PRIVACY-PRESERVING REDISTRIBUTED KEY-POLICY ATTRIBUTE-BASED SECRET WRITING

The Computer Science Department, Bharath University, Chennai, Tamilnadu, India

Mac Donald Khongwir (mac.d.fedrick@gmail.com)

The Computer Science Department, Bharath University, Chennai, Tamilnadu, India

Debabrata Laimayum (rastafarian007@gmail.com)

The Computer Science Department, Bharath University, Chennai, Tamilnadu, India

Ms. Anuradha (Asst.professor)

Abstract: decentralized attribute-based secret writing (ABE) could be a variant of a multi-authority ABE theme wherever every authority will issue secret keys to the user severally with none cooperation and a central authority.[1] This can be in distinction to the previous constructions, where multiple authorities should be on-line and setup the system interactively, that is impractical. Hence, it's clear that a decentralized ABE theme eliminates the serious communication price and also the want for cooperative computation within the setup stage. Moreover, every authority will be part of or leave the system freely while not the requirement of re-initializing the system. [2] In modern multi-authority ABE schemes, a user's secret keys from completely different authorities should be tied to his world symbol (GID) to resist the collusion attack. However, this may compromise the user's privacy. Multiple authorities will collaborate to trace the user by his GID, collect his attributes, and then impersonate him. [3] Therefore, constructing a decentralized ABE theme with privacy-preserving remains a difficult analysis problem. During this paper, we tend to propose a privacy-preserving decentralized key-policy ABE theme wherever every authority will issue secret keys to a user severally while not knowing something regarding his GID. Therefore, albeit multiple authorities are corrupted, they cannot collect the user's attributes by tracing his GID. [4]Notably, our theme solely needs normal quality assumptions (e.g. decisional additive Diffie-Hellman) and doesn't need any cooperation between the multiple authorities, in distinction to the previous comparable theme that needs non-standard quality assumptions (e.g., q-decisional Diffie-Hellman inversion) and interactions among multiple authorities. To the simplest of our data, it's the primary decentralized ABE theme with privacy-preserving supported standard quality assumptions.[5]

I. INTRODUCTION

Privacy-preserving decentralized key-policy ABE wherever every authority will issue the secret keys to a user severally with none cooperation and a central authority. [6]As a result of this, even if multiple authorities' area unit corrupted, they cannot collect the user's attributes by tracing his GID. In AN ABE theme, each the user's secret keys and also the cipher text area unit labeled with sets of attributes. [7] Currently the cipher will encrypt a message underneath a collection of attributes. If wish to decipher the cipher text means that, the receiver should get the information if and on condition that there's a match between his secret keys and also the attributes listed within the cipher text. However in existing multiple authorities' area unit interconnected as a result of this we tend to area unit oral communication that isn't that a lot of secure. [8]As a result of multiple authorities will able to collect user's data by tracing international symbol.

II. Existing System

In existing we tend to used decentralized ABE theme to resist the collusion attack with the help of world symbol GID. World symbol is employed to tie all the user's secret keys from multiple authorities along. [9] So as to let the cipher text be freelance of the user's GID, the central authority should work out a special secret key for the user exploitation his secret key and different authorities' secret keys. [10]Though this theme isn't a centralized ABE theme. However, this will compromise the user's privacy. Multiple authorities will collaborate to trace the user by his GID, collect his attributes, and so impersonate him. [11]

III. Existing System Technique Explanation:

In associate open communication surroundings, sensitive information should be encoding before being transmitted. [12]To do this, encoding theme is utilized to guard the confidentiality of the sensitive information. There are a unit several encoding theme area unit accustomed cypher the information. In existing we tend to used attribute based mostly encoding. [13]

