IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 6, Ver. I (Nov - Dec 2018), PP 33-39
www.iosrjournals.org

A Survey on Secure Key Policy Attribute-Based Encryption Policy for Data Sharing Among Dynamic Groups in the Cloud

[1]Soniya Thomas, Mphil.Scholar, [2]Mr.J.Santhosh MSc, MCA, Mphil
[1]Department Of Computer Science Sree Narayana Guru College Kg Chavady,Coimbatore 641105 Tamilnadu
[2]Asst.Professor Department Of Computer Science Sree Narayana Guru College Kg Chavady,Coimbatore 641105 Tamilnadu
Corresponding Author: Soniya Thomas

Abstract: *Profited from distributed computing, clients can accomplish a powerful and sparing methodology for information sharing among gathering individuals in the cloud with the characters of low support and little administration cost. Then, we should give security insurances to the sharing information records since they are outsourced. Lamentably, in view of the continuous change of the participation, sharing information while giving security saving is still a testing issue, particularly for an untrusted cloud because of the intrigue assault. Besides, to exist conspires, the security of key appropriation depends on the protected correspondence channel, be that as it may, to have such channel is a solid supposition and is troublesome for practice. In this paper, we propose a secure information sharing plan for element individuals. Firstly, we propose a safe way for key conveyance with no protected correspondence channels, and the clients can safely acquire their private keys from gathering chief. Furthermore, our plan can accomplish fine-grained access control, any client in the gathering can utilize the source in the cloud and disavowed clients can't get to the cloud again after they are denied. Thirdly, we can shield the plan from agreement assault, which implies that disavowed clients can't get the first information document regardless of the possibility that they plan with the untrusted cloud.*
Major problem in public clouds is how to share documents based on fine-grained attribute based access control policies, sharing data in a dynamic groups while preserving data and identity privacy from an un trusted cloud is still a challenging issue, due to the frequent change of the membership., encrypting documents with different keys using a public key cryptosystem such as attribute based encryption (ABE), and/or proxy re-encryption (PRE) approach has some weaknesses: it cannot efficiently handle adding/revoking users or identity attributes, and policy changes; it requires to keep multiple encrypted copies of the same documents; it incurs high computational costs. In this paper, I propose a secure multi-owner attribute authorities based data sharing scheme for dynamic groups in the cloud. Tha aim of my paper is secure data sharing in a dynamic group where the there is no fixed Attribute authorities where as multi – owner attribute authorities scheme is possible. key policy key policy attribute-based encryption (KP-ABE) method is used to select dynamic AA(Attribute authorities). By leveraging group signature, signed receipts and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. As the result the computation cost is reduced and storage overhead and encryption computation cost of our scheme are independent with the number of revoked users so the encryption cost is also reduced.

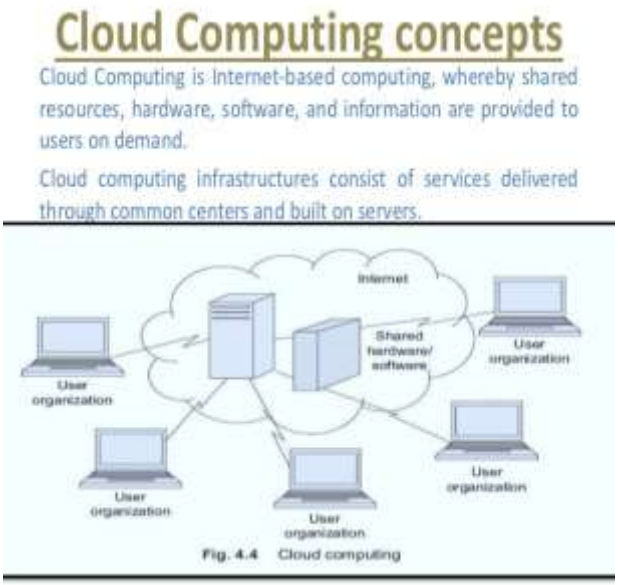
Date of Submission: 29-10-2018 Date of acceptance: 12-11-2018

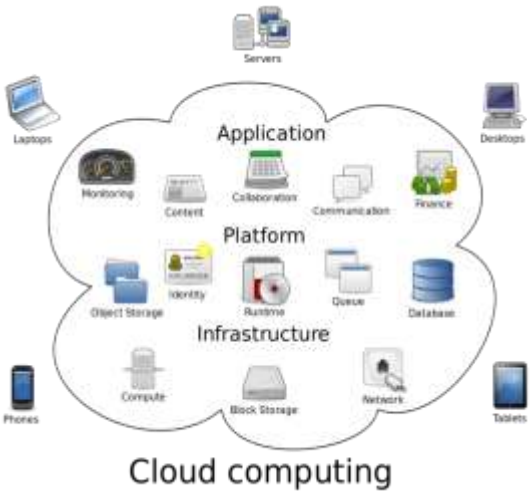
I. Introduction

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and

user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secure under existing security models.

