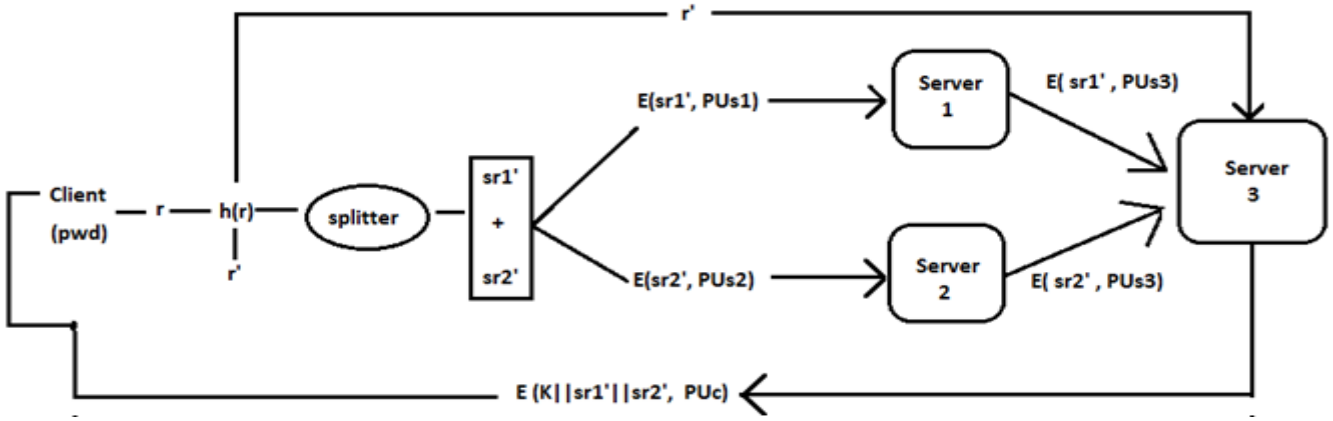

Figure 2: Overview of protocol

With reference to above figure, there are three severs and a client. Client having his password and he wish to communicated with the main server i.e. Server 3, client generate the random number r and prepare the hash value of it and send one copy of that random number to the Server 3, in this setting the client splits the hash code of random number into two equal parts and encrypts these parts with the public key of Server 1 and Server 2 respectively , then send these encrypted hash code send towards the Server1 and Server 2. Server1 and Server2 receives the information, decrypts the encrypted hash code and both the Servers again encrypt it with the public key of Server3 and both send the encrypted massage to the Server 3. Now Server 3 receives the messages, decrypts the massage and performing concatenation operation on the both hash code and compare the concatenated value with r′ which had earlier received from client . After the verification of all these values, the Server 3 send the key along with the hash codes received from the Server 1 & Server 2 by using the public key of client , and hence the client and the main Server (Server3) agree on the particular session key K.

5. Security of Protocol

Theorem 1. *This protocol is secure against any passive and active attack on all four levels i.e. on server1 level, server2 level, server 3 level and client level .*

Proof.
We are using public key cryptography while exchanging the messages or key

5.1 Server 1 and server 2 level security

Client instead of passing his actual password, generate the random number, prepare its hash code and splits the hash code into two parts for S1 & S2 but instead of directly sending the hash code client encrypt the messages with the public keys of S1 & S2 . As the messages are encrypted using the public keys of S1 & S2 so only S1 & S2 can decrypt the massages this is level one and level 2 security.

5.2 Server 3 level security

Server 1 & 2 after decryption of messages again encrypt it by using the public key of S3 and hence only Server 3 can decrypt the message and Server 3 after receiving the data, compare the data of these two Servers with the data of client, hence in case of any insider or outsider attack it can be detected here.

5.3 Client level security

Now client received the session key K from the Server 3, which had encrypted by the public key of client and hence only client can decrypt the data, and along with key it provided the splits hash code of Server 1 and Server2 which earlier had passed by client to both Server1 and Server2 and reflecting or detecting any misbehave with that code in the comparison, hence I proved the multi-level security in this system.

6. Conclusion

In this paper, I proposed a Multi-Server Authentication and Key Exchange protocol. Present protocols for password-only authentication, keeping all the passwords necessary to authenticate the clients on a single server which is not good from the prospect of security. Multi-level security analysis shows that this multi-server protocol is secure, easy and efficient for practical use.

References

[1] Xun Yi, San Ling and Huaxiong Wang , " Efficient Two-Server Password-only Authenticated Key Exchange" IEEE Trans. Parrell and distributed system, VOL 24, NO 9 Sep. 2013.
[2] W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, IT 22, no. 6, pp. 644-654, Nov. 1976.
[3] T. ElGamal, " A public key cryptosytem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Information theory, vol. IT-31, no. 4, july 1985
[4] William Stallings. "Cryptography and network security," Pearson 5th edition
[5] M. Abdalla and D. Pointcheval, "Simple Password-Based Encrypted Key Exchange Protocols," Proc. Int'l Conf. Topics in Cryptology (CT-RSA), pp. 191-208, 2005.
[6] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated Key Exchange Secure against Dictionary Attacks," Proc. 19th Int'l Conf. Theory and Application of Cryptographic Techniques (Eurocrypt '00), pp. 139-155, 2000.