Proposed Identity and Access Management in Future Internet (IAMFI): A Behavioral Modeling Approach

Nancy Ambritta P., Poonam N. Railkar and Parikshit N. Mahalle

Department of Computer Engineering, Smt. Kashibai Navale College of Engineering,University of Pune, Pune, India-411041
Email id: nancy.ambritta@yahoo.com, poonamrailkar@gmail.com, aalborg.pnm@gmail.com

Received: April 11, 2014; Accepted: June 19, 2014
Publication: July, 2014

Abstract

The Future Internet (FI) sees the world of objects completely connected over the Internet all the time. It is like opening one's network doors of say home, companies and organizations to the world where it increases efficiency but at any case should not compromise security by exposing sensitive information, presenting tremendous challenge towards access control and identity management in FI. A well-managed identity management system should provide necessary tools for controlling user access and access to critical information. A fitting example will be the IoT (Internet of Things) where every object will be smart and will take advantage of cloud for storage and processing power.

In this paper we provide an introduction to Identity and access management in FI followed by a simplified architecture of the FI and its components. We then proceed by providing a short description about the frequent threats to data stored on cloud along with possible mitigation techniques to the threats.We also provide a comparative study of existing work on access control and propose a method to overcome the limitation of the existing techniques where sensitive organizational information (access policy) is exposed to the cloud. We address this issue in IAMFI by extending the Attribute based encryption

Journal of ICT, Vol. 2_1, 1–36.
doi: 10.13052/jicts2245-800X.211

technique and allowing users to have control over their attribute exposure at the time of requesting access. We also provide a mechanism in IAMFI for distributed attribute and key management for various users thereby reducing the overhead at a single site.

Keywords: IAMFI, Future Internet, Access Control, Identity, Cloud, Attribute-based encryption, Attack Model.

1 Introduction

The Invention of internet is one of the most important discoveries of mankind. It is a network of networks that connects millions of networks through electronic, wireless and optical networking technologies [1]. Billions of people use Internet and it impacts them in almost every aspect of their lives. We cannot imagine a life without Internet today. The original internet architecture was not designed to meet the current demands and the continuous strain in terms of sophisticated threats, performance, reliability and scalability. This has made the research and design of future internet architecture more critical and more relevant than ever before.

Future Internet has never been a single monolithic or single improvement area over the current internet architecture, whereas it is a generic terminology used for the various research activities on internet architecture to address the issues mentioned above and also take into account of bigger picture of the issues [social, ethical, economical] when society is interacting with internet.[2]. Going by the current trends, one example would be moving towards a phase where everything we interact will be connected to the internet. A Fitting example would be Internet of Things where every object will be smart even though it doesn't need to have the necessary processing power as it will take advantage of cloud computing for processing data. In future, not only the phones and computers will be connected whereas every object we use will be connected.

In general, it's like opening one's network doors of say home, companies, and organizations to the world where it increases efficiency but at any case should not compromise security by exposing sensitive information. It presents tremendous challenges towards the access control and identity management in future internet. Hence Identity and access management in future internet needs to be more resilient to attacks, scalable, should maintain privacy and integrity but also on the same hand should have traceability. A well-managed

Identity management system should provide necessary tools and technology for controlling user access and access to critical information.

Thus, we can define Future Internet as a pervasive network of devices connected over the internet that are uniquely identified by their ID's , and interacting with the environment via associated sensors, communicates with the cloud and customizes the environment according to the person interacting with it based on his/her attributes. The devices are hence made smarter due to the enhanced computing power (in terms of processing and storage power) provided by the cloud. The architecture of Future Internet (FI) provided in section 2 provides a detailed explanation on the definition provided above.

A. Existing Methods and Our Contribution

Several access control schemes have been proposed such as Dynamic broadcast encryption technique [8] and role based access control (RBAC) [12] have addressed various issues namely traceability via trusted third party (TTP) and anonymity. Attribute based encryption [13, 14] has provided an effective mechanism to address the scalability and anonymity issues that has been adopted as a basis in [10, 11]. In addition many mechanisms have been proposed to enhance security mechanism against attacks such as replay attacks by leveraging the usage of timestamps [9]. However, the existing methods work upon the assumption that the cloud is honest (trusted) but curious, which is not an ideal case as the cloud operated by the cloud service provider (CSP) may lie outside the trusted domain of the concerned organization, thereby exposing the access policy to the cloud in order to make decisions upon providing access to requested users which paves a possible way for collusion attack (cloud colludes with an attacker and relaxes the policy providing illegal access to attacker).

Hence this paper adopts the attribute based encryption technique as a basis for the proposal. Further this method is enhanced by providing a means of hiding the access policy from the cloud while still leveraging the high computing power (in terms of processing and storage) of the cloud. In our method we expose the access structure only to the cloud that is sufficient for the cloud to perform its designated task and hide the access policy from the cloud. Further, user privacy is incorporated by allowing a user controlled environment where user decides upon how his/her attributes are to be exposed or portrayed for authentication during access control procedures (explained in section 2.2, Identity Portrayal). Finally a proposal about the idea of the TTP (trusted third party) that has the identity of the participating entities

(CSP and devices) registered with it that helps is establishing a mutual trust and traceability of activities during situations of misuse/fraudulence. Replay attacks are addressed by the usage of timestamps and DoS attack is to be taken care of by establishing a TTP (trusted third party) that helps to track down the activities of the cloud and also by using the session establishment technique.

B. Organization of the Paper

This paper has been organized as follows. In section 2 a basic architecture of the FI (Future Internet) which supports the definition of FI provided in section 1. Section 3 introduces us to the basics of Identity and access management and provides an explanation about Identity portrayal which is the basic idea behind the mechanism that is followed in our paper that allows users to control the exposure of his/her attributes during the access control process. Section 4 provides a high level depiction of where access control finds its place in FI that is explained in detail with a sequence diagram. Section 5 discusses in brief the existing works and also provides an evaluation of the work. Section 6 discusses the various attacks and threats that were considered during the evaluation of related work and also provide possible mitigation techniques that can be followed to address these issues. Section 7 finally proposes an architecture that addresses our major concern of collusion attack by incorporating the idea of separation access policy and access structure and also enhancing user privacy by providing a user controlled environment where user controls the portrayal of his attributes as explained in the scenario provided under section 3.2.

2 Architecture of Future Internet

This section provides one perspective about the organization of future internet. It also provides an insight into the components that find their place in the Future Internet (FI) and their appropriate roles. The basic architecture of the future internet is shown in Figure 1. It has at its lowest layer (i.e., layer 1) the devices (every possible real time object) such as smart phones, smart TV's etc. along with their unique identities (RFID, IPV6, biometrics etc.) to be able to stay connected and communicate to the network. The devices also have their connected sensors that help in the reception of stimuli from external physical environment.

The next layer (i.e., layer 2) is the access network layer that consists of access points including 3G, Wi-Fi and sensory networks (such as WSN gateways for the sensors) that helps to connect the devices over the internet.

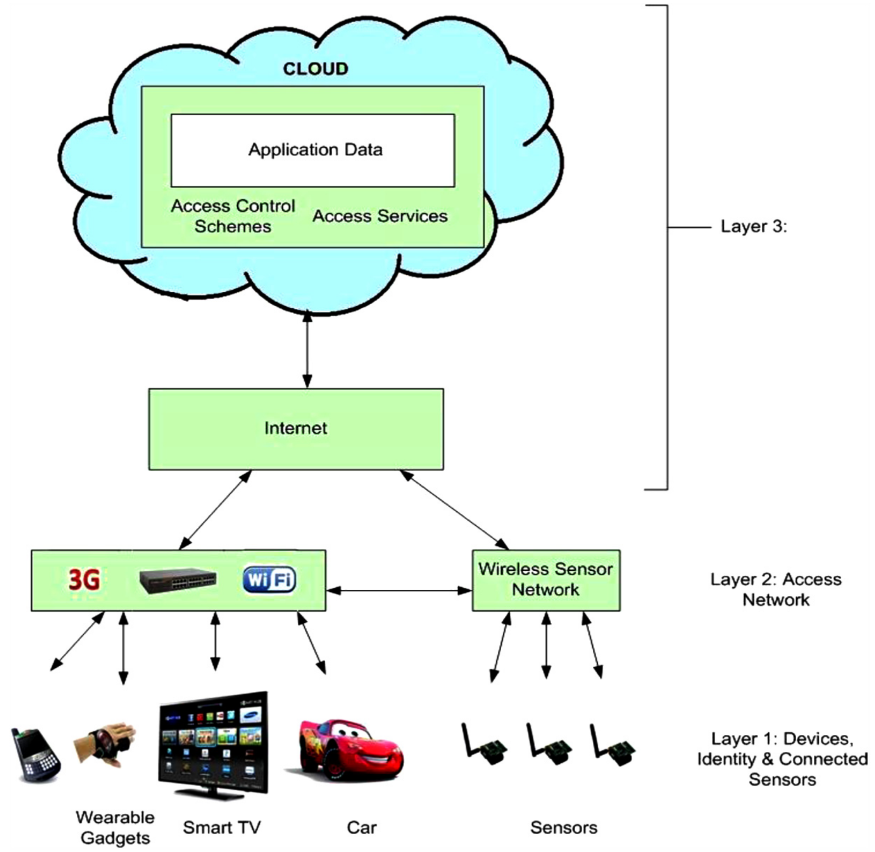


Figure 1 Architecture of future internet

The next layer (i.e., layer 3) consists of the internet that serves as a communication layer over which the cloud operates. The cloud is responsible for storage of data that are collected by the devices and associated sensors. The data for decision making related to access to specific applications based upon the stored (and received information from sensors) information also resides in the cloud. All the huge power consuming computations relating access management are moved on to the cloud which helps arrive at efficient decisions concerned with access control.

