International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 2 | ISSN : 2456-3307

Security Framework for Receiving of Data Using Digital Signature Algorithm

Gopi. A[1], P. Sireesha[2]
[1]Student, Deaprtment of MCA, RCR Institution of Management & Technology, Tirupathi, India.
[2]Assistant Profeesor, Deaprtment of MCA, RCR Institution of Management & Technology, Tirupathi, India

ABSTRACT:
Cloud computing is getting more prominent in the field of software engineering in view of its unwavering quality in putting away and evaluating information remotely. In the nearness situation it is extremely biter to have cell phones as an interface amongst client and server, to access and store information for one's need. Versatile innovation in cloud processing is encourages clients to work on the information for any of the application for their association in versatility. In these viewpoints versatile distributed computing is our current theme of enthusiasm as it is extremely important to secure the information away and access since the transportation of the information is through generally by open system. In this venture the versatile cloud condition is utilized for putting away and evaluating information and along these lines it is needed an effective cloud arrange that is a system for correspondence furthermore, information validation. For verification it is indispensable to outline a security system for portable cloud condition that guarantees better verification of information in the cell phones and in the capacity gadgets. We propose another security structure for accepting of information utilizing the idea of advanced mark.

Keywords: Cloud computing, Security, Digital Signature Algorithm, Cloud Service Provider, Hash

INTRODUCTION:

The most recent utility oriented distributed computing model that has envisioned an immense transformation of Information Technology (IT), to increase capacities of the client access to a common pool of platforms, applications and infrastructures without having to really claim them in distributed computing. In the context of deployment, the cloud computing is grouped into four approaches: (i) public, (ii) private, (iii) hybrid and (iv) community clouds that are described below:

- Public Cloud: In public cloud, the service suppliers transfer various applications as service and encourage the customers by offering access to the resources by means of concentrated distributed servers over the Internet for example, Amazon Web Services, Google App Engine.
- Private Cloud: The services and framework are utilized and supervised absolutely by a performance institution.
- Community Cloud: The services and framework are distributed by an arrangement of institutions that are overseen either privately or by a dependable outsider.
- Hybrid Cloud: Hybrid cloud adopts a blend of on-premises, private cloud

and third-party public cloud services with arrangement among the two platforms.

Security is an important factor in cloud computing, for ensuring clients data is placed on the secure mode in the cloud. Data must not be stolen by the third party, so authentication of client becomes a mandatory task. Here the main issue authentication is discussed. In this paper proposed data authentication to secure data of encryption algorithm with digital signature in mobile cloud computing. If a mobile user has uploaded the files on cloud server for sharing with multiple users, there should be a mechanism to verify the originator of the file. The authentication mechanism may help to verify the originator of the file.

Advanced marks are fundamental in the present current world to confirm the sender of a record's character. A computerized mark is spoken to in a PC as a string of double digits. This mark is PC utilizing an arrangement of standards and parameters (calculation) with the end goal that the character of the individual marking the archive and additionally the creativity of the information can be confirmed. The mark is confirmed makes utilization of a open key which relates to (however not the same, i.e. scientifically infeasible to identify private key from open) the private key. With each client having an open/private key match, this is a case of open key cryptography. Open keys, which are known by everybody, can be utilized to check the mark of a client. The private key, which is never shared, is utilized as a part of mark age, which must be done by the client.

There are three algorithms that are suitable for digital signature generation under the DSS standard. They are Digital Signature Algorithm (DSA), the RSA algorithm, and the Elliptic Curve Digital Signature Algorithm (ECDSA). Also in this standard is a hash function to be used in the signature generation process. It is used to obtain a condensed version of the data, which is called a message digest. This message digest is then put into the digital signature algorithm to generate the digitally signed message. The same hash function is used in the verification process as well. The hash function used in the DSS standard is specified in the Secure Hash Standard (SHS), which are the specifications for the Secure Hash Algorithm (SHA). The SHA is based on principles similar to those used MIT when designing the MD4 message digest algorithm and is closely modeled after that algorithm. When a message of any length $< 2^{64}$ bits is input, the SHA produces a 160-bit output (message digest). Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message.

Algorithm:

DSA Parameters:

p = a prime modulus, where $2L-1 < p < 2L$ for $512 \leq L \leq 1024$ and L is a multiple of 64. So L will be one member of the set {512, 576, 640, 704, 768, 832, 896, 960, 1024}

q = a prime divisor of p-1, where $2^{159} < q < 2^{160}$
$g = h^{(p-1)/} q \bmod p$, where h is any integer with $1 < h < p-1$ such that $h^{(p-1)/} q \bmod p > 1$ (g has order q mod p)
x = a randomly or pseudo randomly generated integer with $0 < x < q$
$y = g^x$ 1-> p
k = a randomly or pseudo randomly generated integer with $0 < k < q$
The parameters p, q, and g are made public. The users will have the private key, x, and the public key y. The parameters x and k are used for signature generation and must be kept private and k will be randomly or pseudo randomly generated for each signature. This part seems to be straightforward so far.
The signature of the message M will be a pair of the numbers r and s which will be computed from the following equations.
$r = (g^k \bmod p) \bmod q$ -> 2
$s = (k\text{-}1(SHA(M) + xr)) \bmod q$ ->3
k^{-1} is the multiplicative inverse of k (mod q). The value of SHA(M) is a 160-bit string which is converted into an integer according to the SHS standard. Then the signature is sent to the verifier.

