ISSN:0975-9646

Enhanced SSO based Multi-Factor Authentication for Web Security

Shruti Bawaskar , Prof. Mahendra Verma

Department of Computer Science & Engineering
Sushila Devi Bansal College of Technology Indore (M.P)

***Abstract*— Network security plays a vital role in the protection of user's confidential information along with its identity verification. The process of verification of user's identity comes under the area of authentication. Traditional system applies authentication in one way or two way means which verifies the user and the provider's information before any service exchanges was performed. Single sign on (SSO) is one of such mechanism which allows the users to get access to their services by entering their identity information only once in the system. During the last few years there are so many SSO models are suggested and applied for different types of applications and based on various signatures, cryptographic and digest approaches. But somewhere they lack in applying the access control in a granular manner. After in depth survey we have found that the traditional SSO is lacking in some areas like protection of cookies, cached data security, temporary storage protection and finally the dependencies on only credential's information for authentications.**

Thus, this work proposes an enhanced SSO based multi-factor authentication for getting the things right according to the user and provider with fewer efforts. We have suggested an continuous bit sequence based certificates based on SSO using some of the additional management schemes. Along with the certificate format, its sequence, transmission information, its protection pin. Thus the complete solution will deals with increasing the protection of overall system by securing the temporary data, cookies and their logs so as to prevent fabrication, modification and eaves dropping attacks.

***Keywords*— AES , Analyzer , Auditor , Authentication , Bit Sequence Certificates (X.509), Cache , Logger , MD5 , Security , Single Sign On (SSO)**

I. INTRODUCTION

In today's world increasing technological needs and users behaviour is changing very rapidly. It is quite complex to sustain the growth rate along with technology modifications. As the number of users connected to the internet is varying there usages and authentication is also suffering from several security concerns. Interfaces are complex and login functionalities are dynamically extending the functionalities. The demand is to be satisfied in such a way which is secure and load of reminding the credential should be reduced. Single Sign on (SSO) is one such solution to implement the service authentication and identity verification is less number of steps. The aim is to make them satisfied and feel secure while they are supplying the important information available in the network. Here the users are authenticated by the distributed functionality machines in the network to hold the services and applications. The SSO system prevents the user load of entering the authentication information, like username and password, multiple times. The primary problem in a large network environment is the way to distribute the specific individual or group roles to form the organizational security policies. Later on it organize the security by resource management, measures the security mechanism and complete the requirements to analyze how those requirements exchange information's with the network.

Security of information is one of the major process of getting the higher trust and reliability of users over the system and prevents the unauthorized access and activities to disrupt the normal operations. Authentication is one of such process that provides high security of information. When a user claims to have an access for the protected operations of network then the user's identity should be checked. The process of verifying the identity is known as authentication. After this process, authorization is taking place for giving limited permission to each authorized user to access the applications inside the network. As it known, username and password is the first oldest solution for authentication, but typically that is not enough to have a secure environment. In today's system authentication is served using three major requirements:

(i) What a user know, like password or a pin number,
(ii) What a user have, like a smart card and
(iii) What a user is, like biometrics.

If a user only uses a password or a pin for an authentication that is called one-factor authentication, which is not secure enough. If password used with both one of the other authentication mechanisms, than it will be two-factor authentication. In addition, to have a strong authentication mechanism, clever combinations needed to come up as a benefit for the system. First of all variety types of authentication mechanisms are presented in the following part to provide strong authentication.

- ***User authentication***

Primary entity of authentication from a user views is passwords which might taken as the first possibility for attackers to get entered in to a network. Preventive measures or action for any device to reduce networks vulnerability is to

generate or create strong passwords along with strong authentication. The password that created must be unique for SSO system. Otherwise, OTP (One Time Password) is another method for the user authentication. OTP is varying every time when it is used. This increases the difficulty of the password based security controls and builds a communication between the user and the applications.

- ***Biometrics authentication***

Biometrics serves strong authentication to the users using people's characteristic behaviors and genetic features such as hand, fingerprint, eyes, retina, hand etc for the user authentication. Using biometric features the system is capable of differentiating one person from another by their physical attributes and provides secure authentication.