The cloud could be a private cloud (corporate wide) to store organizational private data or a public cloud that stores data that is mostly in the encrypted format and access control service data. The cloud here is looked upon as storage as a service and also in most cases serves as a medium to perform tasks that are heavily resource consuming. It is also looked upon to follow the access restriction rules and function as management authority that regulates access to the sensitive data stored by the customers.

Hence, from the above discussion we see that the key responsibility of protecting the data by regulating access (access control) to the stored data is borne by the cloud thereby leading to the point wherein the mechanism of regulating access (access policy) has to be implanted with a strong foundation thereby enhancing the protection mechanism.

3 Identity and Access Management in Future internet (IAMFI)

Identity and access management plays a major role in establishing security in FI. This section serves as an introductory explanation to the reader making him understand what Identity and access management is. Also a sub-section for Identity portrayal has been introduced because in section 7 an idea has been proposed wherein, during the phase when a request to access data on the cloud is sent to the cloud via a device that has the user attributes captured in it, an additional level of user privacy and security is provided where the user is given the flexibility to manage the exposure of his attributes to the cloud. For example, this user privacy establishes its importance in situations where certain social networking sites and email service providers try to access personal information in order to customize advertisements and contents for the appropriate users, which might be offensive for a few users who value their privacy [3].

3.1 Identity Management

Declaring the existence of a user to a system probably in the form of logon ID or username is Identification. Since user IDs are unique and not shared amongst users identification makes it possible to hold users accountable for the actions on the system. The users IDs are subjected to various policies (Eg. ID to meet minimum number of characters. IDs not to reflect usernames etc.) in order to enhance security.

Authentication is a verification done on the users' claimed identity and is implemented via passwords upon logon. Authentication falls under the following three types:

- Type 1: Something you know (e.g., personal ID number)
- Type 2: Something you have (e.g., ATM card)
- Type 3: Something you are (e.g., fingerprints)

Now, with Future Internet when every possible thing or object that is going to be connected to the Internet, identifying these items/object uniquely has to be done in an efficient and effective manner. The IPV6 addressing mechanism and other related RFID identifiers could be possible ways of providing unique ID's to the objects thereby taking care of the exhaustion of ID's available for identification currently in the IPV4 addressing. The existence of the devices and their associated sensors can be identified by means of the identification techniques such as IPV6, RFID, barcode and biometrics to identify and authenticate human beings. Also, Host Identity Protocol (HIP) is another method for assigning identities that includes security as an inherent part of the design and it separates host's identity from the topological location which provides a key basis for mobility of devices in future internet. It provides as a means of addressing the DoS (Denial Of Service) attack to a certain extent. Tools for managing the identities basically run as applications on dedicated servers or on the cloud. These interconnected objects are going to continually collect data, analyse them and use it in various decision making and management activities. Examples of things include people, all electronic devices (e.g. mobiles, smart TV's, food and even clothing).

3.2 Identity Portrayal

Identity management in FI not only concerns the assignment of unique identities to objects and managing their use in internet services, but also includes the management of presentation or portrayal of these identities online for communication. This portrayal of identity influences the enhancement of security and privacy to a greater extent. Management of Identity information by oneself helps to mitigate the threats posed to the access of data by the attackers [5].

The transformation of internet from an academic place to a public place of communication including e-commerce which involves business to business communication and also end users (customers) choices has led the world wide web to evolve into a place that allows exchange of information for everybody. Every user has his/her own profile that serves the purpose of identification. This profile is then used to portray the identity of users during information exchange or communication.

This self-portrayal of Identity follows that, in a communication session between two parties, the owner of identity or profile information can take control of exposing selected or all parts of his/her identity attributes for use in verification or processing by the other party. The attributes are then transmitted from the owner's site to the other party in a standard format. This selected and controlled revealing of identity attributes enhances privacy by preventing unnecessary or undesired processing of personal information.

To explain this, a simple but interesting real life example is shown in Figure 2 which helps us understand the self-portrayal of Identity and its associated privacy. In the figure, George, is a person from a village who is a Goldsmith by profession. He owns a jewellery and gift shop at the town where he sells his handmade products. In this scenario, George, his name is the core Identity by which he is universally identified. He has several other attributes that serves as an identity for him. However, George decides upon which attributes to expose to each of his different environments. For example, George is identified as George son of William along with his family details and personal home address by the people of his village (Persona 1). To the people of the town where John runs his business he does not expose his personal information but is identified with the attributes such as George the goldsmith, the quality of jewellery and gifts he sells, location of his shop and the shop name. In this way George keeps the exposure of his attributes by which he is identified under his control.

3.3 Access Control

Access control is the selective restriction based on certain rules. Access control helps to minimize access risk and fraudulent access to information Identification and authentication are the building blocks of access control systems.

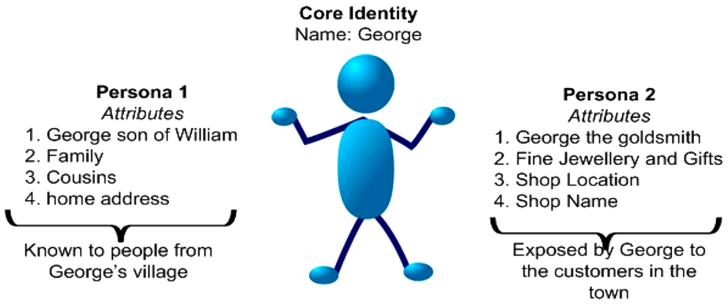


Figure 2 Identity portrayal

Access control belong to identity management by its very nature. Access control is required to preserve the integrity, confidentiality and availability of data over cloud (Future internet). Access control is implemented based upon the policies (high-level statements of management intent) that regulate the access of data and personnel who are authorized to receive the data.

There are a few things that must be considered when imparting access control mechanisms into systems such as

- Threats to the system (events that cause harm to the data)
- The system's vulnerability to the threats (lack of security mechanisms against threats) and
- The risk that might be materialized by the threats.

In the Future Internet, access control has to be implemented as a strong foundation at various interacting layers. At the core of the identity management for FI is the access control, wherein policies are defined that describe which devices and users are allowed to access data on the network and what tasks can be accomplished by the user. Users/customers can set up services and manage their hardware through the cloud access control. Threats coming from networks such as spoofing data should be safeguarded by using access control techniques.

Access control services and schemes (predefined rules and strategies set by data and application owners) are called by the applications and related stored data to decide upon authentication and provisioning of services to requested users who satisfy/dissatisfy the specified strategies.

3.4 Current Trends and Standardizations

In the Future Internet, apart from software based in IAM, the trend is moving towards biometrics and hardware re-inforced security. For example we already have digitally signed BIOS in the newer chipsets [6]. Another approach is going away from passwords entirely and moving the identity and access management in to the devices as passwords tends to be weak and people can't remember passwords for multiple sites [7]. Several attempts in developing an open standard for Identity Management is under work by organizations such as the Cloud Computing work group- Cloud/SOA-Security and architectures for Identity Management. Many security and privacy enhancing mechanisms for ubiquitous cooperation and interaction are being dealt with currently. Many areas supporting the existence of Future Internet and security thereby have been identified and Cloud computing is one such area which has hit its mainstream by recent releases of vendors. The ETSI Specification group has been working in order to develop a common view on Identity and access management in Future Internet, in terms of protocols and architectures relating to network of connected devices. In the event of such attempts of unification of diverse network topologies and multiple devices the FI architecture developed must deal with the identity and access management issues handily. The CSA projects funded under FP7 has jointly ventured into supporting the Standardization activities within the Future Internet Assembly (FIA) that covers the various domains including the security (including access management), internet of things and cloud computing.

