an RSA-predicated system with a sizably voluminous modulus and correspondingly more astronomically immense key. One main advantage of ECC is its diminutive key size. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA [9].

The equation of an elliptic curve is given as,

$\mathbf{Y^2=x^3+ax+b}$

Few terms that will be used,
E - Elliptic Curve
P - Point on the curve
n -Maximum limit (This should be a prime number)

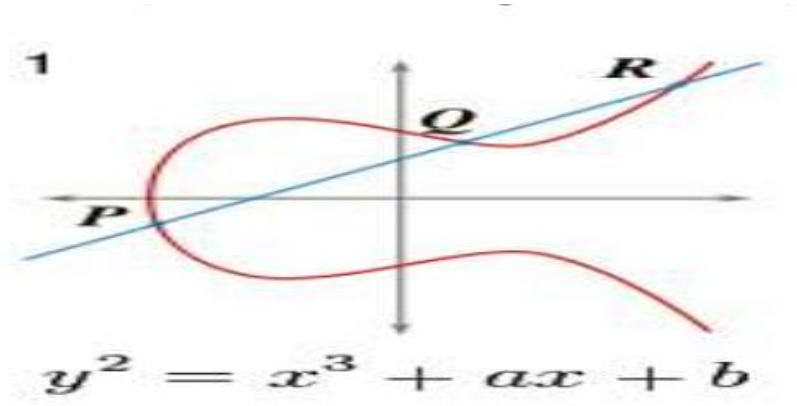

Figure 2 Simple elliptic curves.

Key Generation

Key generation is an important part where user has to generate both public key plus secret key. The transmitter will be encrypting ye content with receiver‘s public key and the receiver will decrypt its private key. Now, user have to select a number ‗d‘within the range of ‘n’
Using the following equation we can generate the public key

Q=d*p

d = the random number that user have selected within the
Range of (1 to n-1).
P is the point on the curve.
Q is the public key.
d is the private key.

Encryption:

Let ‗m‘be the message that user are sending. User has to represent this message on the curve. This has in-depth implementation details. All the advance research on ECC is done by a company called certicom.
Consider ‘m’ has the point ‘M’ on the curve ‘E’. Randomly select ‗k‘ from [1 – (n-1)].Two cipher texts will be gave let it be C1 and C2 [10].
C1=k*p
C2=M+k*Q
C1 and C2 will be sending.

Decryption:

User has to get back the message ‘m’ that was send to us
M = C2 – d * C1
M is the original message that we have send.

Proof:

How do we get back the message?
M = C2 – d * C1
‗M‘ can be represented as ‗C2 – d * C1‘
C2 – d * C1 = (M + k * Q) – d * (k * P)
Where (C2 = M + k * Q and C1 = k * P)
= M + k * d * P – d * k *P
(Canceling out k * d * P)
= M (Original Message)

Upload / Download Working:

In uploading and downloading provides the information about the how the file to be uploaded and already uploaded files how to download it. Designate the group sapient access sanction which includes the sanction about the group that is GKA which group having sanction to upload the files and that access sanction store into database so that whenever required then fetches access sanction from database. Encrypt the document by utilizing contributory broadcast encryption algorithm document will be share in encrypted format only the utilizer having valid key to decrypt the document can only decrypt that document [11]. Group will designate and verify the group key and send session secret key to the intended user‘s mail id after key designation and validation of session secret key utilize are sanction decrypting the document

Figure 3 Upload / Download working.