- ***Token based authentication***

Token is an authentication mechanism that provides a cryptographic token to prove the user identity for the authentication server towards getting the access. It could be a physical device or logical code intended to give effective authentication to be used by only one person to get an access to the system. It has a trusted secret key between the authentication server and the applications that user wants to have an access. But this mechanism is different than a biometric device.

Good examples for tokens are smart card are as follows.

a. Out of band

Out of band authentication is used to support two ways of communication using two ways (factor) of authentication. There is a regular flow of authentication message between the computer and the server, Using out of band means one part of it is uses other way of communication. It might be mobile communication. One part of the information is sent by the network and the other part is sent through the mobile. For instance, nowadays internet banking is popular for the customers. That security requires the user to identify him/her two times. A computer is login in to the bank over the internet. And then to verify the user it is receiving, for instance OTP on sms. That OTP is needed for to authenticate. So that user deals with two different bands. This way of communication makes it hard to hack in, because the attacker needs to hack in several communications.

b. Certificates

There are different ways of gaining trust on humans. Those might be provided by voice, face or handwriting. This is easy for the people have known before. For the rest, it needs more techniques to trust with. Each implemented technique need to be improved personally by asking specific questions to trust the other party. It called as a "trust threshold". It might be a unique form of paper or unique signature of trust.

One way is to have several people inside the organization, police or another third party who could be a voucher for the both parties. The second way is to apply for exchanging cryptographic keys.

Those keys are providing communication between users, like explained before in encryption types. All public keys are attached with each user identity. So that users can trust the communication by knowing with whom they are exchanging the information. However certificates are communicating and identifying users electronically. This protocol is used between different SSO components.

c. PKI structure

It is challenging to believe somebody that is not known without trusted third party. PKI used as a trusted communication in ecommerce contacts made over the Internet. A PKI is designed to enable users to create, manage, store, distribute and revoke digital certificates by implementing public key cryptography. Additionally it is designed to make trusted communications between users within private or public networks. PKI provides services for identification and access control. Those are such as creating certificates with using public key, distributing certificates, signing certificates within an authenticity, adding validation date to certificates and extracting certificates which private keys are no longer validate or the supplier of the certificate is no longer allowed to have access.

d. Network authentication

Nowadays e-businesses are compacting through the internet application systems, emailing, conferences, merging several organizations in one large network. Those countable serious communications are operating through the internet. Large numbers of users are online in the systems for their businesses. Those systems are protected by different security standards in the form of web services for the users and each mechanism has different policies and use of authorized certifications. For the identity issues SSO came in for the systems. SAML is an XML based security standard mechanism for communicating identities between different organizations. It provides authentication documentation according to web user's authentication and authorization attributes including authentication event description for the web user between the application and the enterprise security system. The importance of the SAML is defined in four steps.

- *All the key point of the SAML maintains the multiple authentication credentials like passwords in the multiple locations.*
- *It increases the security and decreases the identity theft by not allowing several credentials for the same user. This also decreases identity phishing inside the network by eliminating the number of times the user needs to login.*
- *It increases application access, so that users do not need to enter the same form of password to enter the application. All they need is to click on the application link.*
- *It prevents from duplicate credentials helps to decrease the administration time and also minimize help desk calls for resetting the last passwords.*

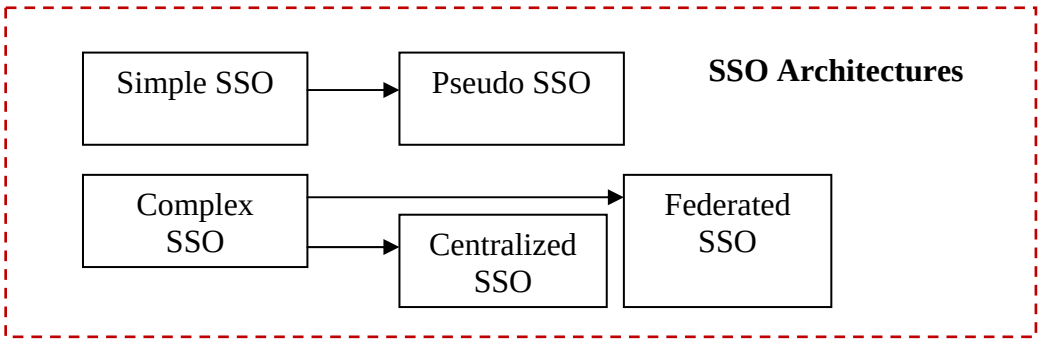


Figure 1: Single Sign On (SSO) Architectures

II. BACKGROUND

Different types of SSO

Most of the SSO products available in the market can be categorized into two types based on the architecture.