4 A Vision of Access Control in Future Internet (FI)

This section provides a glimpse of the importance and place held by access control in FI. This section shows how the identity and access control mentioned in section 3 fits into the real life scenario of FI, where we have shown numerous devices and facilities (in Figure 3 and Figure 4) that are uniquely identified by assigned identities as objects. Access control explained in section 3 is found to have its place in FI where a user is provided restricted access (access control) to various facilities as in Figure 3 and also in Figure 4 where user controls the operations various devices (interaction between devices) within the house. These devices and facilities shown in Figure 3 and Figure 4 form the lowest layer (layer 1) depicted in Figure 1 under Section 2 (basic architecture

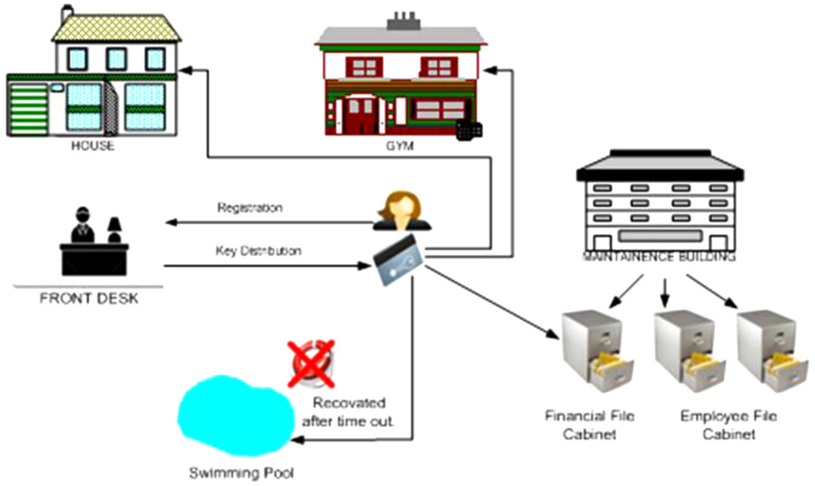


Figure 3 Motivation - building maintenance

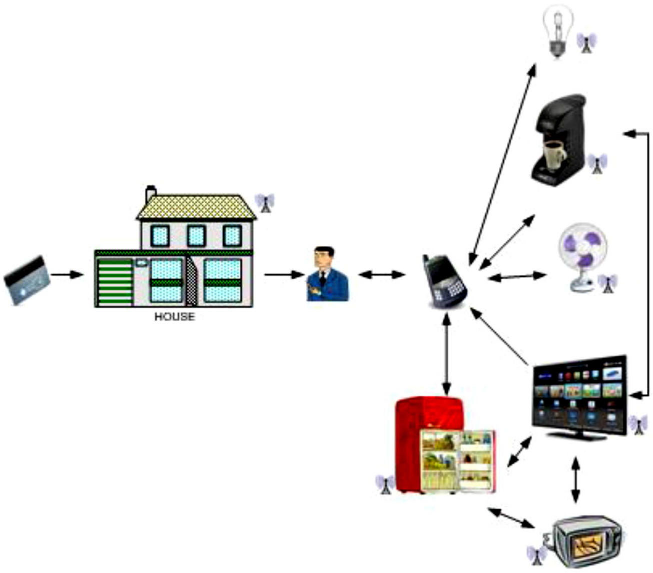


Figure 4 Motivation – device to device communication

of Future Internet). The motive of considering access control in FI (Future Internet) is explained in the following paragraph.

We are moving away from the traditional method of access control i.e., using usernames and passwords as passwords are weak and it is cumbersome to remember due to the transformation of communication methods between entities. Internet of Things is an aspect of Future Internet where numerous devices and sensors will be interacting with each other and the surrounding environment. Just by knowing the scale of this FI aspect the traditional methods cannot prove to handle the access and security issues effectively, thereby motivating us towards working upon the evolution of an access control mechanism that can be applied to the FI scale.

4.1 User Centric Vision

In a buildings' maintenance and operation scenario, there could be a lot of facilities like the swimming pool, library, the maintenance building with houses a lot of sensitive filling cabinets (e.g. financial, corporate, etc.) and a bunch of different homes/apartments. This scenario is depicted in Figure 3 wherein a visualization of one of the possible ways of fitting access control to regulate access to resources is portrayed.

The access and security issues that we have to address may include similar aspects as follows:

- If somebody is employed over the pool for a couple of months (say only for summer) then we need to make sure that they do not have access to the pool after their employment ends.
- Any user who has been given access to the maintenance building then it is very certain that we must take care to see that people are not accessing the information that they are not entitled to.

In order to address these issues we could get rid of the all the keys and provide a key card to access all the facilities and buildings.

Doing so we could ensure that at the end of a user's employment with the pool the key card would automatically revoke access to the pool. This is basically done based upon a role or attributes of the users, meaning that if any user has been given access to the maintenance building and if they were part of the financial group/role then she would be able to access the financial filling cabinet while the others who do not satisfy the role/attribute would be denied access.

The access cards provide facility to keep track of all of the different facilities that users can access at any given point of time. It is also possible to report/track on the different activities (access to facilities). Further, the users contact a help desk in order to request for keys in order to be able to access the facilities across the community. It is also possible to track the workflow involved in granting the access.

4.2 Extended Device to Device Communication – Vision of Future Internet Scenario

Apart from user centred access. Device to device communication is another phenomenon that is addressed in the FI. This device to device communication which forms the essence of Future Internet and consequently invoking a strong need for access control that serves the purpose of addressing security issues relating to Future Internet (FI) is shown in Figure 4 as an extension to the scenario in Figure 3.

Moving on to elaborate upon the above scenario, taking into consideration the possible activities that could take place inside the house, once the user has identified himself as the authorized user he gains access to use the facilities inside the house and also control them.

For example, in Figure 4, the user can turn on/off lights and other electronic equipment via the identity established through his smart phone. A fridge can further communicate to the smart TV that serves as a display for the user to view the contents present in the fridge. The fridge can also communicate with the smart TV to display the recipes that could be cooked with the available grocery and also display a manual for the recipes suggested. The TV in turn could communicate to the microwave oven by providing the oven with the manual for the recipe that has been chosen by the user and start the cooking as specified by the manual. The fan with the associated sensor for the temperature of the room can sense the environment and work accordingly.

A visitor would be allowed to access the house and its facilities by sending him a one-time access code that they could use to get initial access to the door (opening door) by operating it over their smart phones. Other facilities such as access to light up specific rooms, access the microwave oven and TV could be granted upon approval by the current owners/occupants of the house.

4.3 Sequence Diagram Showing the Flow of Actions for Access Control in Distributed Environment

The general sequence of actions that takes place during access control in shown in Figure 5. Initially the user registers himself with a key distribution centre and obtains keys/Unique ID. Here user and devices have been separated because in ideal cases there are situations when the user needs to first identify himself as the authorised users to gain access to the devices and perform further operations using them.

The user then sends his identification information to the device as a request to gain access to the device. The devices have with them associated ID's that identify them uniquely as with that of the users and also has associated sensors that help to sense and gather information related to the environment or other user related information/activities.

The devices upon receiving the access request from the user might not have the capability to verify the validity of the user and hence sends the received information over to the cloud where the user related information and access policy that governs the approval of access is stored. The cloud then verifies the details received and based upon the validation sends a reply to the device whether to permit access or deny access. If the user has been authenticated as a valid user by the cloud the device in turn authenticates and allows access to the user. The user then uses the device to perform further actions.

