further communication. In the user identification phase, each user has to deal with resource access based on the underlying security mechanisms. Between user and service provider there is a series of communications as part of user identification as presented in Figure 2.

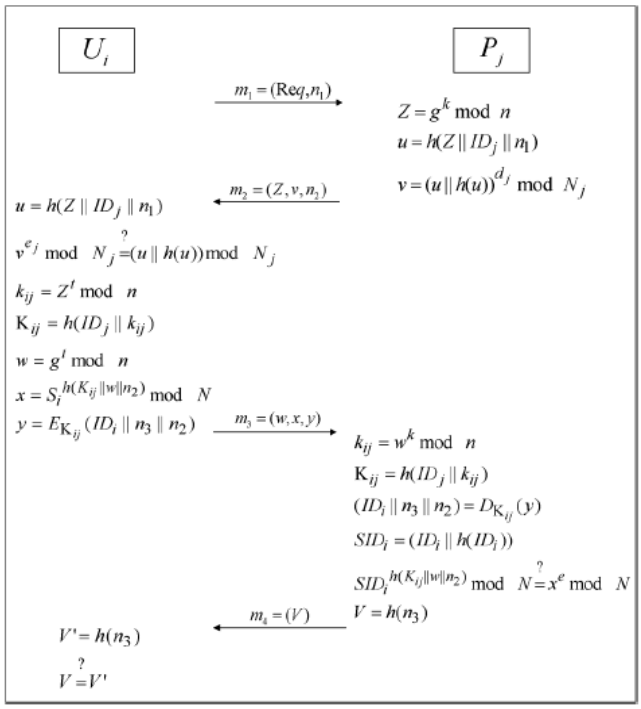

Figure 2: User identification phase [14]

As can be seen in Figure 2, it is evident that the user identification is carried out between two phases as part of the scheme. The scheme facilitates secure communication between two parties and thus it becomes part of the SSO scheme.

3. Implementation

We built a prototype application that demonstrates the concept of single sign on. The proposed scheme has been applied to an application where multiple parties are involved and multiple services are provided with SSO scheme.

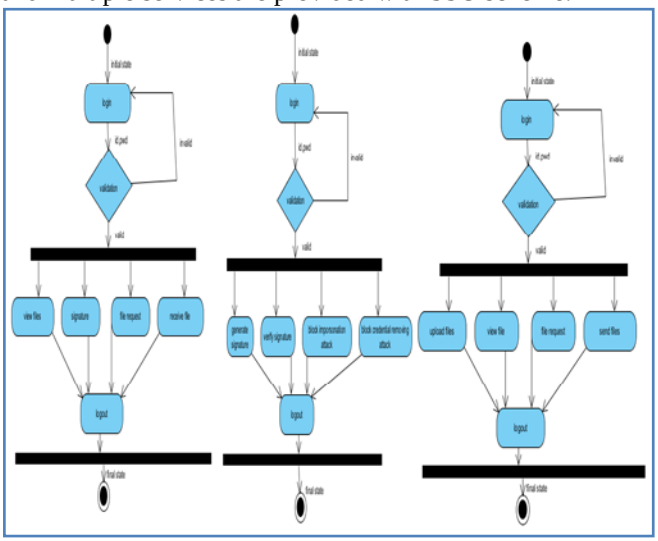

Figure 2: Activities of various users of the application

As can be seen in Figure 2, it is evident that the application has provision for various users such as normal user, SCPC user and service provider. The normal user has provision for various operations after SSO process. They include viewing files, signature, file request, receiving file and logging out. The SCPC user has provision for activities like generating signature, verifying signature, block impersonation attack, block credential removal attack and logging out. The service provider user has provision for operations like uploading files, viewing files, requesting for files, sending files and logging out. Before implementing these activities in web application besides implementation of SSO scheme backend schema was identified through normalization process.

3.1 Prevention of Man-in-the-Middle Attack

The proposed system provides solution for Man-In-The-Middle attack. This attack is generally launched by an adversary who can inject messages into a communication channel, modify existing messages or even eavesdrop messages. This is possible when attacker finds unencrypted WI-FI communications between them. The attack scenario is presented in Figure 3.