(i) Web-based or enterprise SSO

Web-based SSO can be further categorized internet facing intranet facing. Internet facing generally takes care of the SSO for the applications that interact with customers. For example customer support application, billing management etc. These applications can be knit using SSO so that customers can login only once to be able to access both the applications. While the intranet facing serves SSO for the intranet applications that internal users of an organization interact with, using a web browser. For example, an expense reporting application, travel planning etc. Multi-domain: This can be categorized into two types i.e. Intra-organization multi-domain SSO and cross-organization SSO. In first type, the SSO is made between two or more different domains in the same organization while in second one SSO made between the applications of two or more organizations.

(ii) Non Web-based or legacy SSO

Legacy SSO products use a different approach to SSO. A component called the SSO agent gets activated when a user logs into his workstation and remembers the logins and passwords of the user to different applications. It provides the credentials to the applications when the user tries to log into these applications subsequently. Thus, with one authentication session initiated by the SSO agent, legacy single sign-on enables user navigation to various applications on an intranet. Recent versions of legacy single sign-on products support smart card, PKI, and biometric authentication.

Single sign-on application

The single sign on (SSO) solutions are practically implemented in different architecture which was made according to user perspectives or operational scenarios. They are divided in to two different SSO, simple SSO and complex SSO and there further division was also shown in figure 1.

- Pseudo SSO is a single authentication mechanism in which the user is having several identities but only authenticating with one credential for the first system. For other systems user is using other identities to connect.
- In Pseudo SSO, user first directed to the primary authentication which is the Pseudo mechanism. This authentication might require a single username and a password.
- Complex SSO is divided in to Centralized SSO and Federated SSO systems. In this complex environment it is possible to have more than one domain or company.
  - Centralized SSO has a centralized database and a centralized third party of trust communication in one domain. In centralized systems, user has the same identity for all different systems. Token based SSO is one way to authenticate user in the centralized environment.
  - Federated SSO is used in more than one domain in one environment. In this systems user has the own identity which is trusted by other systems. Microsoft Passport, the Liberty Alliance and WS-Federation protocols are used together with the security standards like SAML, Shibboleth and Kerberos to provide secure and friendly environment by sharing the user identities during the data transmissions between different domains, services and applications.

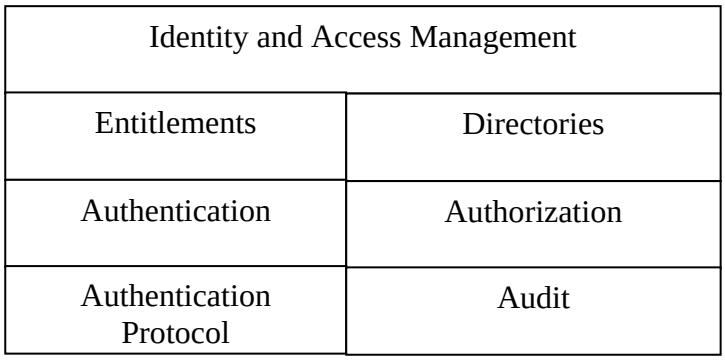


Figure 2: Single Sign on (SSO) Implementation Strategies

After all those explanations about different SSO architectures, standards, protocols, Federated methods and communication tools, here come to build up all those information to have a good implementation strategy for the SSO. Strategically SSO terminology is divided and showed in below blocks in Figure 2.

The blocks represent the complete implementation strategies of effective authentication using SSO. First block is representing the basic system with the entire user profiles. Sub-block is representing further categorization. The entitlements are used to determine the users activities monitoring and tracking about what they can or cannot do. Directory helps SSO to register and store the user identities. The second block is the core system of the network. All are independent and need higher level of security. And this block is in a repeat cycle to check or identify the user rights to enter the system or one system to another. That happens in the future when user entitlements are changed or need to have an entry to the other systems.

