A Review on Keyless Signature Infrastructure over Traditional Cryptographic Techniques for Cloud Data Security

Remya chandran
PhD Research Scholar
Department of Computing Science
Vel's University Chennai

Abstract— **Keyless signatures are an alternative solution to traditional PKI signatures. Keyless signatures are not vulnerable to key compromise and hence provide a solution to the long-term validity of digital signatures. The traditional PKI signatures may be protected by timestamps, but as long as the time-stamping technology itself is PKI-based, the problem of key compromise is still not solved completely. Keyless signatures are a solution to this problem. In a keyless signature system, the functions of signer identification and of evidence integrity protection are separated and delegated to cryptographic tools suitable for those functions. Keyless Signature (KSI) is a Hash-tree based industrial scale Block chain technology that is part of data security. This technology provides real-time massive scale data integrity validation, time stamping and signature signer identification services.**

Keywords— KSI,PKI, attacks, portable.

I. TRADITIONAL APPROACHES

The Cryptography or methods used for securing the information are classified into following categories:

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Digital Signature

A. Symmetric-Key Cryptography

Symmetric-Key Cryptography is a type of encryption in which same secret key is used to encrypt and decrypt information. However, symmetric key cryptographic techniques suffer from many problems:

1. Key distribution problem
2. Key management problem
3. Inability to digitally sign a message.

B. Asymmetric Key Cryptography

The problem with secret keys is exchanging them over the Internet while preventing them from thief. Anyone who knows the secret key can decrypt the message. To overcome this, we have asymmetric encryption technique, in which there is related pair of keys. A public key is available to anyone who might want to send you a message. A second, private key is kept secret, so that only receiver knows it. Any messages that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key.

TABLE I ASYMMETRIC ENCRYPTION ALGORITHMS

Algorithm Family	Crypto system	Security Level(in bit)				Advantage	Disadvantage
		80	128	192	256		
Integer factorization	RSA	1024	3072	7680	15360	Only intended user can read the message using their private key.	Many secret key encryption methods that is significantly faster than any current available public-key encryption.
Discrete logarithm	DH	1024	3072	7680	15360	The shared key (i.e the secret) is never itself transmitted over the channel.	Lack of authentication.
Discrete logarithm	DSA	1024	3072	7680	15360	It is used for authentication and integrity.	The security of private key depends entirely on the security of the computer.
Discrete logarithm	ElGamal	1024	3072	7680	15360	The same planetext gives a different ciphertext(with near certainly) each time it is encrypted.	The need for randomness and slower speed and has long ciphertext.
Elliptic Curves	ECC	160	256	384	512	Short key is faster and requires less computing power.	It is more expensive and it shortens the life time of batteries.

I

Table II Classical symmetric encryption algorithms

SL.NO	Encryption Technique Name	Granularity (stream/block cipher)	Key size	Vulnerable to attack	Uniqueness about the techniques
1	**Caesar Cipher**	**Block cipher**	**25 keys**	**Brute force attack**	**Simple substitution with alphabet**
2	**Playfair**	**Block cipher**	**25 Keys**	**Brute force attack, Frequency analysis**	**Use pair of letters and substitute with 5×5 matrix designed with key and remaining alphabets**
3	**Hill Cipher**	**Block cipher**	25 Keys	**Known plaintext attack**	**Based on Linear algebra, Convert plaintext into matrix based on ASCII value**
4	**Vigenere Cipher**	**Block cipher**	**25 keys**	**Frequency analysis, Kasiski examination**	**Arrange the letters in 26*26 matrix and perform substitution with pair of letters**
5	**Vernam cipher**	**Stream cipher**	**25 keys**	**plaintext**	**plaintext bits and key**
6	**One time pad**	**Stream cipher**	**Equal To plain text size**	**Key and cipher text chosen**	**Same as vigenere cipher but here key size must be equal to plaintext size**
7	**Rail Fence**	**-**		**Known cipher text, Chosen plaintext**	**Plaintext is written downwards on successive "rails" of an imaginary fence, then moving up when we get to the bottom.**
8	**Root cipher**	**-**	**-**	**Known cipher text, Chosen Plaintext.**	**Same as Rail fence but re arranging cipher text as spiral inwards, clockwise, starting from**