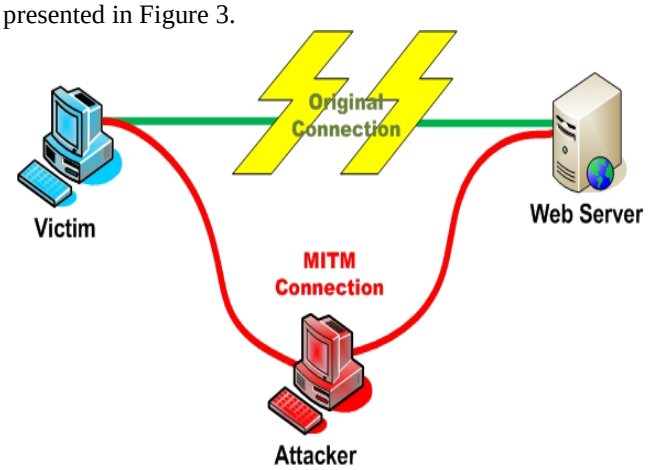

Figure 3: Illustrates man-in-the-middle attack

The proposed solution has prevention for the attack as it ensures strict authentication and authorization procedures as part of the SSO procedure. The secure communications among parties involved in conversation are initiated with fool proof security measures that do not allow attacker to succeed in man-in-the-middle attack. The attacker will not be able to gain access to the network in order to inject messages into the network.

3.2 Backend

MY SQL is used for backend. MY SQL is an RDBSM that is meant for storing the data generated by the proposed application. There are many tables for managing data being generated by the application including the tables that deal with SSO credentials. File management, user management and SSO related credentials are stored in corresponding tables. These tables are accessed from frontend application in order to demonstrates the SSO mechanisms, the attacks on the SSO scheme and other genral operations of the applications as required.

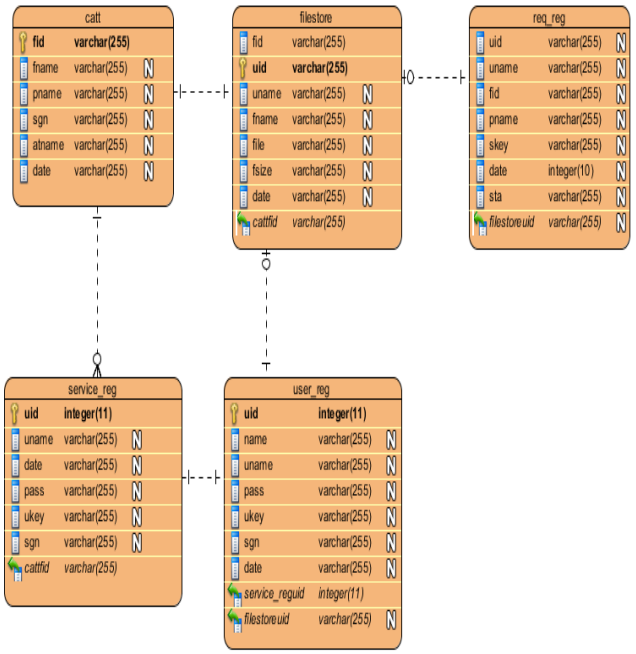

Figure 3: Backend schema

As can be seen in Figure 3, it is evident that the backend schema has several tables and each table contains related attributes. The schema has been normalized in order to have compact tables that provide clear storage provisions in the backend.

3.3 Prototype Application

We built a prototype application that interacts with backend as per the user needs. The application is built in Java technologies like Servlets and JSP. JDBC is used for interacting with the MY SQL and the application is meant for dmeonstratign the normal operations and also the soundness of the SSO scheme in the presence of various attacks. UI for SCPC user is as presented in Figure 4.

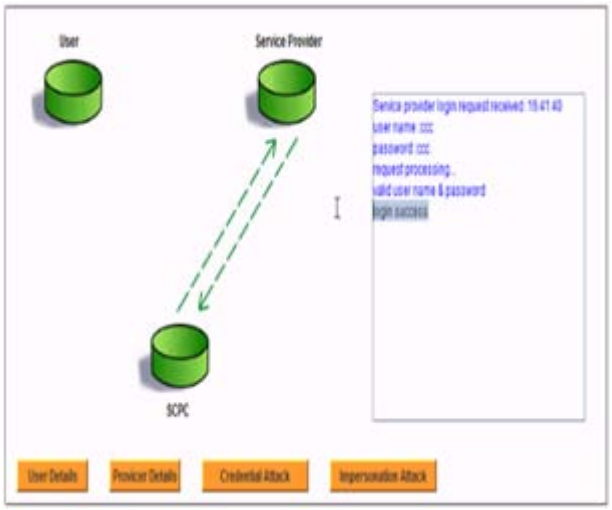

Figure 4: UI for SCPC user activities

As can be seen in Figure 4, it is evident that the SCPC user can perform activities like viewing user details, provider details, and testing the soundness of the SSO scheme by launching attacks such as impersonation attack and credential attack.