In my approach, by utilizing polynomial capacity, we can accomplish a protected client repudiation plan. At long last, our plan can accomplish fine proficiency, which implies past clients need not to upgrade their private keys for the circumstance either another client joins in the bunch or a client is renounced from the gathering. Tha aim of proposed system is secure data sharing in a dynamic group where the there is no fixed Attribute authorities where as multi – owner attribute authorities scheme is possible. key policy key policy attribute-based encryption (KP-ABE) method is used to select dynamic AA (Attribute authorities). By leveraging group signature, signed receipts and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. As the result the computation cost is reduced and storage overhead and encryption computation cost of our scheme are independent with the number of revoked users so the encryption cost is also reduced. Cloud computing provides a more cost effective environment to outsource storage computation. Many enterprises need to store and operate huge amount of data. One serious problem of today's cloud storage service is the management of ever increasing volume of data . To make data management elastic in cloud computing de-duplication system is used. Data de-duplication is a compression technique that improves storage efficiency by eliminating redundant data. In this approach we have proposed a de-duplication technique which is different from traditional de-duplication system. In this system users with differential privileges are also consider in duplicate check which was not possible in previous de-duplication system. Again in this approach we also focus on the confidentiality of sensitive data in support of de-duplication. We are proposing a Hybrid cloud approach. In Hybrid cloud approach two cloud are maintained, public cloud and a private cloud. A private cloud is working as an interface between user and public cloud. Private cloud provides a set of private key to the user. We also presented several new de-duplication constructions supporting authorized duplicate check in hybrid cloud architecture.





II. Proposed System

A) Creating A Grid:

Generally a grid refers to frame like structure which is created for a particular group of departments in an organization and a cluster is loosely connected suborganizations that are viewed as a single organization. This technique initially develops a cluster in which the departments that are belonging to the same organizationare powered under that cluster. Then a frame is developed around that cluster which completely forms a grid for that departmentunder the cloud environment. This will not allow other departments of organization to communicate with that grid. By means of this a trustable service is provided and an unwanted interruption among the department is avoided.

B) Creating A Virtual Private Network:

Virtual private network provides a secured connection across public network. It gives organization a secured way to use the internet pathways. Here the organizations department which is having the previously established grid for them in the cloud environment is directly linked with means of virtual private network. This virtual private network uses the concept of cryptography in which the encryption and decryption concept is

followed while data sharing or service sharing under cloud environment. The virtual private network is established between the department of organization and its respective grid created under cloud to form a convincing infrastructure for their communication and for service sharing with the cloud.

C) Support Provided:

This architecture provides the support for virtualization i.e., when different department or physically distributed branches of same organization is requesting for service in the cloud they can access simultaneously in the same grid that was created for them in the cloud environment. This technique not only provides the support for departments under a public cloud environmentbut also for the departmentof other organizations under private cloud environment. It provides a support for an organization against the issue regarding "loss of control".

III. Advanced Techniques Used

- **Data Encryption Methods**
- **Encryption And Cryptography**
- **Stay Safe And Secure With Encryption**
- **Cryptographic Key Management System**

Data Encryption Methods

AES: The Advanced Encryption Standard, AES, is a symmetric encryption algorithm and one of the most secure. The United States Government use it to protect classified information, and many software and hardware products use it as well. This method uses a block cipher, which encrypts data one fixed-size block at a time, unlike other types of encryption, such as stream ciphers, which encrypt data bit by bit.

AES is comprised of AES-128, AES-192 and AES-256. The key bit you choose encrypts and decrypts blocks in 128 bits, 192 bits and so on. There are different rounds for each bit key. A round is the process of turning plaintext into cipher text. For 128-bit, there are 10 rounds; 192-bit has 12 rounds; and 256-bit has 14 rounds.

Since AES is a symmetric key encryption, you must share the key with other individuals for them to access the encrypted data. Furthermore, if you don't have a secure way to share that key and unauthorized individuals gain access to it, they can decrypt everything encrypted with that specific key.