Verification:

Before getting the digitally signed message the receiver must know the parameters p, q, g, and the sender's public key y.
From original content digital signature is created with the help of recipient private key. It's a secret key. Signing algorithm is implemented to sign on content. Message is authenticated using sender private key. Signing algorithm is used for both data encryption and data decryption.

In this paper, for auditing purpose DSA algorithm is used. Digital signature is responsible for the authentication and we use SHA as a hashing algorithms for the computing the signature.

Encryption operation:

1. User can generate the message digest using the SHA hashing algorithms and sign on plain text.
2. Now the data is encrypted using the DSA encryption algorithms with secret key.
3. The computing server now verifies the signature and stored the file to the storage server.

Decryption operation:

1. Computing server retrieve the file from storage server according to the user request.
2. Now perform the decryption operation and extract the signature.
3. Now compute the signature and verify it. If it is successfully verified then data is stored at the client side otherwise modification is detected and data is stored at the client side.

CONCLUSION

In this paper, verification process is examined. For confirm the proprietor of the information and to locate the first information DSA calculation is utilized. For secure verification cryptography strategy is executed. Computerized signature calculation create signature for plain content. Hash work is used to encode the plain content. Utilizing keys encoding and unraveling process is finished. After sign on the plain content Computerized

signature motor review the information. Check process is produced. On the off chance that the information is unique at that point create declaration else no. At that point information is come back to cloud specialist organization. Utilizing advanced mark calculation, information from cloud is checked.

REFERENCES

1. Lysyanskaya, A. R. Tamassia and N. Triandopoulos, 2004. Multicast Authentication in Fully Adversarial Networks, Proc. IEEE Symp. Security and Privacy (SP '04), pp: 241-253.
2. Miner, S. and J. Staddon, 2001. Graph-Based Authentication of Digital Streams', Proc. IEEE Symp. Security and Privacy (SP '01), pp: 232-246.
3. Udayakumar, R., V. Khanna, T. Saravanan and G. Saritha, 2013. Retinal Image Analysis Using Curvelet Transform and Multistructure Elements Morphology by Reconstruction, Middle-East Journal of Scientific Research, ISSN: 1990-9233, 16(12): 1798-1800.
4. Sibghatullah Nasir, 2013. Microfinance in India Contemporary Issues and Challenges. Middle-East Journal of Scientific Research, 15(2): 191-199.
5. Mueen Uddin, Asadullah Shah, Raed Alsaqour and Jamshed Memon, 2013. Measuring Efficiency of Tier Level Data Centers to Implement Green Energy Efficient Data Centers, Middle-East Journal of Scientific Research, 15(2): 200-207.
6. Hossein Berenjeian Tabrizi, Ali Abbasi and Hajar Jahadian Sarvestani, 2013. Comparing the Static and Dynamic Balances and Their Relationship with the Anthropometrical Characteristics in the Athletes of Selected Sports, Middle-East Journal of Scientific Research, 15(2): 216-221.
7. Anatoliy Viktorovich Molodchik, 2013.
8. Meruert Kylyshbaevna Bissenova and Ermek Leadership Development. A Case of a Russian Talantuly Nurmaganbet. The Notion of Guilt and Business School, Middle-East Journal of Scientific Problems of Legislative Regulations of its Forms. Research, 15(2): 222-228. The Notion of Guilt in the Criminal Law of Kazakstan, Middle-East Journal of Scientific Research, 15(2): 229-236.
9. Somani, Uma, Kanika Lakhani, and Manish Mundra. "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing." Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on. IEEE, 2010. [10] Hashizume, Keiko, et al. "An analysis of security issues for cloud computing." Journal of Internet Services and Applications 4.1 (2013): 1-13.
10. Rani, Sunita, and Ambrish Gangal. "Cloud security with encryption using hybrid algorithm and secured endpoints." International journal of computer science and information technologies 3.3 (2012): 4302-4304.
11. Saravanan, N., et al. "An implementation of RSA algorithm in google cloud using cloud SQL." Research Journal of Applied Sciences, Engineering and Technology 4.19 (2012): 3574-3579.
12. Kumar, K. Vijay, Dr N. Chandra Sekhar Reddy, and B. Srinivas Reddy. "Preserving Data Privacy, Security Models and Cryptographic Algorithms in Cloud Computing." International Journal of Computer Engineering and Applications 7.1 (2015).
13. V. Vinaya, and P. Sumathi, "Implementation of Effective Third Party Auditing for Data Security in Cloud", International Journal of

Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, pp. 382-387, May 2013.s

14. C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services" IEEE Network, vol. 24, no.4, pp. 19-24, 2010.
15. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing", IEEE INFOCOM, pp. 1-9, March 2010.
16. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing". IEEE Transactions on Services Computing, vol.5, no.2, pp.220-232, 2012.
17. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing" IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.
18. K. Yang, and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", IEEE Transactions on Parallel & Distributed Systems, vol. 24, no. 9, pp. 1717-1726, 2012.
19. Y. Zhu, H. Hu, G.-J. Ahn, and S. S. Yau, "Efficient audit service outsourcing for data integrity in clouds," In Journal of Systems and Software, vol. 85, no. 5, pp. 1083-1095, May 2012.