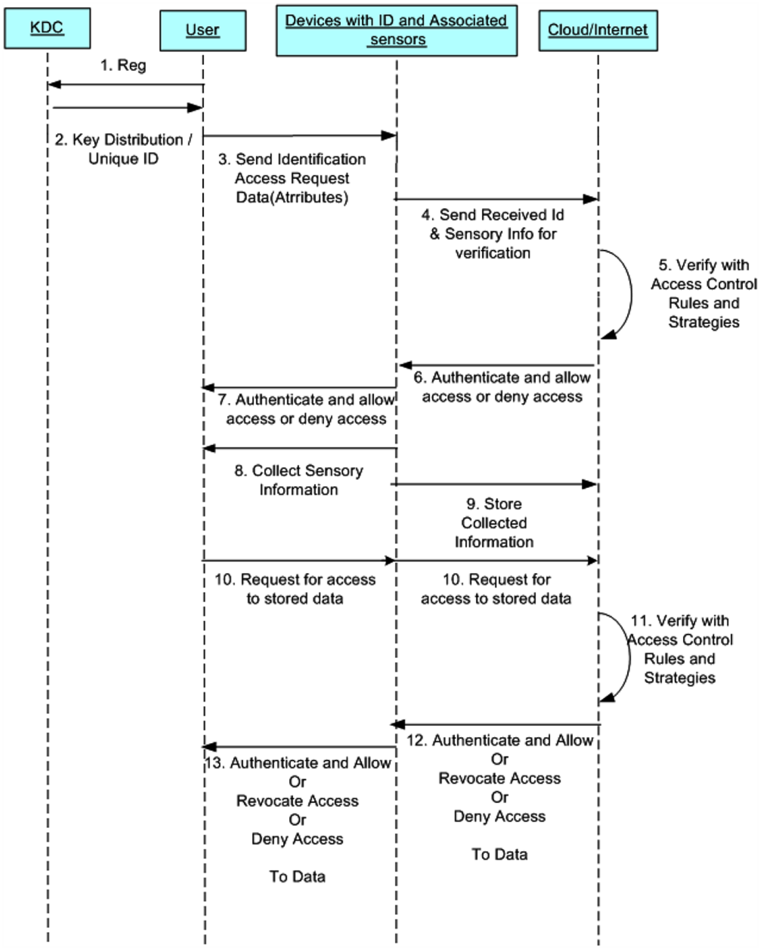

KDC
User
Devices with ID and Associated sensors
Cloud/Internet
1. Reg
2. Key Distribution / Unique ID
3. Send Identification Access Request Data(Atrributes)
4. Send Received Id & Sensory Info for verification
5. Verify with Access Control Rules and Strategies
6. Authenticate and allow access or deny access
7. Authenticate and allow access or deny access
8. Collect Sensory Information
9. Store Collected Information
10. Request for access to stored data
10. Request for access to stored data
11. Verify with Access Control Rules and Strategies
12. Authenticate and Allow Or Revocate Access Or Deny Access To Data
13. Authenticate and Allow Or Revocate Access Or Deny Access To Data

Figure 5 Sequence diagram showing the flow of actions for action control in distributed environment

The user then uses the device to collect information and store the information on the cloud. He also specifies the access policy that tells the cloud about the users who are authorised to access the data based upon which the cloud accepts or rejects the request to access from users. When a second user requests for access to the stored data on the cloud by providing his identity information with the request, the identity is verified by the cloud against the access policy that stands guard for the stored data, and access is provided to those users whose attributes match the access policy or denied access otherwise.

5 Related Works and Evaluation

Several access control mechanisms have been introduced in order to provide effective means of providing access to stored data over the cloud. In [8], the author has proposed an efficient solution for supporting multiple authorized users to read the outsourced data as well as modify the data over the cloud. The author has established the mechanism of maintaining the anonymity of the users who share the data over the cloud by leveraging group signature and dynamic broadcast encryption technique. Adding and revoking users has also been addressed efficiently. However, the technique has adopted a centralized approach to distribution of keys which solely depends upon the group manager which is not an ideal case. Also the existence of a predefined group might not always be possible when cloud computing is under consideration. In [9], the author has adopted the Attribute based signature and attribute based encryption technique, wherein anonymity of the data owner from other users has been preserved, however the traceability has also been provided by the trusted third party under the situations of forged/illegal activity. It also addresses the situation where not only the owner of the data makes changes to the data over cloud but also the authorized users are allowed to update the data and upload it to the cloud. The technique has adopted a decentralized approach towards key distribution.

In [10], the author has adopted the Key rotation and broadcast encryption technique. Due to the existence of a trusted third party between the cloud and the organization there is an establishment of mutual trust between the two parties, which addresses the risks of collusion and forgery from both sides. Also, the trusted third party provides traceability of any illegal activities. The broadcast encryption technique has made the scalability aspect efficient. However, anonymity of users/data owners which is required in certain situations has not been considered in this technique. The technique has also not addressed the possibility of replay attacks that would support forged activity. The user revocation is partial wherein there is trade-off between the computational cost of re-encryption (minimized-lazy revocation) and the availability of data for revoked users i.e. the revoked users can gain access only to the stale data (not updated versions). The mechanism has guided the possibility in which a single owner updates the data and uploads it to cloud while other users can only read the data upon decryption. Multiple authorized users who would find a need to update the data over the cloud is not addressed.

In [11], the author has adopted the ACV-BGKM (Access control vector broadcast group key management) technique which follows the idea of sharing some secrets to users based on the identity attributes they have and later allow them to derive actual symmetric keys based on their secrets and some public information. Thus the adding/revoking users or updating access policies could be performed efficiently. However, the provision to trace any malicious activity by the cloud or the users has not been addressed. In [12], the author has adopted the Role Based Access control Model (RBAC) model and the role based encryption cryptographic technique. The introduction of a separate private cloud to hold sensitive information and usage of public cloud only to share data to users outside the organization has provided a means to prevent external collusion attacks. Also, the organization's sensitive information (eg. the role structure etc.) is hidden from the distrusted public cloud. However, the mechanism poses a difficulty to scalability due to a possibility of role explosion. Also, the mechanism has taken a centralized approach wherein a user has to register to the organizations authority to obtain keys to access and decrypt the required data. The mechanism has guided the possibility in which a single owner updates the data and uploads it to cloud while other users can only read the data upon decryption.

In [13], the author has proposed a new multi-authority CP-ABE (cipher text policy attribute based encryption) technique to efficiently handle adding and revoking users in an environment that needs to support rights to all authorized users to read as well as update his/her part of data over the cloud. It has adopted a decentralized approach towards key management. However, anonymity of users/data owners which is required in certain situations has not been considered in this technique. In [14], A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in cloud Computing, the author has proposed a hierarchical CP-ABE by adopting the traditional CP-ABE thereby inheriting its security schemes enhanced with a hierarchical set of users in order to overcome the limitation of flexibility in implementing complex access control policies. The access control technique has realised a scalable, flexible and fine-grained access control over the data stored on cloud. It has also dealt with user revocation efficiently by employing multiple value assignments for access expiration time. However situations at which a user/owner of the shared data would not like his/her identity to be revealed to other users in the group have not been considered.

All of the above techniques except [12] have not considered the limitation wherein the organizational sensitive information (access policy and attributes) are exposed to the cloud. However in [10], the technique emphasizes that the organization has a private cloud to hold sensitive data and a public cloud to store data, which does not solve the sole purpose of relieving the organization from taking care of availability and maintenance of resources. Another limitation is that all the above techniques have not considered the situations when a CSP could actually refrain from providing services to the authorized users, deletion of data for accommodating space etc. (DoS and mutual trust). It has also not considered the situation where there might be certain situations when authenticated users might also want to update the data and move the copy over the cloud. Table 1 and Table 2 summarize the above discussion and give a comparison between the various key attributes that are to be considered while performing access control to stored data on the cloud. In Table 1 provides a comparison between the major attributes that come into picture when access control is considered in cloud and Table 2 compares the attributes related to key management such as encryption computation cost for the keys and data generated as well as the provision of updating data to users (number of users allowed to read and write) and also the revocation of users and its associated feasibility in key management. In Table 2 the abbreviations in the last column are M-multiple, R-read, W-write and 1-Single.

6 Attack Modelling

This section provides a short description of the attacks such as DoS (Denail of Service), Collusion and Replay attacks. It provides an insight into the possible threats that might cause the system to experience the associated attacks. A modelling of the attacks is depicted via sequence diagrams and mitigation techniques that address such attacks are also explained. This modelling provides a good understanding towards the threats posed to a system and the security measures to be taken when expecting their resultant impact as attacks to the system.

6.1 DoS (Denial of Service) Attack

Denial of service is an attack on a cloud service attempting to indefinitely or temporarily stop the cloud services to the intended or authorized users. Cloud ignoring or losing the updated data by users and hiding loss of data can also be considered as DoS attack, as the cloud is in fact not providing the required service to the user.

