CLOUD BASED AUTHENTICATION SYSTEM

VISHAL SASWADE

Abstract- "Cloud" is a virtualized pool of computing resources. Cloud computing has been around for over some years in different forms. However the third generation trend in IT industry is now ruled over by cloud computing. Cloud computing is an Internet based resource sharing methodology wherein data and resources are shared and integrity of data, resources have become prime concern.Access to intruders can be restricted by providing username and password as first level authentication. In our proposed work we have tried to minimize the loop holes related to the security and the authentication of the user in an organization by providing multi level authentication (User ID , Password and MAC Address) encrypted in digital certificate.

Key Terms- cloud, encryption, security, algorithm, cryptography

I. INTRODUCTION

Cloud computing is an Internet based resource sharing methodology wherein data and resources are shared and integrity of data, resources have become prime concern. Access to intruders can be restricted by providing username and password as first level authentication. In our proposed work we have tried to minimize the loop holes related to the security and the authentication of the user in an organization by providing multi level authentication (User ID , Password and MAC Address) encrypted in digital certificate.

Cloud Based Authentication

In this paper we have implemented a new security architecture model for cloud computing platform. In this model multi level authentication technique is used for giving secured access to a cloud user. Here credentials are encrypted into a digital certificate with AES algorithm in which keys are generated randomly by the system. In our proposed model multi factor authentication is used, thus ensuring higher security. This model also helps to solve main security issues like malicious intruders, hacking, etc. in cloud computing platform.

Comparison between RSA , Blowfish algorithms.

The RSA algorithm is used for secured communication between the users and the servers. Blowfish is also a block cipher[5], meaning that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. Current authentication model (Consolidated Architecture Model) enables smart devices to perform user authentication by using user certificate stored in the devices. It requires web browser such as Internet Explorer, Opera, Safari, Firefox, Chrome etc. Furthermore, this model is designed not to reveal the sensitive data such as digital signature information to Auth Server through end-to-end encryption which ensures its secure delivery between service provider and smart device. [*] However this model does not store Machine Address Code of the device. By adding the MAC to the certificate, we can ensure that user is bonded to use the exact same machine which is assigned to him/her by the administrator.

Blowfish consists of two parts: key-expansion and data encryption. During the key expansion stage, the inputted key is converted into several sub key arrays total 4168 bytes. There is the P array, which is eighteen 32-bit boxes, and the S-boxes, which are four 32-bit arrays with 256 entires each. After the string initialization, the first 32 bits of the key are XORed with P1 (the first 32-bit box in the P-array). The second 32 bits of the key are XORed with P2, and so on, until all 448, or fewer, key bits have been XORed. Cycle through the key bits by returning to the beginning of the key, until the entire P-array has been XORed with the key. Encrypt the all zero string using the Blowfish algorithm, using the modified P-array above, to get a 64 bit block. Replace P1 with the first 32 bits of output, and P2 with the second 32 bits of output (from the 64 bit block). Use the 64 bit output as input back into the Blowfish cipher, to get a new 64 bit block. Replace the next values in the P-array with the block. Repeat for all the values in the P-array and all the S boxes in order.

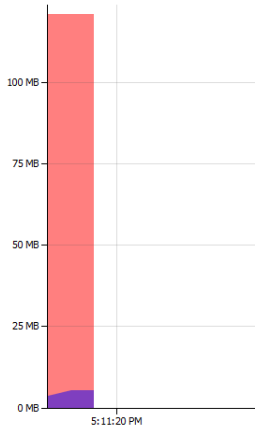


Fig 1.BlowFish Algorithm

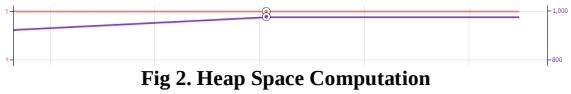
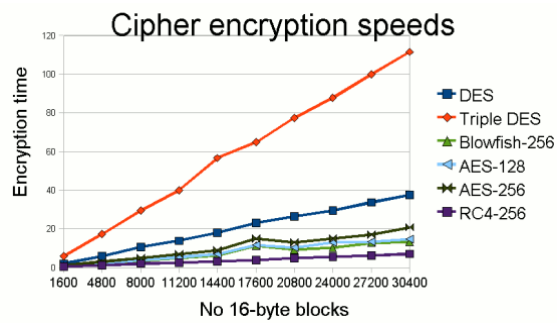


Fig 2. Heap Space Computation



Comparison between DES, TRIPLE DES, BLOWFISH – 256

II. PROPOSED SYSTEM

This system basically uses the Blowfish encryption algorithm [1] to encrypt the data file. This algorithm is a 64-bit block cipher with a variable length key. This algorithm has been used because it requires less memory. It uses only simple operations, therefore it is easy to implement. It is a 64 bit block cipher and it is fast algorithm to encrypt the data. It requires 32 bit microprocessor at a rate of one byte for every 26 clock cycles. It is variable length key block cipher up to 448 bits. Blowfish contains 16 rounds. Each round consists of XOR operation and a function. Each round consists of key expansion and data encryption. Key expansion generally used for generating initial contents of one array and data encryption uses a 16 round Feistal network[3].

