Volume No:3, Issue No:1 (June-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

A Novel Hybrid Authentication Based Key Exchange Protocol for Secure Transmission

Jami Harika
M.Tech Scholar,
Dept of CSE,
AITAM, Tekkali, Srikakulam, AP, India.

Dr.U.D. Prasan
Professor,
Dept of CSE,
AITAM, Tekkali, Srikakulam, AP, India.

ABSTRACT:
Key Exchange or generation protocol is always an interesting research issue in the field of network security and secure computing. Even though we have various traditional centralized and de-centralized approaches available, every model has its own advantages and disadvantages. In this work, we are proposing a novel key exchange protocol and data confidentiality model for secure transmission. Every user can communicate with cloud storage easily without implementing any key based protocols. Hybrid authentication based key exchange protocol improves the authentication and generates secure authentication code to provide security for data. Our proposed implementation shows more efficient results than traditional approaches.

I.INTRODUCTION:
Cloud computing is an internet based resource that provides huge amount of storage, software and search engine services etc. It provides user to store their confidential data with secure methods. Cloud Computing means a remote server that access through the internet which helps in business applications and functionality along with the usage of computer software. Cloud computing saves money that users spend on annually or monthly subscriptions. Organizations, companies store more and more valuable information is on cloud to protect their data from virus, hacking. The benefits of the new computing model include but are not limited to: relief of the trouble for storage administration, data access, and avoidance of high expenditure on hardware mechanism, software, etc.

Besides, in Cloud Computing, data owners may share their outsourced data with many users, who might want to only retrieve certain specific data files they are interested in during a given session. One of the most popular ways to do so is through keyword-based search. This keyword search technique allows users to selectively retrieve files of interest and has been widely applied in plaintext search scenarios. Unfortunately, data encryption, which restricts user's ability to perform keyword search and further demands the protection of keyword privacy, makes the traditional plaintext search methods fail for encrypted cloud data. Some different advantages to clients incorporate versatility, dependability, and effectiveness. Versatility implies that cloud computing offers boundless preparing and capacity limit.

The cloud is dependable in that it empowers access to applications and records any place on the planet by means of the Internet. Cloud computing is regularly viewed as effective because it enables association to free up assets to concentrate on advancement and item improvement. Cloud computing will empower more adaptable IT procurement and changes, which may allow acclimations to systems in view of the affectability of the information. Broad utilization of the cloud may likewise support open models for cloud computing that will build up pattern information security highlights basic crosswise over various administrations and suppliers. Security can enhance because of centralization of information, expanded security-centered assets, and so forth., yet concerns can endure about loss of control over certain touchy information, and the absence of security for put away parts.

Volume No:3, Issue No:1 (June-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Security is regularly in the same class as or superior to other conventional frameworks, to some extent since specialist co-ops can commit assets to fathoming security issues that numerous clients can't stand to handle or which they do not have the specialized abilities to address. However, the intricacy of security is extraordinarily expanded when information is appropriated over a more extensive zone or over a more prominent number of gadgets, and in addition in multi-occupant frameworks shared by disconnected clients. Also, client access to security review logs might be troublesome or incomprehensible. Private cloud establishments are to some extent roused by clients' yearning to hold control over the framework and abstain from losing control of data security.

III.RELATED WORK:

The usage of various authentication methods and features is to prove the identity is based on the property that an unauthorized factor is unlikely to be able to supply the factors required for access control. If, in an authentication attempt, at least one of the components is missing or supplied incorrectly, the user's identity is not established with sufficient certainty and access to the asset. Cloud computing may also allow for better audit trails. In addition, information in the cloud is not as easily lost (when compared to the paper documents or hard drives, for example). While there are benefits, there are privacy and security concerns too. Data is travelling over the Internet and is stored in remote locations. In addition, cloud providers often serve multiple customers simultaneously.

All of this may raise the scale of exposure to possible breaches, both accidental and deliberate. Given that the organization exchanging this data to the supplier is eventually responsible for its assurance, it needs to guarantee that the individual data is suitable taken care of. There are diverse cases of cloud computing like Email correspondence now assumes a focal part in the majority of our bustling lives.

We convey a versatile WI-FI-empowered tablet with us wherever we go or utilize push email on our wireless, having an email customer sitting on our PC at home implies that while all over the place us chance investing energy outside of the correspondence circle. This is one range where the cloud discovers it’s most continuous and valuable application. The far-reaching usage of the TCP/IP convention stack and the resulting promotion of the web have prompt multi-seller organizes that are at no time in the future constrained by organization dividers. Cloud computing in a general sense considers a practical detachment between the assets utilized and the user PC. The computing assets could possibly dwell outside the nearby arrange, for instance in a web associated server farm. What is essential to the individual client is that they simply work. This division between the assets utilized and the user PC moreover has taken into consideration the improvement of new plans of action. Cloud computing refers to the provision of computational resources on demand via a computer network. Because the cloud is the underlying delivery mechanism, cloud based applications and services may support any type of software application or service in use today. Before the advent of computer networks, both data and software were stored and processed on or near the computer.