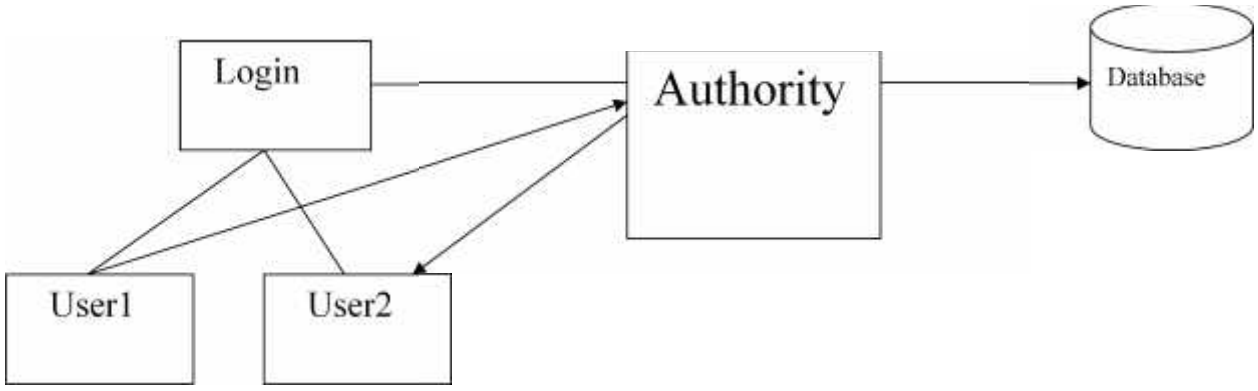
IV. Proposed System

Hear we have a tendency to area unit mistreatment Privacy-preserving localized key-policy ABE theme. [14] This scheme is for giving privacy to multiple authorities and each and every authority will issue secret keys to the users. With the assistance of the attribute based mostly secret writing theme, we have a tendency to area unit storing each user's secret keys and cipertext area unit labeled with the set of attributes. [15]Protecting privacy is a vital issue in distributed systems. Therefore, our privacy preserving decentralized KP-ABE theme are often used as a sound resolution to construct privacy preserving data transfer and access management schemes in distributed systems, wherever knowledge owner will encrypt his knowledge below whose attributes satisfy the desired access structure will access the information. Due to this we will improve the privacy and security. [16]

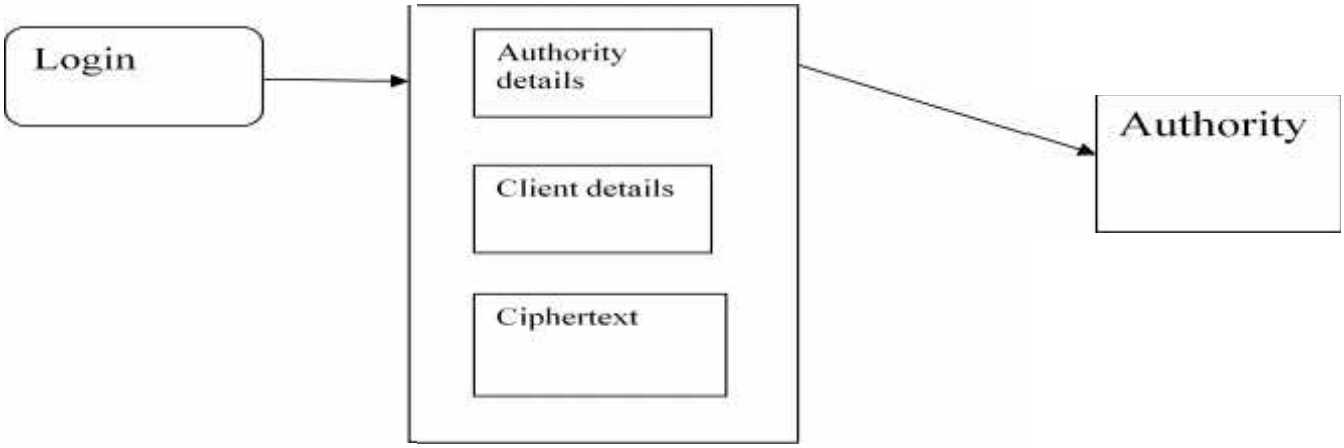
V. Scope of the Project

Main aim of the project is to transfer the date with security. As an example 2 users square measure there. They want to speak with one another. Thus user1 encipher the info with a key that is received by authority and send this knowledge to user2. Currently user2 wish to rewrite that knowledge. So user2 can raise key from authority. Authority can generate the key relying upon the user and send this key to user World Health Organization needs to rewrite the info.