3DES: Triple Data Encryption Standard, or 3DES, is a current standard, and it is a block cipher. It's similar to the older method of encryption, Data Encryption Standard, which uses 56-bit keys. However, 3DES is a symmetric-key encryption that uses three individual 56-bit keys. It encrypts data three times, meaning your 56-bit key becomes a 168-bit key.

Unfortunately, since it encrypts data three times, this method is much slower than others. Also, because 3DES uses shorter block lengths, it is easier to decrypt and leak data. However, many financial institutions and businesses in numerous other industries use this encryption method to keep information secure. As more robust encryption methods emerge, this one is being slowly phased out.

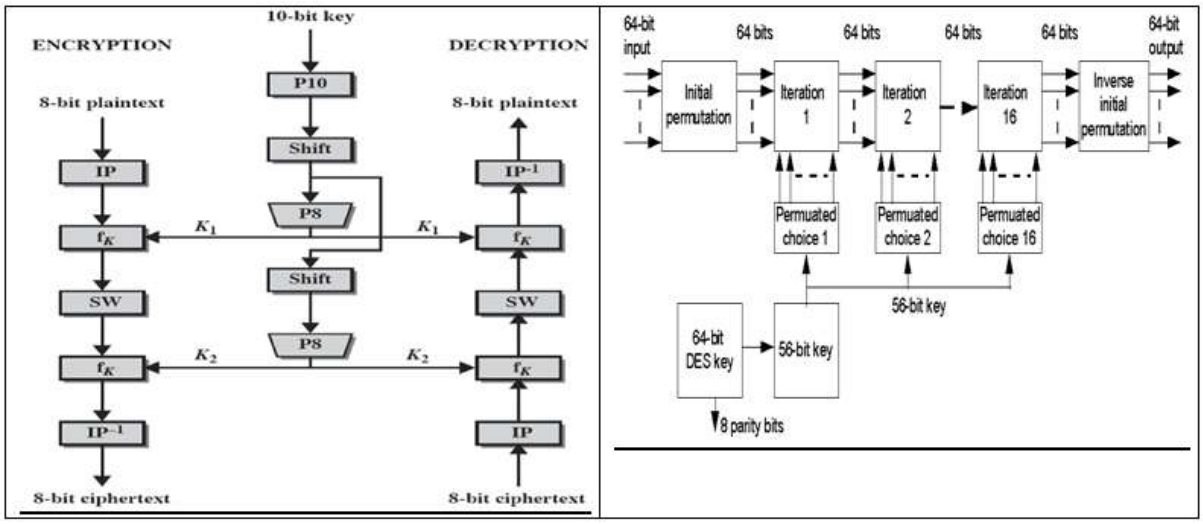
Twofish: Twofish is a symmetric block cipher based on an earlier block cipher – Blowfish. Twofish has a block size of 128-bits to 256 bits, and it works well on smaller CPUs and hardware. Similar to AES, it implements rounds of encryption to turn plaintext into cipher text. However, the number of rounds doesn't vary as with AES; no matter the key size, there are always 16 rounds.

In addition, this method provides plenty of flexibility. You can choose for the key setup to be slow but the encryption process to be quick or vice versa. Furthermore, this form of encryption is unpatented and license free, so you can use it without restrictions.

RSA: This asymmetric algorithm is named after Ron Rivest, Adi Shamir and Len Adelman. It uses public-key cryptography to share data over an insecure network. There are two keys: one public and one private. The public key is just as the name suggests: public. Anyone can access it. However, the private key must be confidential. When using RSA cryptography, you need both keys to encrypt and decrypt a message. You use one key to encrypt your data and the other to decrypt it.

According to Search Security, RSA is secure because it factors large integers that are the product of two large prime numbers. Additionally, the key size is large, which increases the security. Most RSA keys are 1024-bits and 2048-bits long. However, the longer key size does mean it's slower than other encryption methods.

