Secure Information Sharing using Attribute Based Encryption

**ABSTRACT**

Attribute Based Encryption (ABE) is a novel technology that supports fine grained access control cryptographically. This paper proposes ABE as a part of the solution to secure information sharing in multinational operations. ABE is introduced and a way of applying it to secure information sharing is presented. The ABE-based solution is compared against the requirements for secure information sharing in multinational operations and it is found to present a number of advantages compared to other solutions including improved resilience to malware and tolerance of server failures.

**EXISTING SYSTEM**

A weakness with access control lists is that there is no cryptography, so there is a large attack surface for malware to exploit.RM uses cryptography and therefore avoids the access control list vulnerability, but depends upon access to a server each time material is first decrypted by each user. This has increased server workloads and vulnerabilities compared to ABE but has the benefit of fast revocation. Solutions to ABE revocation .But RM has an advantage in that it can prevent revoked users from decrypting already encrypted material without re-encryption. However many threats commence prior to revocation so with both technologies a major part of the solution lies in monitoring access patterns to encrypted material.

**PROPOSED SYSTEM**

ABE has been proposed for secure information sharing in applications ranging from storage in clouds to social networks. This paper proposes ABE as a part of the solution to secure information sharing in collaborative environments such as multinational operations. It gives an overview of the information sharing requirements, which introduces ABE, and shows how ABE could be applied to collaborative environments.

**MODULE DESCRIPTION**:

1. **Attribute-based Encryption**
2. **Multinational Information Sharing**
3. **Secure Collaboration Based on ABE**

**1. Attribute Based Encryption**

ABE is a cryptographic technology where encryption and keys are expressed in terms of attributes. There are two main methods of ABE according to how attributes and policies are applied. In this paper the focus is upon Key Policy ABE where policy is stored in keys; readers are referred to for information about the alternative called Ciphertext Policy ABE. When a file is encrypted it is assigned attributes which are arbitrary pieces of text that are meaningful within the policies of the organisation that encrypts the file, e.g. this paper could be assigned the attributes. ABE is a form of public key cryptography where separate keys are used for encryption and decryption.

**2. Multinational Information Sharing**

The benefits of an information sharing infrastructure include reduced delay and the opportunity to optimise security through carefully planned measures related to the expected threats. Interoperability is fundamental to information sharing. Nations may adopt information sharing using different approaches at different times, so it must be possible to modify information formats and security approaches at national interfaces. Flexibility in information sharing policy is necessary so that it can reflect both differing national requirements and the complexities of the information held.

**3. Secure Collaboration Based on ABE**

A global ABE system would have the cryptographic power to share files securely. However it would be difficult to deploy the scheme incrementally and moreover nations may be unwilling to trust a global key authority. Nations may choose to carry out further checks of incoming material in ingress dataguards. The transmissions from nation 1 to nations 2 and 3 are not ABE encrypted so it is important that some other means of communications confidentiality is deployed between the nations. There is a second scenario for file sharing between ABE nations where the material is not re-encrypted and instead keys are delegated.

**System Configuration:-**

**H/W System Configuration:-**

**Processor - Pentium –III**

Speed - 1.1 GHz

RAM - 256 MB (min)

Hard Disk - 20 GB

Floppy Drive - 1.44 MB

Key Board - Standard Windows Keyboard

Mouse - Two or Three Button Mouse

Monitor - SVGA

**S/W System Configuration:-**

Operating System : Windows95/98/2000/XP

Application Server : Tomcat5.0/6.X

Front End : HTML, Java, Jsp

Scripts : JavaScript.

Server side Script : Java Server Pages.

Database : My sql

Database Connectivity : JDBC.

**CONCLUSION**

ABE is a recent cryptographic development in an area where further innovation is expected. Examples, not discussed in this paper, include Predicate Encryption where the attributes are encrypted and Functional Encryption allowing greater generality in attributes/policies . In the longer term Functional Encryption could lead to the prospect of cryptographically controlled redaction.

ABE may be used by individual nations to support secure information sharing with both ABE adopters and legacy nations. The benefits of this approach are improved security within domains, mainly by minimising the attack surface for insiders and malware, and also by minimising dependency upon critical cryptographic servers. ABE reduces the impact of risks associated with errors in and compromise of egress dataguards, and scenarios have been identified where ABE reduces the need to otherwise secure communications channels. These benefits could lead to improved security and/or cost savings.