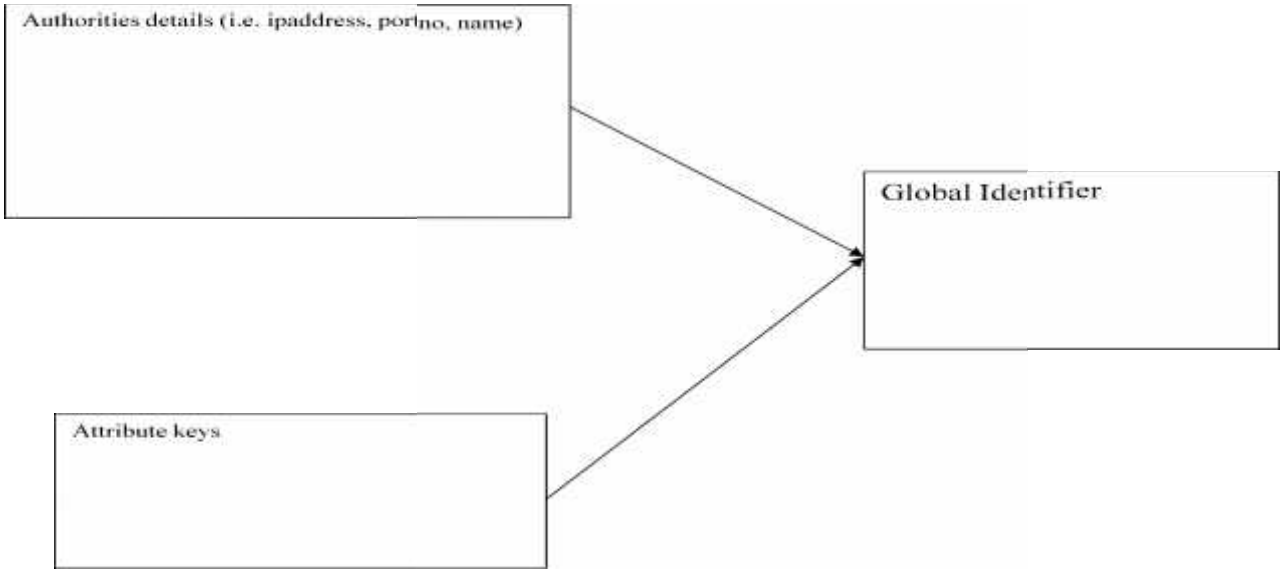
USER INTERFACE DIAGRAM



NETWORK CREATION



GLOBAL IDENTIFIER



VI. LISTS OF MODULES

1. **User Interface Design**
2. **Authority Creation**
3. **Network Creation**
4. **Global Identifier**
5. **Data Transmission**

1. **USER INTERFACE DESIGN**

User interface style or interface engineering is that the style of computers software system applications and websites with the main target on the user's expertise and interaction. During this we tend to area unit mistreatment Swing package in java to style the interface. Swing could be a convenience toolkit for java. It's a part of Sun Microsystems' Java Foundation categories (JFC)-an API for a graphical interface (GUI) for Java programs.

2. **AUTHORITY CREATIONS**

During this module, we tend to area unit making the authority for knowledge transmission and generating keys for attributes. Authority ought to need to understand the small print of the every user in their network. as an example, AN authority having 2 user details if new user moving into the network suggests that these details conjointly should understand by authority and user1 needs to send a knowledge to user2, he can send a message initial to authority then authority can determine that individual user and transfer the message these message are going to be in cipher text formats. Authorities should not have any communication as a result of we tend to area unit causation the message through authority solely and generating keys if 2 authorities area unit in inter-connection implies that 2 authorities can share each and every message and notably attribute keys. Due to this, authority not having privacy, however authority should have privacy at constant time need to defend the key keys. Authority are going to be running specifically ip address and port no. each authority should run in several port no. unremarkably authority having details of client's data. Consumer data suggests that name, ip address and port no of the consumer.