The change is all depending on the user profile and the level of the system. Only that user profile is used and gave rights to the next system. The system authentication is done to prove the user and the authorization is done to verify if that user is authenticated or not according to the user profile. After being authenticated, user is passing through the protocols and standards to work under safe and secure conditions. Different protocols are used for the authentication in higher system levels. That is depending on how high level is intended to be accessible. And then the same cycle is processing for the authentication and authorization. Auditing is controlling and documenting user's activities in case of attacking and faults.

III. LITERATURE SURVEY

During the last few years security is considered as major issues and to make it more robust against the unauthorized access authentication is the major process. Single Sign On is one of such mechanism which provides higher security. Considering this phenomenon here are some related papers studied to get better depth and analysis of existing approaches.

In the paper [8], authors suggested a new proxy signature schemes as the first public key cryptographic method for applying single sign-on in distributed networks. The work is presented in two steps: first it provides the session state management of multiple services and second is granular access control. It is an intrinsic centralized access control which provides an easy way to manage access policies and user rights revocation. The approach significantly improves communication complexity by eliminating any communication between services and identity providers during user identity and access permission verification. This is the first approach to base single sign-on security on public key cryptography and associate such a practical application to proxy signatures.

In the paper [9] a detailed analysis of SSO enabled user accounts is performed on different websites to get the users interest and found that user's perception of web SSO is still poorly understood. After finding the issues the paper offers a web SSO technology acceptance model with design improvements. To reduce user's privacy concerns, it is crucial that RPs practice the principle of gradual engagement, and IdPs provide fine-grained privacy control and on-login profile switching option. In addition, future research should investigate how to enhance users' security perception and mitigate IdP phishing attacks without relying on users' cognitive capability.

The paper [10] specifically focused on developing the SSO for distributed environment by giving a detailed survey. The paper founds that most existing schemes cannot preserve user anonymity when possible attacks occur and those schemes are insecure. Also in existing SSO schemes have not been formally proved to satisfy credential privacy and soundness of credential based authentication. To overcome this drawback, they formalize the security model of single sign-on scheme with authenticated key exchange. Specially, the difference between soundness and credential privacy is pointed out and they define them together in one definition. Also, they propose a provably secure single sign-on authentication scheme, which satisfies soundness, preserves credential privacy, meets user anonymity, and supports session key exchange.

In traditional SSO application architectures, the users required to memorize and utilize a different set of credentials (e.g. username/password or tokens) for each application. However, this approach is inefficient and insecure with the exponential growth in the number of applications and services a user has to access both inside corporative environments and at the Internet. It is shown that the previous schemes are actually insecure as they fails to meet security during communication. For getting the secure authentication, digital signature with hash function is further explored.

The paper [11] also suggests a password-authenticated key agreement scheme using smart cards. In terms of efficiency, besides the low communication costs, proposed solution builds on the efficient cryptographic primitives for smart card environment. It also gives effective results while analyzing mutual authentication, key agreement, initiator anonymity, and the functionality of password updating, DoS attack prevention and initiator traceability.

The article given in [12] proposes a Kerberos V5 protocol based single sign-on authentication model for cloud to prevent DDOS attacks. This model could benefit by filtering against unauthorized access and to reduce the burden, computation and memory usage of cloud against authentication checks for each client. It acts as a trust third party between cloud servers and clients to allow secure access to cloud services. The approach formally described as a network authentication system, initially designed for providing single sign-on to network services. Preliminary investigation is proving effective results in comparison with traditional authentication systems.

In the paper [13] single sign-on SSO mechanism is proposed which controls the authentication using Trusted Authority Center (TAC). The primary task of TAC is to

automatically verify the user's credentials details which will be only one for all applications or services. Previously introduced technique based SSO technology proved to be secure over well-designed SSO system, but fails to provide security during communication. So here emphasis is given on authentication as open problem and on to refining the already proposed SSO process. And to do this along with RSA algorithm which was used in previous SSO process, the paper is using MAC algorithm to control secured pathway for communication over distributed network.TAC i.e. Trusted Authority Center is used for sending token integrated with private and shared public key to user.