Table III Modern symmetric encryption algorithms

SL.NO	Encryption Technique Name	Granularity (stream/block cipher)	Key size	Vulnerable to attack	Uniqueness about the techniques
1	**Camellia**	**Block cipher (128 bits)**	**128, 192, or 256 bits**	**algebraic attack**	**16 rounds 8*8 S-boxes. Nested Feistel Network**
2	**Serpent**	**Block cipher (128 bits)**	**128, 192 or 256 bits**	**Linear cryptanalysis and Rectangle algebraic attack**	**32 rounds, Open source algorithm**
3	**Rijndael**	**Block cipher (128 bits)**	**128, 192 or 256 bits**	**Related Key Attack, Algebraic attack**	**10,12,14 rounds (depending on the key size) maximal size of the input file is 2,097,152 bytes**
4	**Skipjack**	**Block cipher (64 bits)**	**80 bits**	**Slide attack**	**32 rounds unbalanced Feistel Network Structure**
5	**AES**	**Block cipher (128 bits)**	**128, 192, 256 bits**	**Known plaintext, Side channel attack**	**Substitution-permutation network, 10 or 12 or 14 rounds**
6	**RC-6**	**Block cipher (128 bits)**	**128, 192, 256 bits**	**Known plaintext, chosen cipher text**	**Feistel network, 20 rounds**
7	**SEED**	**Block cipher (128 bits)**	**128 bits**	**Chosen plaintext, Known plaintext**	**16 rounds 8*8 s-boxes Nested Feistel Network**
8	**Twofish**	**Block cipher (128 bits)**	**128 256 bits**	**Truncated differential cryptanalysis**	**16 rounds Feistel Structure. Free to use**
9	**CAST-256**	**Block cipher (128 bits)**	**128 160 192 224 256 bits**	**Known plain text and cipher text**	**Feistel Network Structure**

SL.NO	Encryption Technique Name	Granularity (stream/block cipher)	Key size	Vulnerable to attack	Uniqueness about the techniques
10	XTEA	Block cipher (64 bits)	128 bits	Related key differential attack, chosen plaintexts	Variable rounds. Nested Feistel Network
11	RC-2	Block cipher (64 bits)	8-128 bits (64 bits)	Related key attack, Chosen plaintext	18 rounds Source heavy Feistel Network Structure
12	CAST-128	Block cipher (64 bits)	40 to 128 bits	Chosen cipher text and Known plain text	12 or 16 rounds Feistel Network Structure
13	RC-5	Block cipher (32,64,128 bits)	0 to 2040 bits (suggested 128bits)	Differential attack	Feistel-like network, 1 to 255(suggested 12)
14	TEA	Block cipher (64 bits)	128 bits	Related key attack, Chosen plaintext	Variable rounds Feistel Network Structure
15	Blowfish	Block cipher (64 bits)	32-448 bits	Second-order differential attack, Weak key	16 rounds Feistel Structure. Free to use, key independent S-box
16	IDEA	Block cipher (64 bits)	128 bits	Weak keys,	8.5 rounds Feistel Network Structure
17	TDES	Block cipher (64 bits)	112 or 168 Bits	Theoretically possible, Known plaintext, chosen plaintext	48 rounds Feistel Network Structure, Three different keys used
18	DES	Block cipher (64 bits)	56 bits	Differential & Linear Cryptanalysis, Brute-force attack	16rounds Feistel Structure, Left circular shift,Substitution 32-bit swap

C. Digital Signature

For authentication and non-repudiation purpose within cloud computing environment digital signature has assumed great significance. There are various digital signature algorithms which involves the generation of message digest (hash). MD5 and SHA-1 are well known digital signature generation algorithms and comparative study of these are described with the help of table:

Characteristics	MD5	SHA-512
Message Digest Length	128	512
Attack(For original message From MD)	2^{128}	2^{512}
Attack(find two message for same MD)	2^{64}	2^{256}
Successful Attacks	Some attempt reported	No such claims
Speed	Faster	Slow
Software Implementation	Very easy	Easy