3. **NETWORK CREATION**

After making the authority, we tend to area unit getting to produce the users this is often aforesaid to as a network. A network contains authority and users to speak with one another. In this module, we tend to area unit making users. They need to send the information from one user to a different user. Authorities not having any communicate as a result of this each consumer should understand the identification of authorities, for what means? To send the information from one user to a different user. Once we would like to form the user suggests that, initial user need to register their details into info. Once register details into info, user ought to be login to form user window. Currently user has created to transfer message to a different user. Currently user having details of each and every authority. Thus we are able to choose the authority and destination consumer and send message and authority get that message to any method. Suppose we would like to login suggests that, it'll check from info. If with success validates suggests that it'll come back true then user are going to be created.

4. **GLOBAL IDENTIFIER**

In this module, we tend to area unit making the world symbol. This GID accustomed store the small print of the authorities and each and every user attribute keys. Each user having the attribute worth and these attribute values area unit reborn into keys for causation messages. These keys area unit generated by authority relying upon the user attributes and these attribute area unit stores into international symbol. Once these keys area unit matched then solely able to} able to rewrite the message. unremarkably use of the world symbol is, multi-authority ABE schemes, a user's secret keys from totally different authorities should be tied to his international symbol (GID) to resist the collusion attack. In existing multiple authorities' area unit in cooperation. Thus it'll compromise the user's privacy. Multiple authorities will collaborate to trace the user by his GID, collect his attributes then impersonate him. In our project, we tend to plan a Privacy conserving localized key-policy ABE theme wherever every authority will issue secret keys to a user severally while not knowing something regarding his GID.

5. **DATA TRANSMISSION**

This module is for knowledge transmission from one user to a different user. As an example, user needs to send a message suggests that, these messages are going to be encrypted and send it to authority. Authority

identifies that message and sends that message to a different user. If user needs to rewrite the message suggests that, that individual user should have the keys that is send from authority then solely he will ready to rewrite the message if not matched these keys suggests that can't rewrite that message. As an example, user1 needs to send AN encrypted message to user2, user1 generate a cipher text and sent this cipher text to user2 then message are going to be receiver in user2.Currently user2 need to rewrite that message at that point we tend to area unit implementing 2-party secure computation protocol, it'll generate a secret key to rewrite that message. That secret key are going to be generated to each user, thus should receive key from authority then solely able to} able to rewrite that message.

VII. FUTURE ENHANCEMENT

In future we have a tendency to analysis the rationale for cryptography downside and conclude that node ends up in this downside. When identification we have a tendency to ferret that node from this network which node tries to come back at same network suggests that it cannot enter into the network.

VIII. CONCLUSION

This paper projected the Privacy-preserving sub urbanized key-policy ABE theme, from this we are able to offer the privacy to each and every authority to require own call. Malicious authorities cannot get user's attributes and secret keys as a result of authorities not having any cooperation between them and no got to submit his GID to authorities.

REFERENCES

[1] B. C. Neuman and T. Ts'o, "Kerberos: An authentication sewice for computer networks," *IEEE Communications Magazine*,vol.32, no. 9, pp. 33–38, 1994.

[2] N. P. Smart, "Access control using pairing based cryptography,"in *The Cryptographers' Track at the RSA Conference - CT-RSA'03*,vol. 2612 of *LNCS*, pp. 111–121, 2003.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings: IEEE Symposium on Securityand Privacy (S & P'07)*, (Oakland, California, USA), pp. 321–34, IEEE, May 20-23 2007.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings: Advances in Cryptology - EUROCRYPT'05* (R. Cramer,ed.), vol. 3494 of *Lecture Notes in Computer Science*, (Aarhus,Denmark), pp. 457–473, Springer, May 22-26 2005.