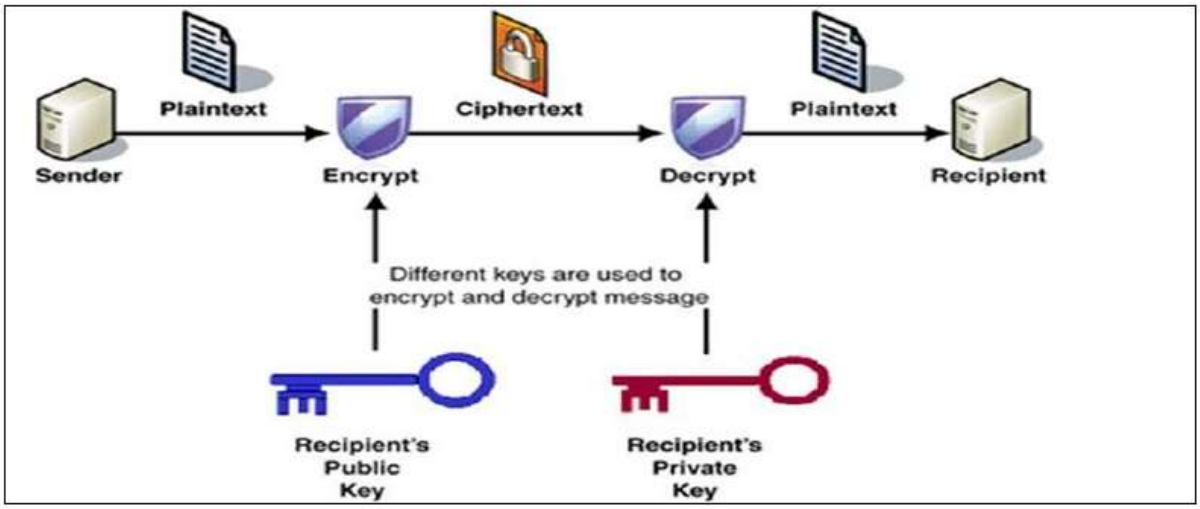
While there are many additional encryption methods available, knowing about and using the most secure ones ensures your confidential data stays secure and away from unwanted eyes.



Cryptography And Encryption

Cryptography or **cryptology** is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages, various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation[4] are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating ciphertext that can be read only if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-randomencryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.



Stay Safe And Secure With Encryption

1.Email: Rethink your email setup. Assume that all "free" email and webmail services (Gmail etc) are suspect. Be prepared to pay for a service, such as Fastmail,that is not based in the US – though some of its servers are in New York with backups in Norway. (My hunch is that more non-US email services will appear as entrepreneurs spot the business opportunity created by the Snowden revelations.) It would also be worth checking that your

organisation has not quietly outsourced its email and IT systems to Google or Microsoft – as many UK organisations (including newspapers and universities) have.

The real difficulty with email is that while there are ways of keeping the content of messages private (see encryption), the "metadata" that goes with the message (the "envelope", as it were) can be very revealing, and there's no way of encrypting that because its needed by the internet routing system and is available to most security services without a warrant.

2.Encryption: Encryption used to be the sole province of geeks and mathematicians, but a lot has changed in recent years. In particular, various publicly available tools have taken the rocket science out of encrypting (and decrypting) email and files. GPG for Mail, for example, is an open source plug-in for the Apple Mail program that makes it easy to encrypt, decrypt, sign and verify emails using the OpenPGP standard. And for protecting files, newer versions of Apple's OS X operating system come with FileVault, a program that encrypts the hard drive of a computer. Those running Microsoft Windows have a similarprogram. This software will scramble your data, but won't protect you from government authorities demanding your encryption key under the Regulation of Investigatory Powers Act (2000), which is why some aficionados recommend TrueCrypt, a program with some very interesting facilities, which might have been useful to David Miranda.

3 Web browsing: Since browsing is probably what internet users do most, it's worth taking browser security and privacy seriously. If you're unhappy that your clickstream (the log of the sites you visit) is in effect public property as far as the security services are concerned, you might consider using freely available tools such as Tor Browser to obscure your clickstream. And to protect yourself against the amazingly brazen efforts by commercial companies to track your online behaviour you should, at the very minimum, configure your browser so that it repels many of these would-be boarders.

4.Cloud services: The message of the Snowden revelations is that you should avoid all cloud services (Dropbox, iCloud, Evernote, etc) that are based in the US, the UK, France and other jurisdictions known to be tolerant of NSA-style snooping. Your working assumption should be that anything stored on such systems is potentially accessible by others. And if you must entrust data to them, make sure it's encrypted.

5.File storage and archiving: An option that an increasing numbers of people are exploring is running their own personal cloud service using products such as PogoPlug and Transporterthat provide Dropbox-type facilities, but on internet connected drives that you own and control. And if you carry around confidential data on a USB stick, make sure it's encrypted using TrueCrypt.