IV. PROPOSED WORK:

In our work, we proposed Hybrid authentication and reducing of data processing. The process of method is divided into two parts. First one is authentication and second one is data transmission. Authentication takes more time to execute the protocol because it is the complex process to give access control of our system. In the study of the existing methods cryptographic techniques and key exchange protocol are very basic protocols which is easily breakable in the networks and less security. In the elgamal scheme there is problem with the hash algorithms leads to more calculation complexity and the takes more processing time. So, we introduced a highly secured.

Volume No:3, Issue No:1 (June-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

In used Symmetric password based key exchanging protocol and Advanced Standard Encryption cryptographic scheme and random value based method is used to provide security for the data and the client authentication.Two servers maintain this authentication and cryptography. One server for authentication and another server for cryptography. By using we can reduce more hacking problems in the network. Client and servers share the public property and communicate with each other.

Algorithm: Hybrid authentication and data exchange algorithm:

Registration:

For every user in the system have to register in to server. When user send a request to store/retrieve data from cloud, we designed a method that is random value based protocol that processes the key exchange between the user and the first server.

Algorithm:

Input: user Id 'UId', random number 'R'

Algorithm:

Step 1: - User select a random number R and sends to server S1.

Step 2: - Sever S1 generates key.

Sever selects a random numbers Q1 and random numbers Q2

Send these two random numbers to User 'UId'.

Step3: - User reveals the secret key Sk=(R*Q1)+Q2

After generating this key user uses this key for encrypting the text.

Encryption and Decryption:

AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext.

The number of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

1. Key Expansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. Initial Round
   2.1. Add Round Key—each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds
   3.1. Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
   3.2. Shift Rows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
   3.3. Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
   3.4. Add Round Key
4. Final Round (no Mix Columns)

Volume No:3, Issue No:1 (June-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

4.1. Sub Bytes
4.2. Shift Rows
4.3. Add Round Key.

Verification:

For verification purpose, we used secure code for authentication at the time of retrieving and storing the information in the second server S2. At the time of the user request First server sends secure code to the user through mail. After entering the code, it verifies the user and grants privileges to users.

IV.CONCLUSION

In our work, we introduced that combines with cryptographic properties with secure storage. Our structure presents secure information reviewing for numerous proprietors and Upload their information in outsider server. By utilizing our strategy, we can diminish the work heap of the verification and the capacity of administrations. By utilizing cryptographic methods and secure code confirmation we expanded the certification for the security of the information and the database.

REFERENCES:

[1] M. Armbrust et al., "Above the Clouds: A Berkeley View of Cloud Computing," technical report, Univ. of California, Feb. 2009.

[2] S. Das, D. Agrawal, and A.E. Abbadi, "Elastras: An Elastic Transactional Data Store in the Cloud," Proc. Conf. Hot Topics in Cloud Computing (USENIX HotCloud '09), 2009.

[3] D.J. Abadi, "Data Management in the Cloud: Limitations and Opportunities," IEEE Data Eng. Bull., vol. 32, no. 1, pp. 3-12, Mar. 2009.

[4] A.J. Lee and M. Winslett, "Safety and Consistency in Policy-Based Authorization Systems," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), 2006.

[5] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - Ocsp," RFC 2560, http://tools.ietf.org/html/rfc5280, June 1999.

[6] E. Rissanen, "Extensible Access Control Markup Language (Xacml) Version 3.0," http://docs.oasis-open.org/xacml/3.0/ xacml-3.0-core-spec-os-en.html, Jan. 2013.

[7] D. Cooper et al., "Internet x.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 5280, http://tools.ietf.org/html/rfc5280, May 2008.

[8] J. Li, N. Li, and W.H. Winsborough, "Automated Trust Negotiation Using Cryptographic Credentials," Proc. 12th ACM Conf. Computer and Comm. Security (CCS '05), Nov. 2005.

[9] L. Bauer et al., "Distributed Proving in Access-Control Systems," Proc. IEEE Symp. Security and Privacy, May 2005.

[10] J. Li and N. Li, "OACerts: Oblivious Attribute Based Certificates," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 4, pp. 340- 352, Oct.-Dec. 2006.

[11] J. Camenisch and A. Lysyanskaya, "An Efficient System for Non- Transferable Anonymous Credentials with Optional Anonymity Revocation," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT '01), 2001.

[12] P.K. Chrysanthis, G. Samaras, and Y.J. Al-Houmaily, "Recovery and Performance of Atomic Commit Processing in Distributed Database Systems,"

Volume No:3, Issue No:1 (June-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Recovery Mechanisms in Database Systems, Prentice Hall PTR, 1998.

[13] M.K. Iskander, D.W. Wilkinson, A.J. Lee, and P.K. Chrysanthis, "Enforcing Policy and Data Consistency of Cloud Transactions," Proc. IEEE Second Int'l Workshop Security and Privacy in Cloud Computing (ICDCS-SPCCICDCS-SPCC), 2011.

[14] G. DeCandia et al., "Dynamo: Amazons Highly Available Key- Value Store," Proc. 21st ACM SIGOPS Symp. Operating Systems Principles (SOSP '07), 2007.

[15] F. Chang et al., "Bigtable: A Distributed Storage System for Structured Data," Proc. Seventh USENIX Symp. Operating System Design and Implementation (OSDI '06), 2006.