IV. EXPERIMENTAL WORK

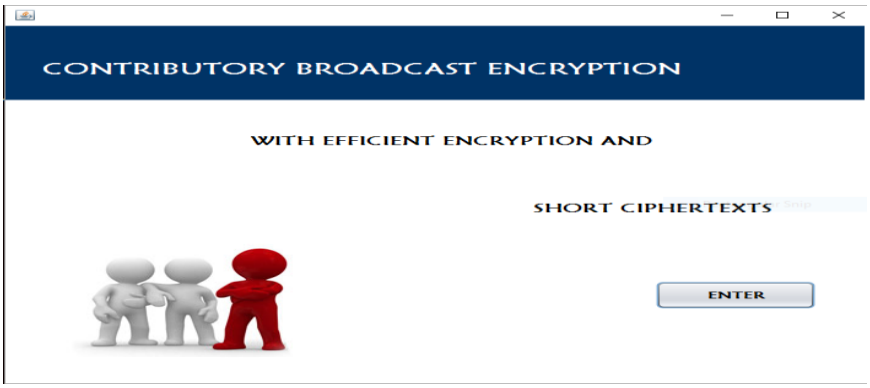

Fig 4: System Home Page.

Fig 5: Encryption and Short Ciphertext.

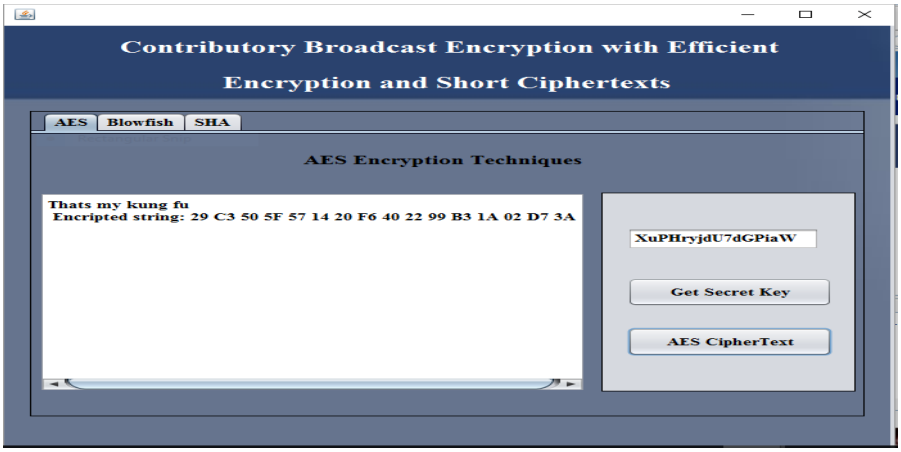

Fig 6: AES_Encryption Technique.

Fig 7: Data Efficiency.

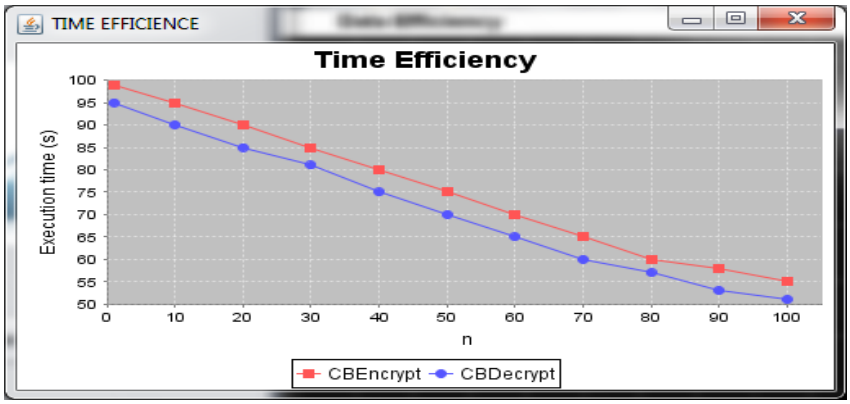

Fig 8: Time Efficiency.

V. CONCLUSION

The CBE is a primitive which bridges the GKA and BE notions. In CBE, anyone can send secret messages to any subset of the group members, plus ye organization does not involve a trusted key server. Neither the vicissitude of the sender nor the dynamic cull of the intended receivers requires extra rounds to negotiate group encryption / decryption keys. Following the CBE model, here instantiated an efficient CBE scheme that is secure in the standard model. As a multifarious ECC algorithm primitive and KDS, CBE notion opens an incipient avenue to establish secure broadcast channels and secure legion issuing disseminated calculation apps. Our system is going to avail to group communication in which there is need to apportion documents in secure and to intended utilizer.