Table 1 Comparison chart of related work major attributes

Paper No	Attack Resistance			Anonimity	Traccability	Mutual Trust	Fine Grained	Scalability	key Distribution	Confidentiality of Access Policy and Attributes
	DOS	**Replay**	**Collusion**							
5	No	Not efficient	Yes, but collusion between cloud+revoked users and data+authorized users agains cloud not addressed	Yes	Yes-Group manger	No cloud accountability	Yes	More efficient	Centralized	Access policy and attributes known to cloud
6	No	Efficient	Yes, but collusion between cloud+revoked users and data+authorized users agains cloud not addressed	Yes	Yes-trusted third party(only for users not cloud)	No cloud accountability	Yes	Yes, but incurs more computational cost	Decentralized	Access policy and attributes known to cloud
7	Yes	No	Yes (due to trusted third party traceablity ob both sides)	No	Yes-trusted third party	Accountabilit y from both sides	Yes	More efficient	Centralized	Access policy and attributes known to cloud

8	No	Yes	Yes, but collusion between cloud+revoked users and data+authorized users agains cloud not addressed	Yes	Not addresed	No cloud account-ability	Yes	More efficient	Decentralized (keys computed at time of decryption)	Access policy and attributes known to cloud
9	Not addressed	No	Yes (cloud cannot collude with revocated users)	No	Yes	No cloud account-ability	No	Not efficient due to possibility of role explosion	Centralized	Organisation's sensitive structure information (rolcs etc.,) are hidden fromthe cloud
10	No	No	Yes, but collusion between cloud+revoked users and data+authorized users agains cloud not addressed	No	Yes	No cloud account-ability	Yes	Yes	Decentralized	Access policy and attributes known to cloud
11	No	Yes (expirati on time for small window of vulneribility)	Not addressed	No	Yes	No cloud account-ability	Yes	More Efficient	Centralized	Access policy and attributes known to cloud

Table 2 Comparison chart of related work (key management attributes)

Paper No	Encryption Computation Cost	User Revocation	R/W Access
5	Independent of no of revoked users	Yes, but requires multiple encryted copies of same data file	M-R-M-W
6	Most expensive operations moved to cloud	Yes, but requires multiple encryted copies of same data file	M-R-M-W
7	Cost of reencrytion minimized (lazy revocation)	Partial-Lazy revocation trade off	1-W-M-R
8	Minimized	Yes	1-W-M-R
9	Minimized	Yes, but requires multiple encryted copies of same data file	1-W-M-R
10	Minimized computational cost as compared to the traditional CP-ABE (ciphertext attribute based encryption)	Yes by attribute authority	M-R-M-W
11	Minimized when compare to traditional ABE	Yes, but requires multiple encryted copies of same data file	1-W-M-R

6.1.1 Threats leading to denial of service

- Improper Design Techniques of Cloud. Where the cloud doesn't foresee the resource required for the user. In case of less storage space the cloud either deletes the contents or does not allow the updates.
- Typically an external attacker would use SQL Injection, Regular Expression Parsing, Buffer Overflow, Unexpected Exceptions and excessively large file uploading by attacker.

Overwriting of old data(knowingly/unknowingly) with new data(probably data belonging to another customer) can be considered as an indirect deletion of old data. Thereby, leading to the denial of servicing request for old data that resided at the cloud prior to overwriting. Hence, there is always a possibility of cloud deleting data knowingly or unknowingly and it is therefore a valid assumption.

On August 8, 2008 a 45% of customers lost their data from an online storage company Linkup and it was shutdown. There was finger pointing between it and another company Nirvanix on which Linkup had relied upon [15]. Secondly forensics on cloud is not yet evolved to imply cloud legally that

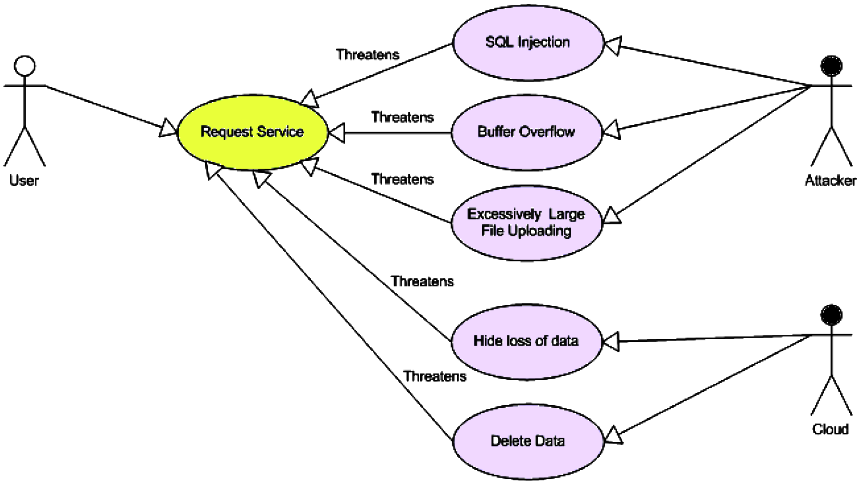


Figure 6 Mis-use case diagram depicting dos attack

cloud has accidentally or due to inefficient infrastructure design had caused data loss by removing, overwriting existing data. [16].

The Mis-Use Case depicting a typical scenario where an attacker uses the cloud system vulnerabilities to deny a legitimate user access to the cloud is shown in Figure 6. Here, a legitimate user requests for a service from the Cloud, meanwhile an attacker performs undesirable activities such as SQL injection, buffer overflow, or exclusively large file uploading that bombards the communication channel of the CSP (Cloud service provider) and thereby poses a threat to the responsive action of the CSP in servicing the request posed by the legitimate user. Also, activities such as hiding any loss of data or deliberate deletion of data by the cloud, in the former case to maintain reputation and in the latter case to make space for more customers poses a threat to the request of data posed by the user. In either case the cloud refrains from providing the requested service to the legitimate user which is denial of service.

6.1.2 DoS (denial of sevice) attack modelling

The sequence of actions depicting the DoS attack is shown in Figure 7 and Figure 8. In Figure 7, the owner/device sends his relevant information to the cloud as proof of identity and upon verification is given authorized access to store encrypted data along with the access policy on the cloud. When a second legitimate and authorized user/device requests access to the stored data, the

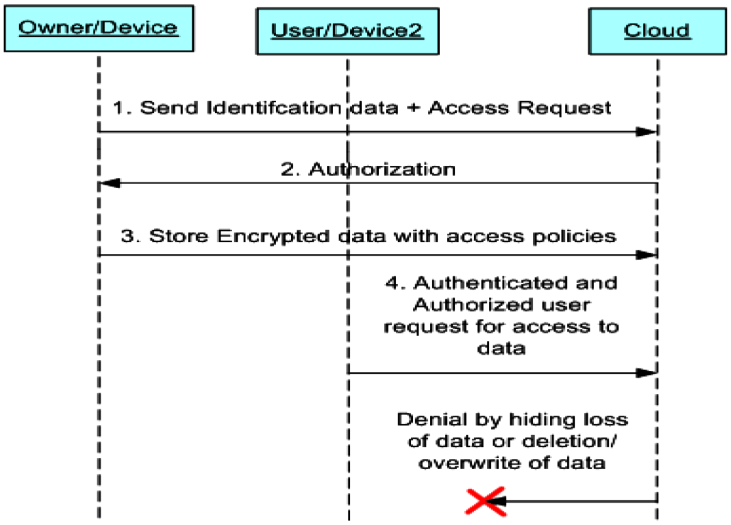

Owner/Device
User/Device2
Cloud
1. Send Identifcation data + Access Request
2. Authorization
3. Store Encrypted data with access policies
4. Authenticated and Authorized user request for access to data
Denial by hiding loss of data or deletion/ overwrite of data

Figure 7 Sequence diagram depicting DoS by cloud

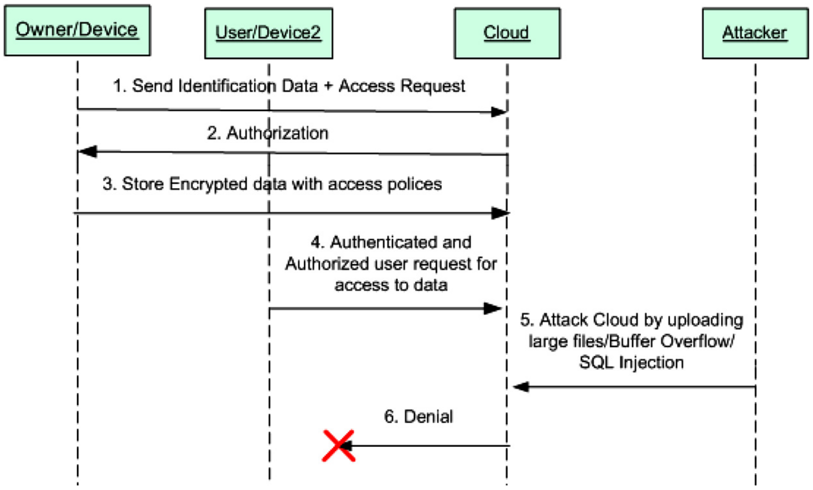

Owner/Device
User/Device2
Cloud
Attacker
1. Send Identification Data + Access Request
2. Authorization
3. Store Encrypted data with access polices
4. Authenticated and Authorized user request for access to data
5. Attack Cloud by uploading large files/Buffer Overflow/ SQL Injection
6. Denial

Figure 8 Sequence diagram depicting DoS by attacker

cloud refuses to provide the service. The reason for the denial could be the result of unacceptable activities such as loss of data due to certain internal reasons or deliberate deletion of data by the cloud. Additionally the cloud might as well claim that the data never resided with him.