The paper [14] focuses on applying Single Sign-On (SSO) based authentication for cloud computing services. Here the SSO can be used to verify the legitimate users without requiring them to get authenticated with each service provider separately. For developing a prototype CloudSim is used as a simulation tool configured with different cloud scenarios. As of now, the simulator lacks effective user authentication and authorization methods with it. Thus the paper also discusses the design and implementation of SSO mechanism in the Cloud Federation scenario using the CloudSim toolkit. The paper uses Fully Hashed Menezes-Qu-Vanstone (FHMQV) protocol for the key exchange and the Symmetric Key Encryption technique AES-128 for encrypting the identity tokens. The paper is also gives the workflow model for the proposed approach for different execution time taken in the simulation.

The paper [15] discussed some of the existing single sign-on (SSO) systems like OpenID and OAuth for authenticating web sites. They consider them as relying parties (RPs) and provides effective user authentication as a service to identity providers (IdPs) likes Google or Facebook. It also founds that in Mozilla's Browser system, current SSO is not designed with user privacy control. Unfortunately, recently discovered attacks exploit these design flaws of BrowserID. Thus, the paper proposes first privacy-respecting SSO system for the web, called SPRESSO (for Secure Privacy- REspecting Single Sign-On). The system is easy to use, decentralized, and platform independent. It is based solely on standard HTML5 and web features and uses no browser extensions, plug-ins, or other executables. Existing SSO systems and the numerous attacks on such systems illustrate that the design of secure SSO systems is highly non-trivial. The paper also carries out a formal analysis of SPRESSO based on an expressive model of the web in order to formally prove that SPRESSO enjoys strong authentication and privacy properties.

IV. PROBLEM IDENTIFICATION

After analyzing the complete usage scenarios and working of single sign on (SSO) application and implementation details along with the research works, this work identifies some of the issues which remains unsolved. Some of the authentication situation and security primitives needs to be improved in comparison with the traditional approaches.

- Single Sign on (SSO) uses the continue access to the cookies which holds the access patterns and other details of users credential and authentication information. Thus, with traditional system cookies are not looked over and its access is not protected or encoded by which it is directly open to the normal and malicious users. Thus there must be some encryption or encoding phenomenon with traditional SSO.
- Likewise the above issue there is an also associated problem to that regarding the cached component of the software system. It might hold the authentication information also. Thus all the access mechanism for getting the cache directly readable to user must also be controlled and protected.
- After using the temporary storage for passwords, they are stored there till the next information gets stored in that buffer. This casual nature of SSO made them vulnerable against the attacker. There must be some mechanism which automatically destroys all the temporary information just after their use is over.
- Log files are also not secure thus some auto erasable logs or transferrable logs to secure server just after their use is over must be integrated with the traditional SSO.

V. RESEARCH OBJECTIVES

This work describes the risk handling and strong security primitive based SSO for complex system environment. It primarily focuses on the complete security by finding an optimal solution about usage of SSO. The goal is to make a implemented solution for improved SSO against the above mentioned issues using set of standards and protocols effectively. Futuristic results will be presented is later stages of this work by using prototype developed as a proof. Thus by this work to be completed there are some objectives on which the work is performed in some next stages of this work. These are:

- Analysis of information security requirements and develops a solution and test its results before and after implementation of SSO.
- Develops a trusted SSO using some physical device based authentication
- Integrate the protocols and standards require achieving the Robust and More secure SSO.
- Analyze the critical functionalities that SSO-service would need to work proper
- Proof of Concept development for proposed approach