REFERENCES

[1]. Ankush V. Ajmire, Prof. Avinash P. Wadhe,‖Review paper on Key Generation Technique With Contributory Broadcast Encryption, ‖ IC-QUEST 2016, 5Th International Conference on Quality Up-gradation in Engineering, Science & Technology on 12th April 2016.

[2]. C.K. Wong, M. Gouda and S. Lam, ―Secure Group Communications Using Key Graphs,‖ IEEE/ACM Transactions on Networking, vol. 8, no. 1, pp. 16-30, 2000

[3]. J.H. Park, H.J. Kim, M.H. Sung and D.H. Lee, ―Public Key Broadcast Encryption Schemes With Shorter Transmissions,‖ IEEE Transactions on Broadcasting, vol. 54, no. 3, pp. 401-411, 2008.

[4]. Z. Yu and Y. Guan, ―A Key Management Scheme Using Deployment Knowledge for Wireless Sensor Networks,‖ IEEE Transactions Parallel Distributed Systems, vol. 19, no. 10, pp. 1411-1425, 2008.

[5]. Q. Wu, B. Qin, L. Zhang, J. Domingo, ―Contributory Broadcast Encryption with Efficient Encryption and Short Ciphertexts,‖ IEEE Transactions On Computer, 2015.

[6]. I. Ingemarsson, D.T. Tang and C.K. Wong, ―A Conference Key Distribution System,‖ IEEE Transactions on Information Theory, vol. 28, no.5, pp. 714-720, 1982.

[7]. Q. Wu, Y. Mu, W. Susilo, B. Qin and J. Domingo-Ferrer, ―Asymmetric Group Key Agreement,‖ in Proc. Eurocrypt 2009, 2009, vol. LNCS 5479, Lecture Notes in Computer Science, pp. 153-170.

[8]. Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer and O. Farras, ―Bridging Broadcast Encryption and Group Key Agreement,‖ in Proc. Asiacrypt2011, 2011, vol. LNCS 7073, Lecture Notes in Computer Science, pp. 143-160.

[9]. D. H. Phan, D. Pointcheval and M. Strefler, ―Decentralized Dynamic Broadcast Encryption,‖ in Proc. SCN 2012, 2011, vol. LNCS 7485, Lecture Notes in Computer Science, pp. 166-183.

[10]. M. Steiner, G. Tsudik and M. Waidner, ―Key Agreement in Dynamic Peer Groups,‖ IEEE Transactions on Parallel and Distributed Systems, vol. 11, no. 8, pp. 769-780, 2000.

[11]. A. Sherman and D. McGrew, ―Key Establishment in Large Dynamic Groups Using One-way Function Trees,‖ IEEE Transactions on Software Engineering, vol. 29, no. 5, pp. 444- 458, 2003.

[12]. Y. Kim, A. Perrig and G. Tsudik, ―Tree-Based Group Key Agreement,‖ ACM Transactions on Information System Security, vol. 7, no. 1, pp. 60-96, 2004.

[13]. Y. Mao, Y. Sun, M. Wu and K.J.R. Liu, ―JET: Dynamic JoinExit- Tree Amortization and Scheduling for Contributory Key Management,‖ IEEE/ACM Transactions on Networking, vol. 14, no. 5, pp. 1128-1140, 2006.

[14]. M. Abdalla, C. Chevalier, M. Manulis and D. Pointcheval, ―FlexibleGroup Key Exchange with On-demand Computation of Subgroup Keys,‖ in Proc. Africacrypt 2010, 2010, vol. LNCS 6055, Lecture Notes in Computer Science, pp. 351-368.