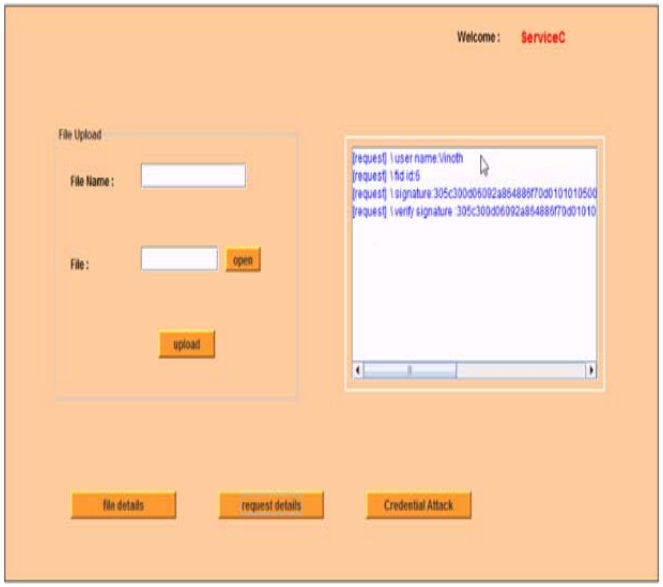

Figure 5: UI for service provider user

As can be seen in Figure 5, it is evident that the service provider user can provide various operations like uploading files, viewing file details, requesting details and even launching credential attack for testing the soundness of SSO schme.

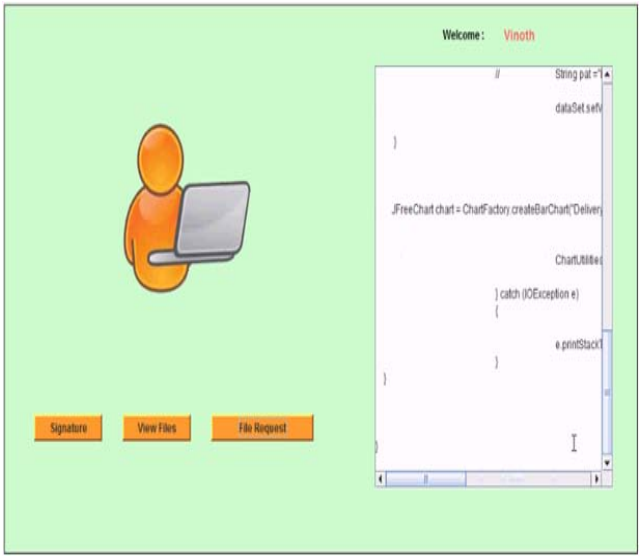

Figure 6: UI for normal user

As can be seen in Figure 6, it is evident that the normal end user can have operations like viewing files, making file request and so on. These operations are performed by end user after due SSO process and with single sign on users can perform various operations and jump to related services as well.

4. Experimental Results

Experiments are made in terms of testing the soundnesss of the proposed application. Two attacks such as credential attack and impersonation attack are made around 100 times and the average prevention capabilities are recorded. The

results of the proposed application are comkpared with existing solution. The results are presented in Figure 7.

