International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 2, Mar-April-2021, ISSN (Online): 2395-566X

Security in ad-hoc network using encrypted data transmission and Steganography

Prof. Ravindra Ghugare, Ankita Patil, Ajay Jha, Dhiraj Kuslekar
Department of Computer Science Engineering
Bharati Vidyapeeth College of Engineering, Navi Mumbai, India.

Abstract- Currently, there has been an increasing trend in outsourcing data to remote cloud, where the people outsource their data at Cloud Service Provider(CSP) who offers huge storage space with low cost. Thus users can reduce the maintenance and burden of local data storage. Meanwhile, once data goes into cloud they lose control of their data, which inevitably brings new security risks toward integrity and confidentiality. Hence, efficient and effective methods are needed to ensure the data integrity and confidentiality of outsource data on untrusted cloud servers. Thepreviously proposed protocols fail to provide strong security assurance to the users. In this paper, we propose an efficient and secure protocol to address these issues. Our method allows third party auditor to periodically verify the data integrity stored at CSP without retrieving original data. To compare with existing schemes, our scheme is more secure and efficient.

Keywords- Least Significant Bit, Steganography, Cryptography, Cloud Service Provider, Elliptical Curve Cryptography.

I. INTRODUCTION

With the invention of Storage, the days of keeping all your documents, photos, music files etc. on your computer's hardware are gradually coming to a close. Today, the storage is fulfilling the need for more storage space to hold all of your digital data. Storage space providers operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them.

The data center operators, in the background, virtualizes the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects. Physically, the resource may span across multiple servers. Storage can be used from smaller computing devices to desktop computers and servers. Storage services may be accessed through a web service API or through a Web-based user interface. The storage architectures build a single virtual storage system. The data when stored on Storage space has the following threats:

1. When data is distributed, it is stored at multiple locations increasing the risk of unauthorized physical access to the data.
2. The number of people with access to the data who could be compromised (i.e. bribed or coerced) increases dramatically.
3. It increases the number of networks over which the data travels. Instead of just a local area network (LAN) or storage area network (SAN), data stored on a Storage space requires a WAN (wide area network) to connect them both.
4. Sharing of storage and networks with many other users/customers it is possible for other customers to access your data.

To secure data, most systems use a combination of techniques, including:

1. Encryption, which means they use a complex algorithm to encode information. To decode the encrypted files, a user needs an encryption key. While it's possible to crack encrypted information, most hackers don't have access to the amount of computer processing power they would need to decrypt information.
2. Authentication processes, which require creating a user name and password.
3. Authorization practices -- the client lists the people who are authorized to access information stored on the storage system.

Many corporations have multiple levels of authorization. For example, a front-line employee might have very limited access to data stored on a storage system, while the head of human resources might have extensive access to files. Storage approach poses a potential security threat to your data and moreover, only the password access to storage is not sufficient as the password can be hacked by an intruder.

Also the data can be captured en-route to the storage services. The need to access storage on thin clients and mobile devices is becoming an emerging application. But due to smaller processor speed and run time memory; these devices need an algorithm which can be used in such small computing devices. Security of stored data and data in transit may be a concern when storing sensitive data at a storage space provider.

© 2021 IJSRET

II. RELATED WORK

RSA algorithm is the most widely used public key cryptography algorithm for encryption and decryption by many vendors today. This is the first generation algorithm that was used for providing data security. It can be used to encrypt a message without the need to exchange a secret key separately. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. Party A can send an encrypted message to party B without any prior exchange of and B decrypts it using the private key, which only he knows. RSA can also be used to sign a message, so A can sign a message using their private key and B can verify it using A's public key.

Encryption of a message, m, involves exponentiation, c = me mod n, which requires a lot of mathematical computations. In RSA cryptosystem, user A (say Alice) picks up two large primes p and q and computes their product, n = p*q. Now Alice's public key is a pair of integers {n, e} and the private key is d.
Key Generation:
INPUT: Security parameter l.
OUTPUT: RSA public key (n, e) and private key d.
1. Select two primes p and q of the same bit length l/2.
2. Compute n = p*q and φ = (p−1)*(q −1).
3. Select arbitrary integer e with 1 < e <φ and gcd(e, φ) = 1.
4. Compute integer d satisfying 1 < d <φ and e*d ≡ 1 (mod φ).
5. Return (n, e, d).
Encryption:
INPUT: RSA public key (n, e), plaintext m ∈ [0, n−1].
OUTPUT: Cipher text c.
1. Compute c = me mod n.
2. Return(c).
Decryption:
INPUT: Public key (n, e), private key d, cipher text c.
OUTPUT: Plaintext m.
1. Compute m = cd mod n.
2. Return (m).