Comparision of digital signature algorithms

II. DIFFERENT ATTACKS USING TRADITIONAL CRYPTOGRAPHIC APPROACHES

a. Cipher text Attack

In this type of attack, the cryptanalyst has the cipher text of several messages and they have been encrypted using the same encryption algorithm. The job of cryptanalyst is to recover the plaintext as possible or could deduce the key(s) which is used to encrypt and decrypt the message.

b. Known-Plaintext Attack

In this type of attack, the cryptanalyst knows the encryption algorithm and cipher text to be deduced. Cryptanalyst's role is to deduce the key(s) used to encrypt the message or an algorithm to decrypt the new message encrypted with the same key(s).

c. Chosen-Plaintext Attack

In this type, the cryptanalyst has access not only to cipher text and associated plaintext for several data but also chooses the specific plaintext blocks to encrypt which yield more information about the key. Cryptanalyst job is to deduce the key(s) used to encrypt the messages or an algorithm to decrypt any new message encrypted with the same key(s).

d. Chosen-Cipher text Attack

In this attack, the cryptanalyst knows different cipher texts to be decrypted and has access to the decrypted plaintext. Cryptanalyst's job is to deduce the key.

e. Meet-in-the-middle attack

It is another type of known plaintext. The Meet-in-the middle attacker uses two different keys to encrypt the plaintext with a different combination of keys and decrypt the cipher text with another set of keys to get the necessary key to get the original message.

f. Man in the Middle Attack

This type of attack occurs when the secure socket layer (SSL) is not properly installed when two parties are communicating with each other then there is a possibility that all the data communication between two parties could be hacked by the middle party. Therefore countermeasures are required to be taken to protect the data from the middle attack.

g. Brute Force Attack

A brute force attack is a trial-and-error method used to obtain information such as a user password or Personal Identification Number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data.

h. Dictionary Attack

In this attack, every word in the dictionary is tried as a possible password for an encrypted message. A dictionary attack is generally more efficient than brute force attack.

i. Birthday attack

It is another class of brute-force attack which uses probability theory in a set of randomly selected people. A number of permutations are applied to get information from the communication among a set of people.

j. Pre-computation attack

The attacker makes a list of possible keys and compiles a look up table in order to decrypt the cipher text. One of the values in the look up table cracks the encrypted message. It is another class of dictionary attack.

k. Denial of service

In cloud computing, hacker attack on the server by sending thousands of requests to the server that server is unable to respond to the regular clients in this way server will not work properly. Counter measure for this attack is to reduce the privileges of the user that connected to a server. This will help to reduce the DOS attack.

l. Side Channel Attack

An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack. Side-channel attacks have emerged as a kind of effective security threat targeting system implementation of cryptographic algorithms. Evaluating a cryptographic system's resilience to side-channel attacks is therefore important for secure system design.

m. Network Sniffing

When the unencrypted data is send on the cloud through the network then the hacker can sniff the passwords from the data on transit.

n. Port Scanning

There may be some issues regarding port scanning that could be used by an attacker as Port 80(HTTP) is always open that is used for providing the web services to the user. Other ports such as 21(FTP) etc are not opened all the time it will open when needed therefore ports should be secured by encrypted until and unless the server software is configured properly. Counter measure for this attack is that firewall is used to secure the data from port attacks.

o. Sql Injection Attack

SQL injection attacks are the attacks where a hackers uses the special characters to return the data for example in SQL scripting the query end up with where clause that may be modified by adding more information in it.

p. Cross Site Scripting

It is a type of attack in which user enters the correct URL of a website and hacker on the other site redirects the user to its own website and gain access to its credentials. The aforementioned attacks weaken the security of encrypted data stored on cloud. Eventually, these attacks are the major barriers for a broader adoption of data outsourcing to cloud. Hence mitigating the threats, attacks and vulnerabilities is the vital factor to be considered in cloud storage in order to achieve data confidentiality.