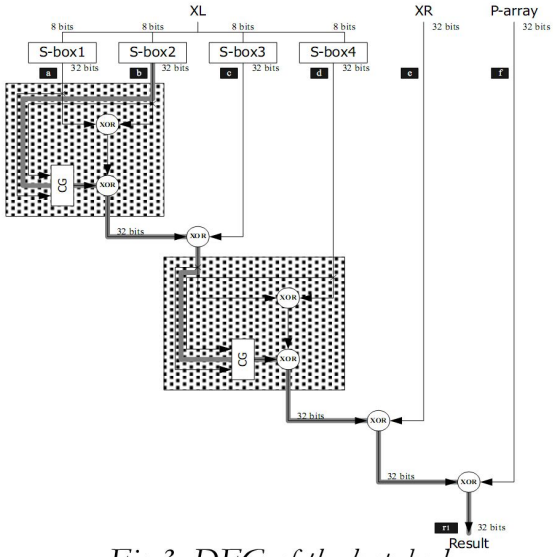


Fig 3. DFG of the loop body

Private Key

Public key encryption requires that a public key and a private key be generated for an application. Data encrypted with the public key can only be decrypted using the corresponding private key. Data encrypted with the private key can only be decrypted using the corresponding public key. The private key is stored in a key database file that is password-protected. Only the owner of the private key can access the private key to decrypt messages that are encrypted using the corresponding public key.

The issuer of the certificate signs it with a digital signature to verify its authenticity. This signature is compared to the signature on the corresponding CA certificate to verify that the certificate originated from a trusted certificate authority.

ALGORITHM STEPS:

It is having a function to iterate 16 times of network. Each round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round.

Algorithm

Divide x into two 32-bit halves: xL, xR
For i = 1to 32:
xL = XL XOR Pi
xR = F(XL) XOR xR
Swap XL and xR
Swap XL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR

Definition and Basic Scheme

We have proposed new security architecture model for cloud computing platform. In this model multi level authentication technique is used for giving secured access to a cloud user. Here credentials are encrypted into a digital certificate with AES algorithm in which keys are generated randomly by the system. In our proposed model multi factor authentication is used, thus ensuring higher security. This model also helps to solve main security issues like malicious intruders, hacking, etc. in cloud computing platform. The RSA algorithm is used for secured communication between the users and the servers.

CONCLUSION

The proposed algorithm of the Blowfish can achieve efficient data encryption up to 4 bits per clock. In this design, we avoid I/O limited constraint by modifying the I/O from 64 bits to 16 bits. The proposed architecture should satisfy the need of high-speed data encryption and can be applied to various devices respectively.

REFERENCES

[1] Bruce Schneier, "Applied Cryptography", John Wiley & Sons, Inc. 1996

[2] The homepage of description of a new variable-length key, 64-bit block cipher http://www.counterpane.com/bfsverlag.html

[3] Patterson and Hennessy, “Computer Organization & Design: The Hardware/ Software Interface”, Morgan Kaufmann, Inc. 1994

[4] B. Schneier, "Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish)," Fast Software Encryption: Second International Workshop, Leuven, Belgium, December 1994, Proceedings, Springer-Verlag,1994, pp.191-204.

[5] S. Vaudenay, "On the Weak Keys in Blowsh," Fast Software Encryption, Third International Workshop Proceedings, Springer-Verlag, 1996, pp. 27-32.

[6] P. Karthigai Kumar and K. Baskaran. 2010. An ASIC implementation of low power and high throughput blowfish crypto algorithm. Microelectron. J. 41, 6 (June 2010), 347-355.

[7] E. Mykletun, M. Narasimha, and G. Tsudik, “Authentication and integrity in outsourced databases,” Trans. Storage, vol. 2, no. 2, pp. 107–138, 2006.

[8] Bo Wang, HongYu Xing IEEE - The Application of Cloud Computing in Education Informatization, Modern Educational Tech... center .

[9] NIST Definition http://www.au.af.mil/au/awc/awcgate/nist/cloud-defv15.doc

[10] CA Technologies cloud authentication system http://www.ca.com/us/authentication-system.aspx

[11] X. Suo, Y. Zhu, G. S. Owen, “Graphical passwords: A survey,” in Proc. 21st Annual Computer Security Application. Conf. Dec. 5–9, 2005, pp. 463–472.

[12] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, “Authentication using graphical passwords: Basic results,” in Proc. Human-Comput. Interaction Int., Las Vegas, NV, Jul. 25–27, 2005.

[13] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik,“Three-Dimensional Password for More Secure Authentication,” IEEE, http://ieeexplore.ieee.org., Last Updated – 6 Feb 2008

[14] Cloud Computing services & comparisons http://www.thbs.com/pdfs/Comparison%20of%20Cloud%20computing%20services.pdf

[15] A User Identity Management Protocol for Cloud Computing Paradigm Safiriyu Eludiora1, Olatunde Abiona2, Ayodeji Oluwatope1, Adeniran Oluwaranti1, Clement Onime3,Lawrence Kehinde apered in Int. J. Communications, Network and System Sciences, 2011, 4, 152-163

★★★