infrastructures, and data security is a main concern in such systems [2] is the observation made by the authors. The authors propose an altered form of cryptography approach to support data security. A formulated threat model is proposed and a Hash chain based encryption method is proposed for the additional and layered security model.

In their paper [3] authors propose a system based on biometrics authentication to secure the medical data available in the public domain, as that provides uniqueness and low intrusiveness. Biometrics authentication is fused with secret PIN. The first factor uses simple and effective behavioral biometrics keystroke analysis model whilst the second factor uses secret PIN mechanism. A trust score is maintained after each level and access is granted on a final trust score.

A study on online financial services like online shopping, online banking etc. suggest that the end user environments face the threat of malwares like key logger and screen logger [4]. The paper proposes a novel approach of password protection called trusted Password Input Method (T-PIM), which provides a secure input method for passwords to the users. This acts as a security mechanism to avoid password extraction from a malware by employing hypervisor technology to isolate a trusted domain.

3. Proposed System

Public key Infrastructure (PKI) has proven over the years to be an effective and successful method and approach of security.

A **public key infrastructure** (**PKI**) is a set of policies and procedures needed to create, manage, use, store, and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

A. Encryption and Decryption

The benefits of PKI are delivered through the use of Public Key Cryptography. A core aspect of Public Key Cryptography is the encryption and decryption of **digital data**.

Encryption is the conversion of data into seemingly random, incomprehensible data. Its meaningless form ensures that it remains unintelligible to everyone for whom it is not intended, even if the intended have access to the encrypted data.

The only way to transform the data back into intelligible form is to reverse the encryption (known as decryption). Public Key Cryptography encryption and decryption is performed with Public and Private Keys.

The Public and Private Key pair comprise of two uniquely related cryptographic keys (basically long random numbers). Below is an example of a Public Key:

3048 0241 00C9 18FA CF8D EB2D EFD5 FD37 89B9

E069 EA97 FC20 5E35 F577 EE31 C4FB C6E4 4811

7D86 BC8F BAFA 362F 922B F01B 2F40 C744 2654 C0DD 2881 D673 CA2B 4003 C266 E2CD CB02 0301 0001

The Public Key is what its name suggests - Public. It is made available to everyone via a publicly accessible repository or directory. On the other hand, the Private Key must remain confidential to its respective owner.

Because the key pair is mathematically related, whatever is encrypted with a Public Key may only be decrypted by its corresponding Private Key and vice versa.

For example, if “A” wants to send sensitive data to “B”, and wants to be sure that only “B” can read it, he will encrypt the data with “B” Public Key. Only “B” has access to his corresponding Private Key and as a result is the only person with the capability of decrypting the encrypted data back into its original form.

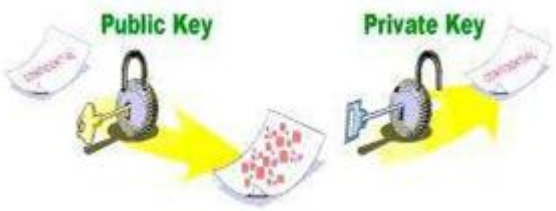

Figure 1: Encryption

As only “B” has access to Private Key, it is possible that only Alice can decrypt the encrypted data. Even if someone else gains access to the encrypted data, it will remain confidential as they do not have access to “B”’s
Private Key. Public Key Cryptography can therefore achieve Confidentiality.

B. Model

In this paper we propose the use of PKI for providing an additional layer of security for a person using a local system and wants to login to a remote machine securely. This approach also expands itself to any application or software that needs to connect or access a remote machine in a data critical environment.

The initial requirement for this model is the configuration of SSH on the remote machine and the local machine. Configuring SSH is very simple and doesn’t require much expertise on the domain.

In this model we exploit the fact that is core for the PKI, i.e. anything that is encrypted with the public key can only be decrypted by the corresponding private key. So to demonstrate the power of this architecture, we can consider the following scenario.

A system and 2 different users, both of these users have their different accounts in the system but they both have access to a single remote server. These both users have same access levels or permission rights over the remote machine. Now they come across a scenario where person A wants to store something in remote which he wants some other person C to access but not B. since A, B both have same rights, just keeping the data in remote is not sufficient for the requirement in hand. Now PKI's power becomes apparent. A encrypts the data with C's public key, and stores it in remote. Now all A, B and C can see the encrypted file in remote, but only C can decrypt it and use it as only he has the Private key. Which provided the security which was necessary. "Hiding in plain sight" is what was achieved by PKI in this scenario.