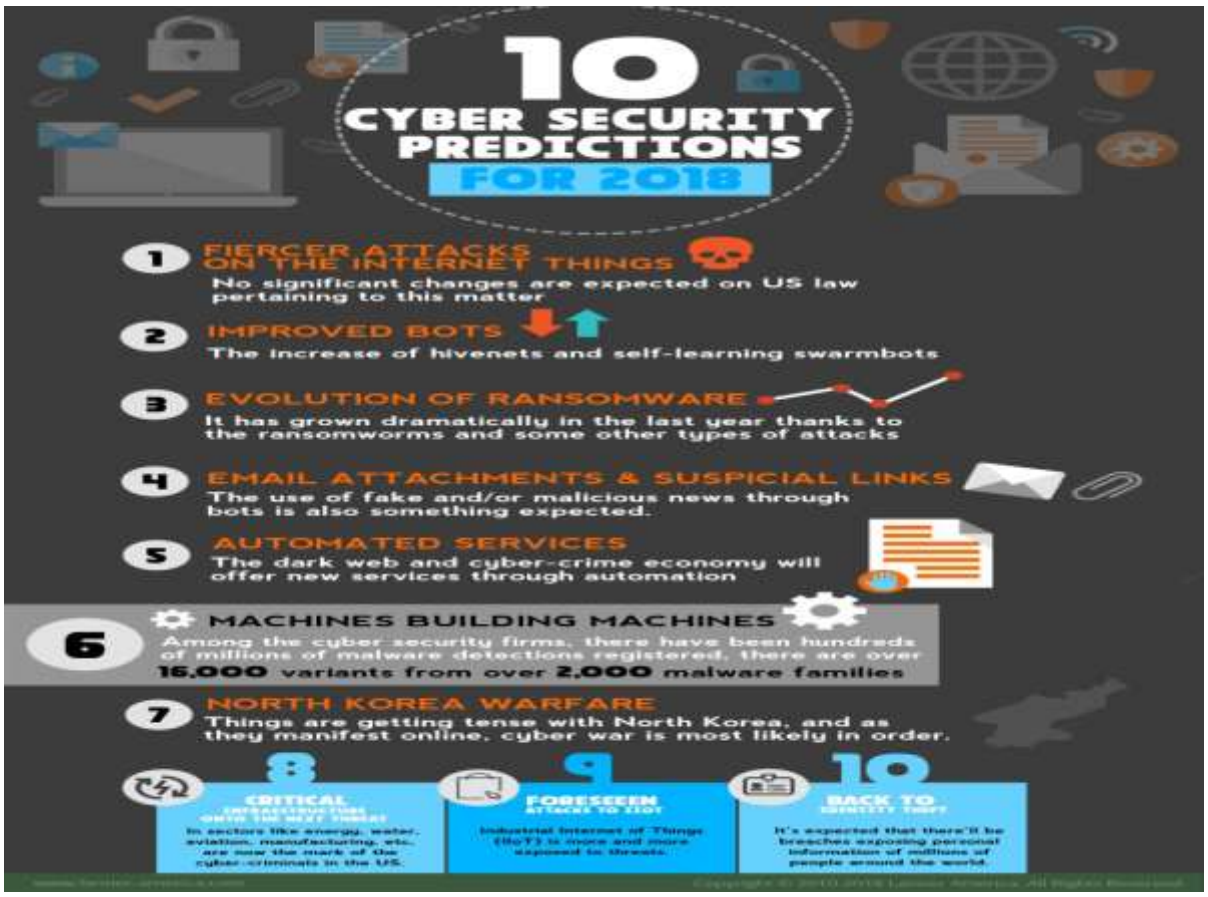
6.Social networking: Delete your Facebook account. Why do the CIA's work for it? And if you must use it, don't put your date of birth on your profile. Why give identity thieves an even break? And remember that, no matter what your privacy settings, you don't have control over information about you that is posted by your "friends".

7.Location data: Avoid using services such as FourSquare that require location information.

8.Wireless services: Have Bluetooth off by default in all your mobile devices. Only switch it on when you explicitly need to use it. Otherwise you'll find that even a dustbin can snoop on it. Similarly, beware of using open wifi in public places. At the very minimum, make sure that any site you interact with uses HTTPS rather than unencrypted HTTP connections. If you don't then anyone nearby can use Firesheep to see everything you're doing.