In Figure 8, the owner/device sends his relevant information to the cloud as proof of identity and upon verification is given authorized access to store encrypted data along with the access policy on the cloud. When a second user/device is a legitimate and authorized user requests access to the stored data the cloud refuses to provide the service due to unacceptable activities performed by the attacker such as SQL injection, buffer overflow and uploading of large files.

6.1.3 DoS mitigation techniques:

- TTP (Trusted Third Party) to Monitor the activities of participants (Cloud and the users)
- Installation of monitoring s/w tools that identifies DoS patterns and takes steps accordingly.
- Cloud Design has to be validated by TTP for reliable storage and operational failures so that hiding loss of data and updates to data can be monitored. The Cloud has to be built with secured software interfaces & APIs so that the attacker doesn't take advantage of the cloud's vulnerabilities and stun the system functionality.

6.2 Collusion Attack

In Collusion Attack, two or more participants join hands in order to develop privileges that satisfy the required access policies that stand guard for the protected data. In the mis-use case diagram below both cloud and the malicious user collude to threaten user's access policy and authorization info.

6.2.1 Threats leading to collusion attack:

- Malicious Insider and untrusted cloud: Malicious Insider can join hands with cloud in order to gain access over the sensitive information. The cloud having known the access policy and being trusted to provide access to users relaxes the policy to allow access to malicious insiders with insufficient authentication information.
- External Attackers and untrusted cloud: Malicious external users gain unauthorized access to user's account information and manipulate the data. The Cloud Service Provider partners with this user knowingly or unknowingly to sabotage confidential information.

The mis-use case diagram in Figure 9, shows the possible activities of the malicious user and its collusion with the cloud to compromise on access rules

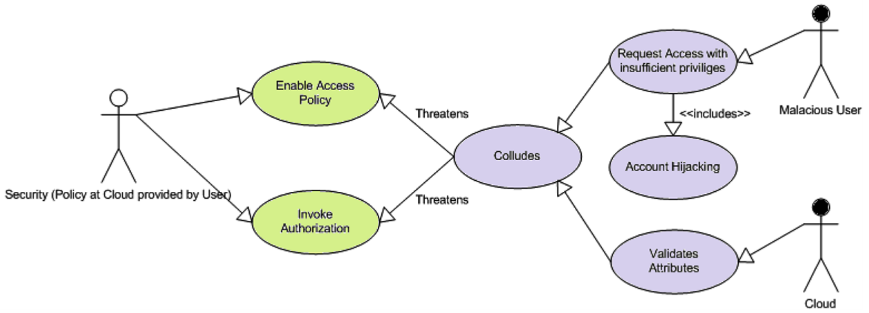


Figure 9 Mis-use case diagram depicting collusion

that threatens the normal security activities that executes in order to safeguard the data. Here, the malicious user with insufficient or totally unmatched privileges requests access to a confidential data stored in the cloud. The cloud on the other hand who is responsible to validate users based upon the access policy and provide access to only the authorized users colludes with the malicious user and relaxes the access policy restrictions allowing the malicious user to portray himself as a legitimate user (mask himself under a valid account-account hijacking) and provides illegal access to the data.

6.2.2 Collusion attack modelling

The sequence of actions depicting the Collusion attack is sown in Figure 10. Here, the owner/device sends his relevant information to the cloud as proof of identity and upon verification is given authorized access to store encrypted data along with the access policy on the cloud. When an attacker/malicious user (insider or an outsider) requests access with insufficient privileges the cloud relaxes the access policy constraints and deliberately colludes with the malicious user/attacker and allows him to access the data as if he were a legitimate user.

6.2.3 Collusion attack mitigation technique

Trusted Third Party can be used to audit the participants' (cloud and the users) activities for fraudulent behaviour, so as to increase the transparency and to trace the source of fraudulence with the help of the identities of the participants that are registered with the TTP.

Nothing is safe in the cloud because "Cloud is assumed to be honest "which is not an ideal case [8, 9]. On this ground a method wherein we could hide even the access policy from the cloud and thus prevent the facility of cloud

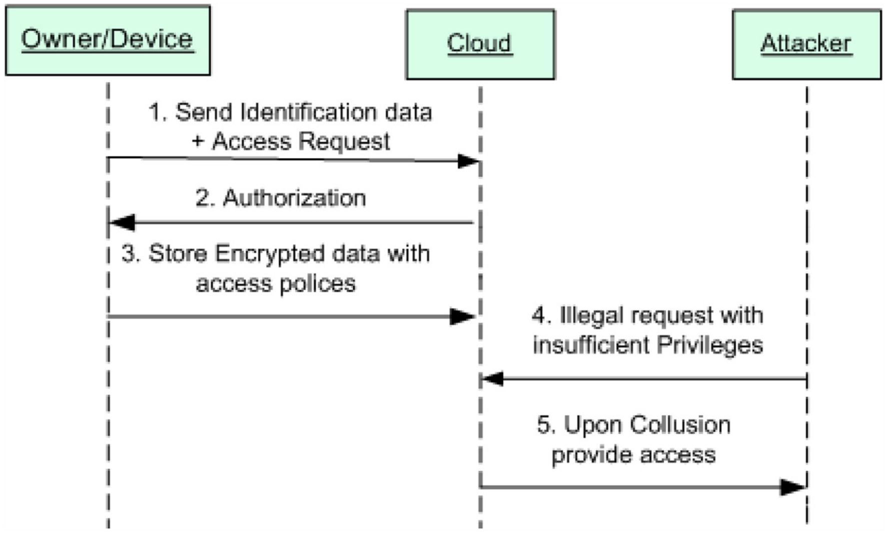

Owner/Device
Cloud
Attacker
1. Send Identification data + Access Request
2. Authorization
3. Store Encrypted data with access polices
4. Illegal request with insufficient Privileges
5. Upon Collusion provide access

Figure 10 Sequence diagram depicting collusion

allowing unauthorized access to stored data which is the crux of the proposed idea in Section 7 has been proposed.

And as mentioned in the paper in Section 6.2.1, collusion attack is described as one happening when situations wherein cloud joins hands with malicious insiders and also the external attackers, and even though the cloud knows that the user is not an authorised one to access data, there are possibilities wherein the cloud could relax the access policy and provide access. This happens because the cloud is not a trusted one all the time. We cannot work upon the assumption that the cloud is honest but curious as is the case with most of the related work discussed in the paper. Relaxation of access policy occurs because the access policy is by default open to the cloud and the cloud is the one that is trusted by the data owner to take care of regulating access to the data and in situations where the cloud is outside the trusted domain of the owner the data is always under threat. Hence an idea has been proposed wherein we make use of cloud to only store data and do some complex resource consuming operations while the decision about regulating access still lies in the hands of the owner or personnel within his trusted domain, by providing only the access structure to the cloud and hiding the access policy. The entire working is explained in Section 7.

6.3 Replay Attack

A replay attack is one in which the transmitted data from the source to the destination over a channel is sniffed by an attacker wherein he hold back the data midway for a stipulated amount of time, tampers the data and sends the tampered or inappropriate data that was not actually the intended information to the destination.

6.3.1 Threat leading to replay attack

- An attacker sniffs the channel for any confidential communication or user related information.
- An attacker waiting over the transmission channel tries to manipulate the transmitted data by holding it back for some time.

The mis-use case diagram in Figure 11 shows the activities of the attacker such as sniffing and monitoring the communication channel in order to get access to confidential data during transmission and alteration of data that threatens the security and confidentiality of the encrypted data that was intended to be sent to the destination by the source.

6.3.2 Replay attack modelling

The sequence of actions depicting the Replay attack is shown in Figure 12. Here, the owner/device sends his relevant information to the cloud as proof of identity and upon verification is given authorized access to store encrypted data along with the access policy on the cloud. A second legitimate and authorized user/device initiates a request for access to the data stored on the cloud and the cloud upon verification of the authenticity initiates the transmission of requested data over the communication link. An attacker who has been monitoring the link holds back the transmitted data tampers or changes the entire information and sends the tampered/inappropriate data to the legitimate user/device which could