[5] M. Chase, "Multi-authority attribute based encryption," in *Proceedings:Theory of Cryptography Conference-TCC'07* (S. P. Vadhan,ed.), vol. 4392 of *Lecture Notes in Computer Science*, (Amsterdam,The Netherlands), pp. 515–534, Springer, February 21-24 2007.

[6] S. M¨uller, S. Katzenbeisser, and C. Eckert, "Distributed attribute based encryption," in *Proceedings: Information Security and Cryptology-ICISC'08* (P. J. Lee and J. H. Cheon, eds.), vol. 5461of *Lecture Notes in Computer Science*, (Seoul, Korea), pp. 20–36, Springer, December 3-5 2008.

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multiauthority attribute based encryption without a central authority," in *Proceedings: International Conference on Cryptology in India-INDOCRYPT'08* (D. R. Chowdhury, V. Rijmen, and A. Das, eds.), vol. 5365 of *Lecture Notes in Computer Science*, (Kharagpur, India),pp. 426–436, Springer, December 14-17 2008.

[8] A. Lewko and B. Waters, "Decentralizing attribute - based encryption,"in *Proceedings: Advances in Cryptology-EUROCRYPT'11* (K. G. Paterson, ed.), vol. 6632 of *Lecture Notes in Computer Science*,(Tallinn, Estonia), pp. 568–588, Springer, May 15-19 2011.

[9] J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, "Multi-authority ciphertext-policy attribute-based encryption with accountability," in *Proceedings: ACM Symposium on Information, Computer and Communications Security-ASIACCS'11*, pp. 386–390, ACM, 2011.

[10] D. Boneh and M. K. Franklin, "Identity-based encryption from theweil pairing," in *Proceedings: Advances in Cryptology-CRYPTO'01*(J. Kilian, ed.), vol. 2139 of *Lecture Notes in Computer Science*, (SantaBarbara, California, USA), pp. 213–229, Springer, August 19-232001.

[11] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings: Advances in Cryptology - CRYPTO'84* (G. R. Blakley and D. Chaum, eds.), vol. 196 of *Lecture Notes inComputer Science*, (Santa Barbara, California, USA), pp. 47–53, Springer, August 19-22 1985.

[12] C. Gentry, “Practical identity-based encryption without random oracles,” in *Proceedings: Advances in Cryptology-EUROCRYPT’06*(S. Vaudenay, ed.), vol. 4004 of *Lecture Notes in Computer Science*,(St. Petersburg, Russia), pp. 445–464, Springer, May 28-June 12006.

[13] B. Waters, “Efficient identity-based encryption without random oracles,” in *Proceedings: Advances in Cryptology-EUROCRYPT’05*(R. Cramer, ed.), vol. 3494 of *Lecture Notes in Computer Science*,(Aarhus, Denmark), pp. 114–127, Springer, May 22-26 2005.

[14] D. Boneh and X. Boyen, “Efficient selective-id secure identity based encryption without random oracles,” in *Proceedings: Advances in Cryptology-EUROCRYP’04* (C. Cachin and J. Camenisch,eds.), vol. 3027 of *Lecture Notes in Computer Science*, (Interlaken,Switzerland), pp. 223–238, Springer, May 2-6 2004.

[15] M. Chase and S. S. Chow, “Improving privacy and security inmulti-authority attribute-based encryption,” in *Proceedings: ACM Conference on Computer and Communications Security-CCS’09* (E. Al-Shaer, S. Jha, and A. D. Keromytis, eds.), (Chicago, Illinois, USA),pp. 121–130, ACM, November 9-13 2009.

[16] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in *Procedings: ACM Conference on Computer and CommunicationsSecurity-CCS’06* (A. Juels, R. N. Wright, and S. D. C. di Vimercati,eds.), (Alexandria, VA, USA), pp. 89–98, ACM, October 30-November 3 2006.