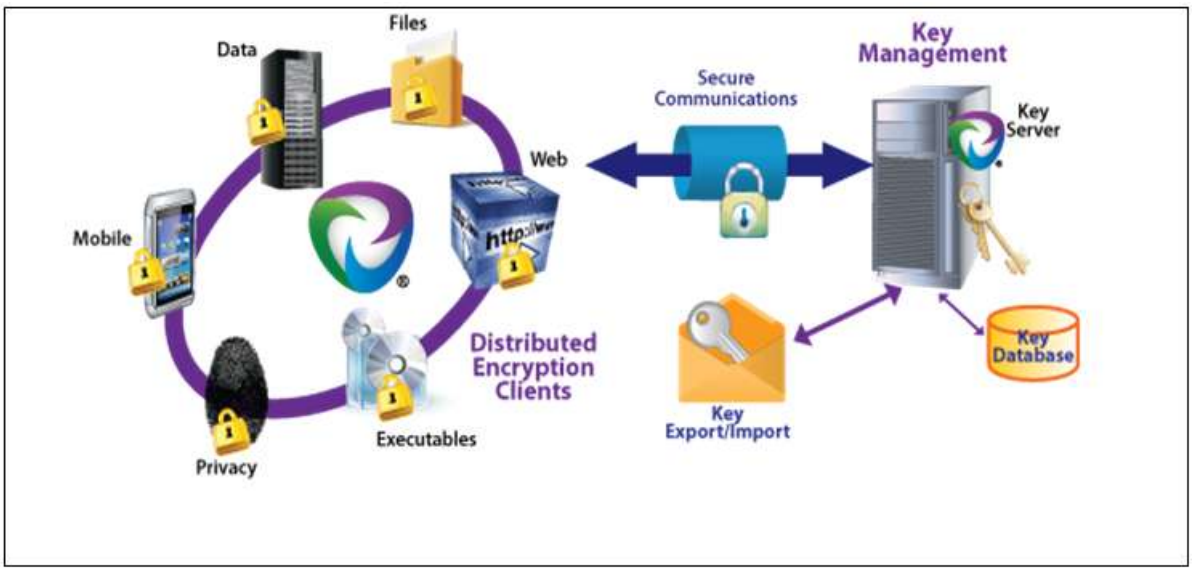
9.Personal security: Forget password, think passphrase – ie a meaningless sentence that you will remember – and do some transformations on it (first and third letters of every word maybe) so that you can generate a stronger password from it every time. Or use a password-management app like LastPass or 1Password. And if a service offers multi-factor authentication, make use of it.

10.Search engines: All the big search engines track your search history and build profiles on you to serve you personalised results based on your search history. if you want to escape from this "filter bubble" you need to switch to a search engine that does not track your inquiries. The most obvious one is the bizarrely named but quite effective DuckDuckGo.



Cryptographic Key Management System

Encryption key management is the administration of tasks involved with protecting, storing, backing up and organizing encryption keys.High-profile data losses and regulatory compliance requirements have caused a dramatic increase in the use of encryption in the enterprise. A single enterprise might use several dozen different and possibly incompatible encryption tools, resulting in thousands of encryption keys. Each key must be securely stored, protected and retrievable.There are several encryption key management standards efforts underway. The best known is the Key Management Interoperability Protocol (KMIP) developed by vendors and submitted to the Organization for the Advancement of Structured Information Standards (OASIS). The goal of KMIP is to allow users to attach any encryption device to a key management system.



There are three primary types of keys that need to be kept safe and secure:

1. **Symmetric keys –** typically used to encrypt bulk data with symmetric algorithms like 3DES or AES; anyone with the secret key can decrypt the data
2. **Private keys –** the secret half of public/private key pairs used in public-key cryptography with asymmetric algorithms like RSA or ECDSA; anyone with the private key can impersonate the owner of the private key to decrypt private data, gain unauthorized access to systems or generate a fraudulent digital signature that appears authentic
3. **Hash keys –** used to safeguard the integrity and authenticity of data and transactions with algorithms like HMAC-SHA256; anyone with the secret key can impersonate the originator of the data/transactions and thus modify the original data/transactions or create entirely false data/transactions that any recipient will believe is authentic.

Soniya Thomas. "A Survey on Secure Key Policy Attribute-Based Encryption Policy for Data Sharing Among Dynamic Groups in the Cloud" IOSR Journal of Computer Engineering (IOSR-JCE) 20.6 (2018): 33-39.