Below given steps explain the approach in which the above model can be achieved.

Step1: we generate the PKI key pair using any of the methods of Keygen by java, openSSL. Which gives us the public key and private key pairs.

Step 2: The person/ system from where we want to access the remote system keeps the private key and copies the public key on the remote machine. This public key should be a part of the **authorized_keys** in **.ssh** folder, created in the system once after the configuration of SSH is done. The configuration of SSH is necessary if you want to access a remote machine via SSH connections.

The **authorized_keys** file contains the keys and certificates certified and verified by an authentic CA (certificate Authority), it means that if a key is present is **authorized_keys**, it is recognized that it is valid and secure.

Step 3: The person/ system with the local system having the private key now SSH into the remote machine, now the remote machine doesn't ask him for password for the account he is logging in to. It is taken care the matching of private and public keys.

Ex: ssh root@1.2.3.4

Last login: some date, time stamp:

Below figure explains how the mechanism works.

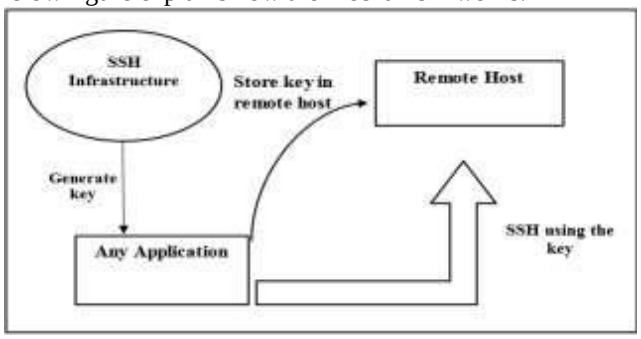

Figure 2: Model for Authentication over PKI.

In many data critical systems, the above model provides the additional and extra layer of security which is easy to use and also strong enough to prevent from the masqueraders and spyware and man in middle attacks.

4. Conclusion

Multiple layers of security are needed for the data centric systems and also for the systems which want to give their clients a bit additional security as add on factor. Many multi factor systems already exist which provide the necessary additional security mechanisms. Each application/ system can choose one of these methods based on their requirements and considering cost benefits and other factors. Some of these methods, though effective, include inherent risks and complex natures of implementation. The method proposed in this paper is elegant, effective and simple enough to incorporate over any existing systems. And also provides a special and enhanced security over the data centric applications and data share intensive environments.

References

[1] G. Matanović and M. Mikuc, "Implementing certificate-based authentication protocol on smart cards," *MIPRO, 2012 Proceedings of the 35th International Convention*, Opatija, 2012, pp. 1514-1519.
[2] H. Cao, P. Zhu, X. Lu and A. Gurtov, "A layered encryption mechanism for networked critical infrastructures," in *IEEE Network*, vol. 27, no. 1, pp. 12-18, January-February 2013.
[3] T. Bhattasali and K. Saeed, "Two factor remote authentication in healthcare," *Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on*, New Delhi, 2014, pp. 380-386.
[4] M. Hirano, T. Umeda, T. Okuda, E. Kawai and S. Yamaguchi, "T-PIM: Trusted Password Input Method against Data Stealing Malware," *Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference on*, Las Vegas, NV, 2009, pp. 429-434.
[5] S. Chaudhari, S. S. Tomar and A. Rawat, "Design, implementation and analysis of multi layer, Multi Factor Authentication (MFA) setup for webmail access in multi trust networks," *Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on*, Udaipur, 2011, pp. 27-32.
[6] Z. Mao, D. Florêncio and C. Herley, "Painless migration from passwords to two factor authentication," *2011 IEEE International Workshop on Information Forensics and Security*, Iguacu Falls, 2011, pp. 1-6.
[7] C. Su; B. Santoso; Y. Li; R. Deng; X. Huang, "Universally Composable RFID Mutual Authentication," in *IEEE Transactions on Dependable and Secure Computing* , vol.PP, no.99, pp.1-1