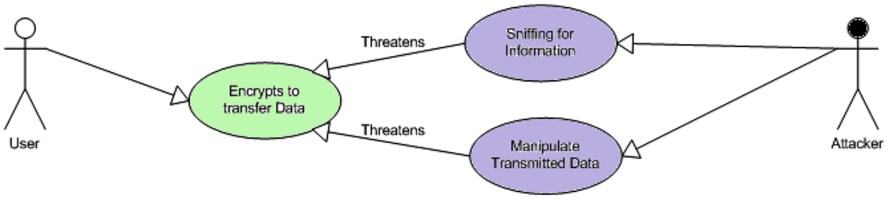


Figure 11 Mis-use case diagram depicting replay attack

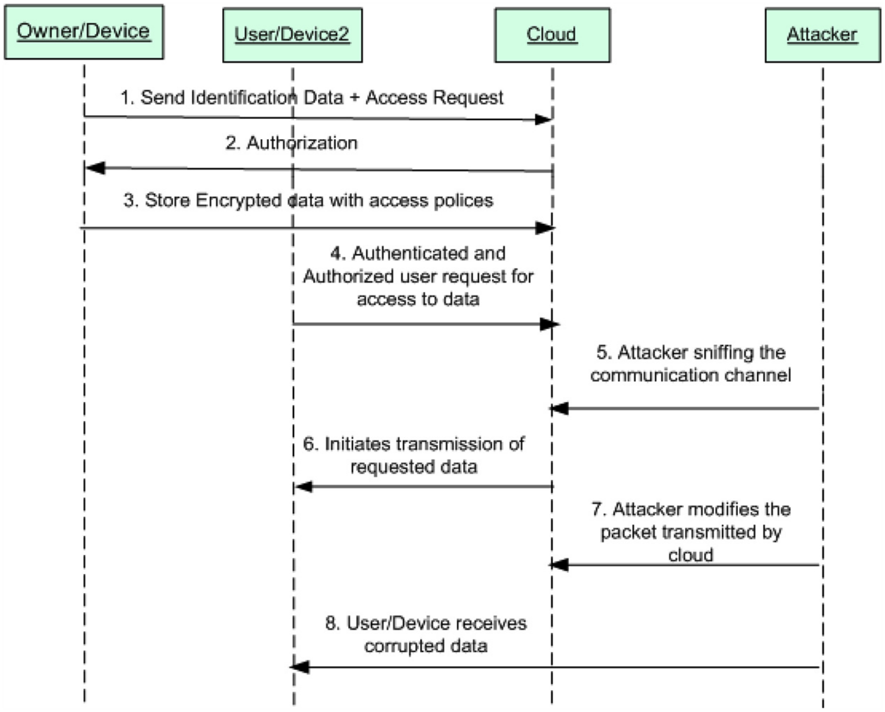

Owner/Device
User/Device2
Cloud
Attacker
1. Send Identification Data + Access Request
2. Authorization
3. Store Encrypted data with access polices
4. Authenticated and Authorized user request for access to data
5. Attacker sniffing the communication channel
6. Initiates transmission of requested data
7. Attacker modifies the packet transmitted by cloud
8. User/Device receives corrupted data

Figure 12 Sequence diagram depicting replay attack

hamper normal functionality. Alternatively this tampering of data over the communication link can also happen when the legitimate user/device sends some data to be stored over the cloud so that when some other user wants to access the data that was originally sent by the owner, is given inappropriate data.

6.3.3 Replay attack mitigation technique

When the message is sent from the user to the cloud, it should include a time stamp or other similar techniques that would pose control based on a predefined (minimal) duration of time that is set at the time of transmission from sender. This is an estimation of the time required for information to reach the destination during normal operation. If this time is exceeded the information is assumed to be tampered and hence it is retransmitted upon suitable request from destination or is ignored at the destination.

7 Proposed IAMFI Architecture

IAMFI addresses the issue wherein the access policy and the attributes (sensitive organizational information) are exposed to the cloud. IAMFI attempts to provide a mechanism of privacy of the attribute information by incorporating the idea of separation of profile information and profile structure [18–20] into the attribute based encryption method for providing access to users who request access to the stored data on the cloud.

As mentioned in architecture of FI given in Section 2, we see that the sensitive accessible data along with the access policy lies in the cloud. So the point of access control comes in existence when the devices communicate with the cloud to access the stored data. Also from the paper [21] and from the discussions from Section 4.2 we understand that the devices serve as a medium of communication between the users and the cloud. These devices connected over the internet along with cloud makes the future internet. Devices could be autonomous as in the case where a light switch controls light in a room over IP. The light lets any device to control it as long as the device is located in the same room, or devices could operate on behalf of users by capturing the user attributes to perform the required function.

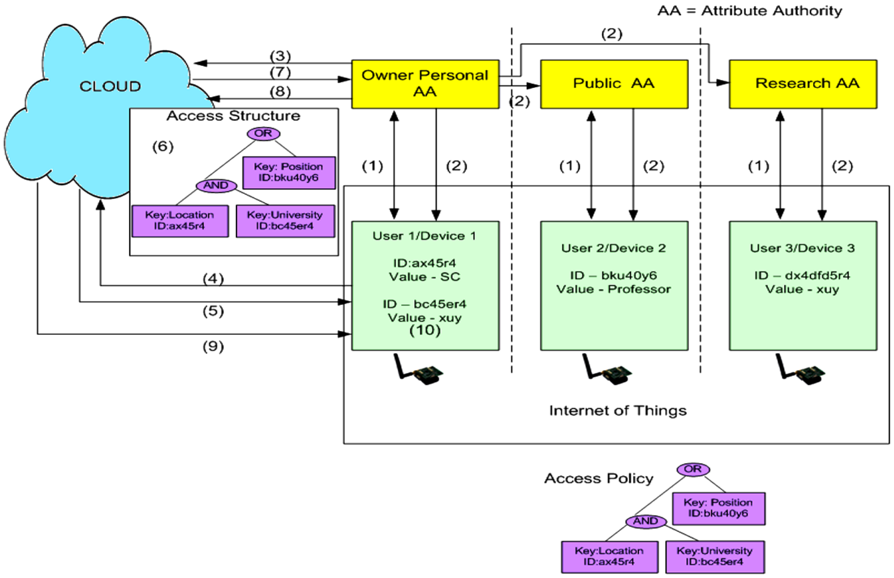
Therefore, the proposed IAMFI has considered the later scenario, wherein the device captures the user attributes and serves and medium of access to the cloud. In the Figure 13, we have represented the IoT (Internet of Things) assuming that the devices are connected over the internet and unique Identities are assigned using various techniques such as RFID, Near Field Communication, IPv6, HIP etc. The following scenario explains the high level architecture of IAMFI.

The proposed IAMFI architecture is shown in Figure 13 wherein, the owner (organization) of the data has several attribute authorities (AA) depending upon the domain under which the various categories of users who access his data. For example, an organization can have users who belong to the same organization (owner is the AA for his personal domain i.e. Personal AA in Figure 13), the researchers who require the organizational data9i.e, Research AA in Figure 13) and common people who are indirectly related to the organization (i.e., Public AA in Figure 13). In all such cases the appropriate attribute authority maintains the management of the users who fall under his category or domain.

The AAs (personal and other attribute authorities) distribute keys to the users who wish to obtain access to the data. The attribute authorities (AA) are also responsible for making decisions upon whether or not to provide access to a user/device that requests access to stored data.

The users who wish read and write access first register themselves with the attribute authority (AA) and obtain appropriate attributes that determine his/her access to data. The AA is responsible for secret key distribution so that the overhead of assigning keys to all the users collectively does not bother the owner (Personal AA).

The Owners (Personal AA) encrypt their data under a certain selected set of attributes. The owner also specifies an access structure tied with the encrypted data that is stored on to the cloud. We consider the attributes of users to be associated with certain keys [18]. For Example, the pairs that say [University = XUY, Location = SC Position = Professor]. Here the values [Position, University and Location] are taken as the keys and the values associated with them [XUY and SC, Manager] are the actual values/attributes/data



1. Obtain attributes
2. Provide write and secret keys
3. Outsource Encrypted Data with access structure
4. Read/write request
5. Access attribute info under user control
6. Map values to access structure
7. Send Mapped Structure to attribute authority
8. Verify valid users and report to cloud (Allow or Deny Access)
9. Authorized users allowed to download
10. Decrypt with secret key

Figure 13 IAMFI architecture

that are required for providing access. To enhance privacy we only provide the access structure to the cloud as shown in Figure 13. For example, [location and university or position].We associate IDs with the keys that reside in the access structure, for example, [key = Location ID = ax45r4] and also associate same IDs to the corresponding data/value/attribute that reside at the user's associated devices for example, [Value = SC, ID= ax45r4]. It is to be noted here that the sensitive data that is the exact attributes or roles that are intrinsic to the organization are not exposed to the cloud.

When a user requests for data for read/write access, the cloud will request for attribute verification. A session is established where the user is in full control while the cloud accesses the attributes of the user. The cloud checks for an ID match to retrieve the values/attributes to the keys that are mentioned in the attribute structure. For example cloud uses the ID [key=Location ID=ax45r4] that is mentioned in the access structure to compare it against the IDs present at the user's devices. Upon finding [Value = SC, ID= ax45r4] that has a matching ID the cloud maps the value/attribute to the key Location in the access structure thus forming the <key,value> pair i.e., <Location,SC>. The cloud uses these attributes to map them to the attribute structure provided by the Owner and computes a Boolean value or any other similar form of representation and sends it to the Owner or the corresponding domain AA(attribute authorities) for verification. The domain to which the computed value has to be sent is made known to the cloud whenever the user/device sends a request to the cloud by appending the information about the domain to which it belongs to. This data is considered to be a non-sensitive data that does not need to be protected from the cloud as the cloud cannot pose a threat based upon the location information. Also, all the attribute authorities lie within the trusted domain of the owner of the data and hence the owner also shares the access policy against which decisions are to be made for allowing access, with the various individual AAs. Once the data has been sent the session is closed and any data corresponding to the attributes of the user is deleted from the cloud storage.