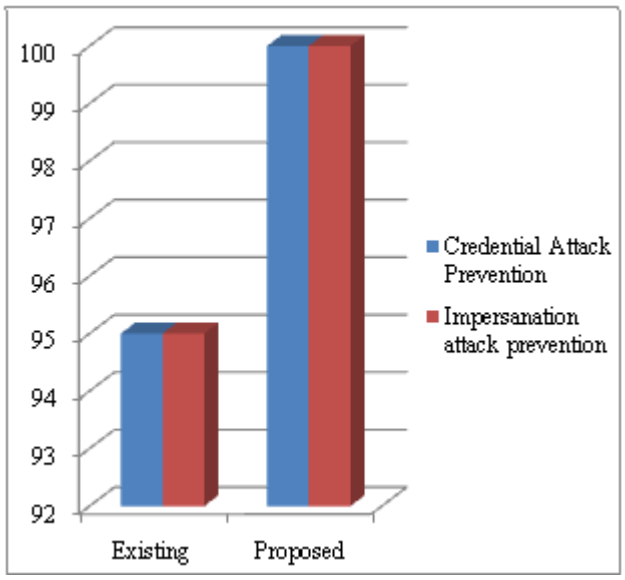

Figure 7: Attack prevention capabilities of proposed system

As can be seen in Figure 7, it is evident that the proposed SSO scheme and the application demonstrates the soundness of the technique. There is 100% security evident with respect to the SSO scheme implemented in this paper while the existing solution is vulnerable to credential and impersonation attacks.

5. Conclusions and Future Work

In this paper, we study the soundness of SSO schemes. SSO allows users to have single credential to have provision to visit multiple sites or to perform multiple activities. This will help in distributed computing environment to gain access to multiple service providers. This can avoid remembering many credentials as well. Single credential authentication has its advantages but when the credential is compromised, security is lost. Therefore it is essential to ensure that the credential is not disclosed. In this paper our focus was on making review on the SSO schemes and building a new SSO scheme that overcomes the drawbacks of existing scheme. The existing scheme was proved to be inefficient with attacks such as credential attack and impersonation attack. We built a prototype application to implement the SSO scheme and also demonstrate the soundness of SSO scheme for accessing multiple services using a single credential. In future we intend to implement SSO to real time applications.

References

[1] W. B. Lee and C. C. Chang, “User identification and key distribution maintaining anonymity for distributed computer networks,” Comput. Syst. Sci. Eng., vol. 15, no. 4, pp. 113–116, 2000.
[2] W. Juang, S. Chen, and H. Liaw, “Robust and efficient password authenticated key agreement using smart cards,” IEEE Trans. Ind. Electron., vol. 15, no. 6, pp. 2551–2556, Jun. 2008.
[3] Y. Yang, S. Wang, F. Bao, J. Wang, and R. H. Deng, “New efficient user identification and key distribution scheme providing enhanced security,” Comput. Security, vol. 23, no. 8, pp. 697–704, 2004.
[4] K. V. Mangipudi and R. S. Katti, “A secure identification and key agreement protocol with user anonymity (SIKA),” Comput. Security, vol. 25, no. 6, pp. 420–425, 2006.
[5] C.-L. Hsu and Y.-H. Chuang, “A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks,” Inf. Sci., vol. 179, no. 4, pp. 422–429, 2009.
[6] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, “oPass: A user authentication protocol resistant to password stealing and password reuse attacks,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 651–663, Apr.2012.
[7] A. Valenzano, L. Durante, and M. Cheminod, “Review of security issues in industrial networks,” IEEE Trans. Ind. Inf., vol. PP, no. 99, 2012, DOI 10.1109/TII/2012.2198666.
[8] B. Fabian, T. Ermakova, and C. Muller, “SHARDIS: A privacy-enhanced discovery service for RFID-based product information,” IEEE Trans. Ind. Inf., vol. 8, no. 3, pp. 707–718, Aug. 2012.
[9] B. Wang and M. Ma, “A server independent authentication scheme for RFID systems,” IEEE Trans. Ind. Inf., vol. 8, no. 3, pp. 689–696, Aug. 2012.
[10] “Security Forum on Single Sign-On,” The Open Group [Online]. Available: http://www.opengroup.org/security/l2-sso.htm
[11] J. Han, Y. Mu, W. Susilo, and J. Yan, “A generic construction of dynamic single sign-on with strong security,” in Proc. SecureComm’, 2010, pp. 181–198, Springer.
[12] U. Feige, A. Fiat, and A. Shamir, “Zero-knowledge proofs of identity,” J. Crytography, vol. 1, no. 2, pp. 77–94, 1988.
[13] C.-C. Chang and C.-Y. Lee, “A secure single sign-on mechanism for distributed computer networks,” IEEE Trans. Ind. Electron., vol. 59, no. 1, pp. 629–637, Jan. 2012.
[14] Guilin Wang, Jiangshan Yu, and Qi Xie. (2013). Security Analysis of a Single Sign-On Mechanism for Distributed Computer Networks. *IEEE*. 9 (1), p294-302.