III. LITERATURE SURVEY

Cloud storage is a model of networked enterprise storage where data is stored not only in the user's computer, but in virtualized pools of storage which are generally hosted by third parties. Ravi Shankar Dhakar et al [17] talk about the "Modified RSA Encryption Algorithm (MREA)" where the talk about factorization in RSA cryptosystem, and their implementation compares the existing system and their system with key sizes up to 1024 bit. The authors claim their system to be better than existing system for the brute-force attack. Suli Wang et al [18] talk about the "File encryption and decryption system based on RSA algorithm" where theyused RSA for encryption and decryption of files with smaller sizes. Maryam Savari et al [19] in "Comparison of ECC and RSA Algorithm in Multipurpose Smart Card Application" compare the security of RSA 1024-bit key versus ECC 160- bit key sizes. P.R. Vijayalakshmi et al [20] in "Performance Analysis of RSA and ECC in Identity-Based Authenticated New Multiparty Key Agreement Protocol" compare ECC algorithm with 128 bits with that of RSA algorithm with 1024 bits key size. Kamlesh Gupta et al [21] in "ECC over RSA for Asymmetric Encryption: A Review" demonstrated the use ECC for portable devices and applications. Arjun Kumar et al (22) propose a method that allows user to store and access the data securely from the cloud storage in "Secure Storage and Access of Data in Cloud Computing". Xiao Zhang et al (23) talk about the physical security of data in data centers "Ensure Data Security in Cloud Storage". Somani, U et al (24) proposed implementation digital signature with RSA algorithm to enhance data security in cloud storage. Chakraborty, T.K et al (25) proposed a model for data security in cloud. Over last 10 years, a great deal of work has taken place to ensure that ECC meets these goals and is specified in an ever-increasing number of standards. It started with the IEEE P1363 in 1994 (becoming a standard in 2000), and now includes many accredited standards organizations:
i) ISO (in ISO 14888-3: ECDSA and other ECC-based signature schemes)
ii) IEEE (in IEEE 1363-2000 for public-key cryptography)
iii) The American National Standards Institute (in ANSI X9: cryptography for financial-services industry).

NIST also specifies ECC in FIPS 186-2: Federal Information Processing Standards ECDSA and SP 800-56: Special Publication on Key management. While in Europe, BSI in Germany also specifies ECC. Though there are several papers published on the comparison of ECC and RSA in terms of key sizes and security, this paper talks about the reduced key generation time, comparison of encrypted file (cipher text) cloud storage. The simulation system provides the key sizes of up to 15360 bits. In this work the used file sizes are up to 40 MB for the simulation i.e. encryption and decryption. This work compares the security of ECC in the key range of 160 - 512 bits and RSA key sizes ranging from 512 - 3072 bits. The simulation experiments compare the ECC and RSA at different levels of key sizes and block sizes.

IV. CONCLUSION

Elliptic Curve Cryptography is more safe and reliable than first-generation public key techniques like RSA, which are currently in use. When it comes to upgrading their systems, vendors should seriously consider the elliptic curve option because of the computational and bandwidth benefits it provides while maintaining comparable security. Although the security of ECC has not been fully assessed, it is expected to be widely used in the future in a variety of fields. When comparing the RSA and ECC cyphers, it was discovered that ECC has significantly

© 2021 IJSRET

lower overheads than RSA. Since it can have the same degree of protection as RSA by using shorter keys, the ECC has a lot of advantages. However, one flaw that could obscure its appeal is its lack of maturity, as mathematicians conclude that not enough research has been done in ECC. Since today's applications (smart cards, pagers, and cellular telephones, for example) cannot bear the overheads introduced by RSA, ECC appears to have a better future than RSA. ECC can be used for encryption and decryption in today's small computing devices because it needs smaller key sizes and has less computing complexity than RSA. As a result, ECC is an excellent option for compact, mobile, and low-power applications, as well as cloud integration. The time taken by the two algorithms for key generation and encryption is compared in this paper. The significance of this research is that it demonstrates the use of the ECC algorithm in cloud storage, which provides improved protection. This research can be expanded to equate ECC with other algorithms for digital signatures, key exchanges, and data integrity.

REFERENCES

[1] Study on Watermarking Techniques in Digital ImagesPurnima Pal1 M.Tech (Communication Engineering) KNIT Sultanpur purnima22pal@gmail.com Harsh Vikram Singh2 Associate Prof.2(Electronics Department) KNIT Sultanpur harshvikram@gmail.com Sarvesh Kumar Verma3 M.Tech3(Communication Engineering) KNIT Sultanpur sarvesh24816@gmail.com3

[2] A Robust Double-Blind Secure High Capacity Watermarking and Information Hiding Scheme For Authentication and Tampering Recovery Via the Wavelet and Arnold Transforms S. Swapnil and D. B. Megherbi - Center forComputer Man/Human Intelligence Networking and Distributed Systems (CMINDS),Department of Electrical and Computer Engineering, University of Massachusetts, Lowell, MA

[3] An Invisible WatermarkingTechnique ForImage Verification. Minewa M. Yeung and Fred Mintzer-IBM T.J. Watson Research Center, Yorktown Heights, NY 10598. {yeung,mintzer} @ watson.ibm.com

[4] Elliptic curve cryptography, https://en.wkipedia.org/wiki/Elliptic_curve_cryptography

[5] RSA (algorithm), http: //en.wikipedia.og/wiki/RSA_(algorithm)

[6] JavaTM Cryptography Extension (JCE), Reference Guide.http://docs.oracle.com/javase/1.5.0/docs/guide/security/jce/JCE RefGuide.html

© 2021 IJSRET