The owner or the corresponding AA checks the received computed value against the access policy that it has at its end and if a match is found then the owner sends a reply to the cloud to allow access to the user or deny access in case there is no match found. In this way the cloud is prevented from knowing the access policy or attributes that satisfy the specified access policy. Once access has been granted to the user/device, s/he can download the data and decrypt it using the secret keys received from the attribute authority. It is to be noted here that the identity assignment to devices has not been included in the scope of this paper. It is assumed that devices that exist online already have been assigned unique Identities.

Hence, the proposed IAMFI architecture helps to avoid the possibility of collusion attack as mentioned in Section 6.2 by hiding the exact access policy from the cloud. Hence the cloud has no possible chance of learning the exact access policy that provides access to stored data, additionally since the decision about providing access to data still lies in the hands of the owner or other trusted personnel within his trusted domain the possibility of cloud colluding with the malicious attackers and providing unauthorised access is being taken care of. Further replay attacks are to be taken care of by appending a timestamp T and a MAC (message authentication code) to the request/data that is sent. Also a predefined threshold value is provided. If the intended destination finds that the timestamp T is greater than the predefined threshold it is assumed to be held back midway and tampered and is discarded. Finally the DoS attack is to be taken care of by establishing a TTP (trusted third party) that helps to track down the activities of the cloud. Further the DoS attack that happens due to the attack on a cloud service by devices attempting to indefinitely or temporarily stop the cloud services to the intended or authorized users is taken care of by the session establishment that is proposed in this section and the associated device identities. It is easy to manage the access using one ID per session and also address the access of the same ID to the same resource by regulating it to one session at a time.

8 Conclusion and Future Work

Thus IAMFI provides a mechanism of privacy of the attribute information by incorporating the idea of separation of profile information and profile structure into the attribute based encryption method for providing access to users who request access to the stored data on the cloud. IAMFI also relieves the owner from the overhead of managing the user registration and key management activities. The attribute authority will be able to trace the activity of the user in case of malpractice with the registered Identity of the user. It is also possible for the personal attribute authority to trace the activity of the cloud service provider by allowing the attribute authority to have the ID of the CSP registered with it. Alternatively, a trusted third party (TTP) can also be introduced wherein the users and the CSP register their IDs with the TTP. In the event of any fraudulent activity the TTP serves as a mediator who would track the IDs and identify the person responsible for the fraudulence.

In future extension to this work will be done by developing appropriate algorithms and models for implementing IAMFI with suitable key management techniques that takes care of user attributes/identities and appropriate key generation in our following papers. We will also be extending our work by developing detailed protocols to address the various attacks that are mentioned in this paper will be developed.

9 List of Abbreviations

Acronym	Expansion
IAMFI	Identity and Access Management in Future Internet
FI	Future Internet
IoT	Internet of Things
CSP	Cloud Service Provider
AA	Attribute Authority
ACV-BGKM	Access control vector broadcast group key management
RBAC	Role Based Access control Model
CP-ABE	cipher text policy attribute based encryption
DoS	Denial of Service
TTP	Trusted Third Party
KDC	Key Distribution Center

References

[1] http://en.wikipedia.org/wiki/Internet

[2] http://www.nets-fia.net/

[3] http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-accessto-internal-google-and-yahoo-cloud- data/

[4] http://www.csoonline.com/article/205053/the-abcs-of-identity-management

[5] https://vsis-www.informatik.uni-hamburg.de/getDoc.php/publications/201/BaierKunze04-INetSec.pdf

[6] http://www.zdnet.com/access-control-changes-a-must-for-future-safe-internet-vint-cerfsays[7000018569/

[7] HolgerKinkelin, HeikoNiedermayer, Ralph Holz, and Georg Carle, 'TPM-based Access Control for the Future Internet', Network Architectures and Services TechnischeUniversitätMünchen

[8] Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan, 'Mona: Secure Multi- Owner Data Sharing for Dynamic Groups in the Cloud', IEEE Transactions On Parallel and Distributed Systems, Vol. 24, No. 6, June 2013.

[9] SushmitaRuj, Member, IEEE, Milos Stojmenovic, Member, IEEE, and AmiyaNayak, Senior Member, IEEE, 'Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds', IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014.

[10] AyadBarsoum and Anwar Hasan, Senior Member, IEEE, 'Enabling Dynamic data and indirect mutual trust for cloud computing storage systems', IEEE Transactions OnParallel And Distributed Systems, Vol. 24, No. 12, December 2013.

[11] Mohamed Nabeel, Member, IEEE, Ning Shang, and Elisa Bertino, Fellow, IEEE 'Privacy Preserving Policy-Based Content Sharing in Public Clouds', IEEE Transactions On Knowledge and Data Engineering Vol. 25, No. 11, November 2013.

[12] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, 'Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage', IEEE Transactions On Information Forensics and Security, Vol. 8, No. 12, December 2013.

[13] Kan Yang, Associate Member, IEEE, XiaohuaJia, Fellow, IEEE, KuiRen, Senior Member, IEEE, Bo Zhang, Member, IEEE, and RuitaoXie, Student Member, IEEE, 'DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems', IEEE Transactions On Information Forensics And Security, Vol. 8, No. 11, November 2013.

[14] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE, 'HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing', IEEE Transactions On Information Forensics and Security, VOL. 7, NO. 2, APRIL 2012.

[15] BRODKIN, J. Loss of customer d.ata spurs closure of online storage service 'The Linkup'. Network World (August 2008).

[16] CLOIDIFIN.http://community.zdnet.co.uk/blog/0,1000000567,2000625196b,00.htm?new_comment

[17] Mervat Adib Bamiah, Advanced Informatics School Universiti Teknolog, Malaysia Kuala Lumpur, Sarfraz Nawaz Brohi Advanced Informatics School Universiti Teknologi, Malaysia, Kuala Lumpur, 'Seven Deadly Threats and Vulnerabilities in Cloud Computing', International Journal Of Advanced Engineering Sciences and Technilogies, Vol No. 9, Issue No. 1, 087 – 090, 2011

[18] BjoernWuest, Olaf Drogehorn, KausDavid, ‘Architecture for profile translation’, Supported in part by European Union Information Society Technology, February 04 2005.

[19] R.M. Arlien, B. Jai, M. Jakobsson, F. Monrose, M.C. Reiter, ‘Privacy–preserving global customization’, In Proceedings of the second ACM conference on Electronic commerce, Minneapolis, *USA*, p.176–184, October 2000.

[20] S.Riche, GBrener, M.Gittler, ‘Client-side ProifleSorage: a means to put user in control’, Public Technical Report. Heweltt Packard Laboratories Grenoble, November 2001.

[21] Jan Janak, Hyunwoo Nam, and Henning Schulzrinne Columbia University, ‘On Access Control in the Internet of Things’, February 15, 2012.

Biographies

Nancy Ambritta P. graduated in Computer Science and Engineering from Anna University, Tamil Nadu, India in the year 2010. She is currently pursuing Masters in Computer Engineering at Smt. Kashibai Navale College of Engineering, Pune. Her research interests are cloud security and the Future Internet.

Poonam Railkar received the Masters in Computer Networks from Pune University Maharashtra, India in the year 2013. She is currently working as an Assistant Professor at Smt. Kashibai Navale College of Engineering, Pune. She has published 6 journals and 3 conference papers. Her research interests are Mobile Computing and Security.

Parikshit N. Mahalle received PhD (Wireless Communication) from CTIF, Aalborg university, Aalborg, Denmark and is IEEE member, ACM member, Life member ISTE and graduated in Computer Engineering from Amravati University, Maharashtra, India in 2000 and received Master in Computer Engineering from Pune University in 2007. From 2000 to 2005, was working as lecturer in Vishwakarma Institute of technology, Pune, India. From August 2005, he is working as Professor and Head in Department of Computer Engineering, STES 's Smt. Kashibai Navale College of Engineering, and Pune, India. He published 40 papers at national and international level. He has authored 5 books on subjects like Data Structures, Theory of Computations and Programming Languages. He is also the recipient of "Best Faculty Award" by STES and Cognizant Technologies Solutions. His research interests are Algorithms, IoT, Identity Management and Security.