III. PROPERTIES OF KEYLESS SIGNATURE INFRASTRUCTURE (KSI)

- **Massive Scale**

The massive scale of the KSI enables signing and verification of billions of data items every second. The KSI signatures can be generated at Exabyte-scale.

- **Portability**

The properties of the signed data can be verified even after that data has crossed geographic or organizational boundaries and service providers.

- **Quantum Immunity**

The cryptography behind the KSI signatures ensures that they never expire and remain quantum-immune i.e. secure even after the realization of quantum computation.

- **Independent Verification**

The properties of the signed data (time: when was the data signed, integrity: the underlying data has not changed, and order: which data was signed in which order) can be verified without reliance or need for a trusted authority.

- **Data Privacy**

KSI system is based on one-way cryptographic hash functions that result in hash values uniquely representing the data, but are irreversible such that one cannot start with the hash value and reconstruct the data - data privacy is guaranteed at all times.

- **Active Integrity**

The process of continuously verifying the integrity of electronic data for:

1) Detection whether data has not been manipulated,

2) Alerting in the event of detection,

3) Mitigation, either manual or automated in the event of an alert.

- **Attributable Network**

On an attributable network, every action can be traced back to an original source so that every user is legally responsible for their actions (non-repudiation).Attributable networks can be achieved using the TTL (Tag, Track, Locate) functionality of KSI by signing all digital asset ,so that they can be audited, independently from service providers and network administrators, based on forensically strong proof.

- **Clean State Proof**

The mathematical proof provided by KSI that a network is in a clean state and free of compromise. Once this state has been achieved it then becomes possible to continuously verify that the network remains in a clean state and act when a compromise is detected.

- **Forensic Audit ability**

The ability to conduct an audit that produces forensically sound and legally admissible evidence. The evidence is legally acceptable, and can be verified independently by a court or other third party.

- **Independent Verification**

It means that digital evidence can be verified without reliance on chain of custody, security of keys or any trusted human.

- **Information Assurance**

Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data.

- **Mutual Audit ability**

Mutual Audit ability means that in a networked environment it is possible for an administrator to prove to a user, in the event of a dispute, that their actions were their own and not the administrator's.

- **Portability of Evidence**

Evidence portability means that data can be independently authenticated, no matter where it travels.

IV. CONCLUSION

Keyless Signature Infrastructure is designed to provide digital signature based authentication for data, traditional approaches that depend on public cryptography or asymmetric key cryptography, KSI uses only hash-function cryptography, allowing verification to rely on the security of hash- functions. The proposed Keyless Signature Infrastructure (KSI) technology invokes one-way hashes that cannot be broken, even under attack from the theoretical capabilities of quantum computers. KSI uses formal mathematical methods to independently authenticate any type of electronic data, at scale, in real time, without the need of trusted keys, cryptographic secrets, or credentials that can be compromised. Privacy is assured. With KSI, digital assets acquire immutable properties with forensic proof for provenance, security and integrity.

V. REFERENCES

[1] **“**Enhancing Cloud Data Security Using Elliptical Curve Cryptography” Ms. Nikita N Chintawar , Ms. Sonali J Gajare , Ms. Shruti V Fatak , Ms. Sayali S Shinde , Prof. Gauri Virkar, IJARCCE, Vol. 5, Issue 3, March 2016.

[2] “An investigation on the Techniques used for encryption and authentication for Data Security in Cloud computing”, Tamilarasi Rajamani, PrabuSevugan, Swarnalatha Purushotham, ISSN: 0976-3104

[3] “Security Issues and Use of Cryptography in Cloud Computing”, Jashanpreet Pal Kaur , Rajbhupinder Kaur, Volume 4, Issue 7, July 2014 ISSN: 2277 128X

[4] “Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage”, Dr. S. S. Manikandasaran, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol.6, No1, Jan-Feb 2016

[5] “Secure Attribute Based Partitioning Technique for Cloud Structural Storage Data- A Review”, Miss. Snehal Asare1 , Prof. Fazeel Zama, IJCSMC, Vol. 4, Issue. 12, December 2015.

I.