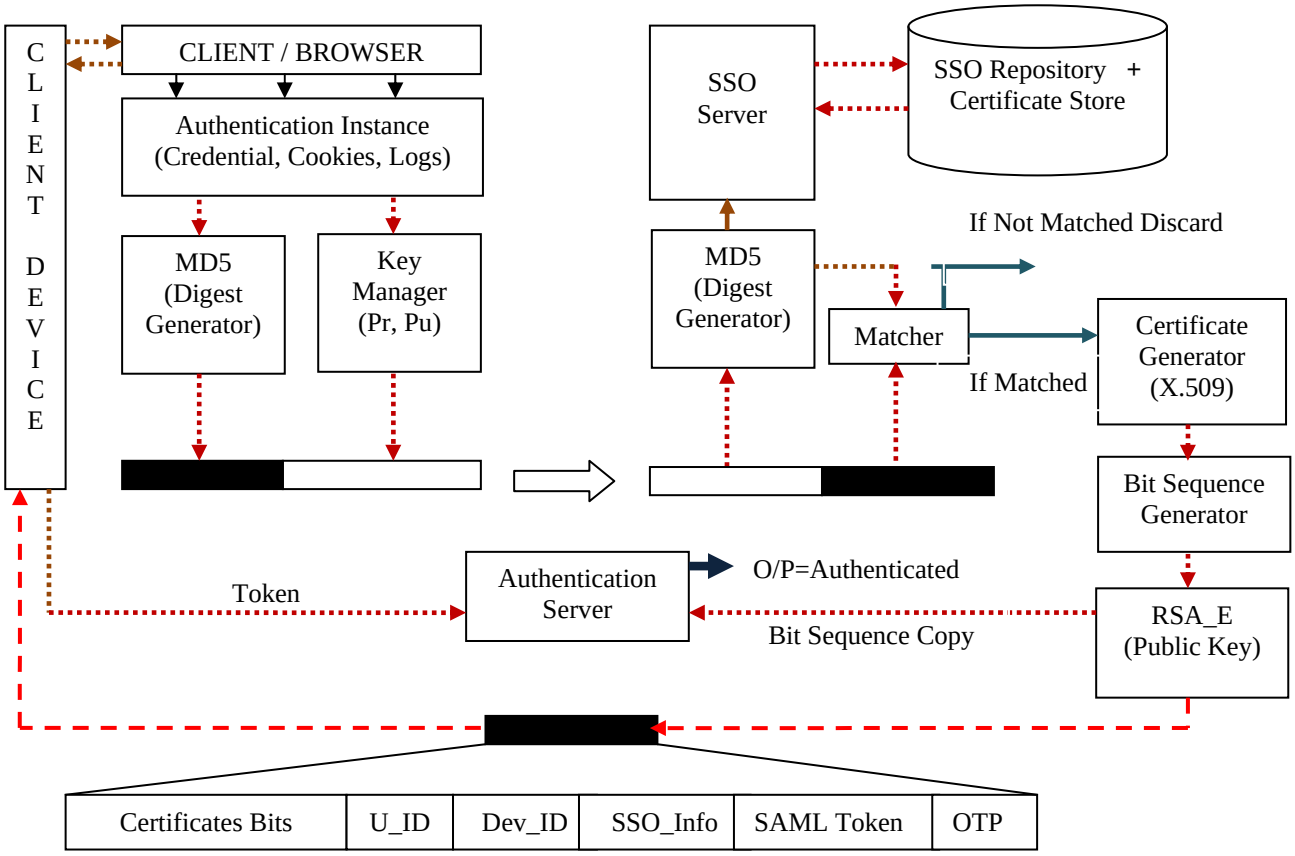
VI. PROPOSED SOLUTION

This work proposes a novel strong authentication system using improved Single sign on (SSO). This system is having three entities: User, Certification Authority and SSO Server. The user is having the regular exchange of security certificates between them. For developing a more robust system the work is also using the phenomenon of Smart Cards. It is a secure authentication mechanism with security

primitives holding integrated chips. As it was an hardware device whose custody is kept with the authenticated user only. But somewhere it can be lost thus the SSO works in integration with the credentials and smart card. Also the smart card availability is not there with every user and the machines for swapping these cards require certain hardware cost. With this work we are introducing the smart card functionality with the pen drives which works as certificate holding and generator device. Smart cards functionality based pen drives works as storage for token stored with personal information of user with strong cryptographic computational capability for authentication.

The smart card pen drive is inserted to the system from where authentication is demanded and then the credential is passed along with the auto generated digest by the device is passed to the server.

The server recalculates the digest which and matches it with newly calculated digest and if the things matched then the authentication is provided. This prevents users to remember several different usernames and passwords to have an access.



It can also hold the users activity logs and cookies information which was previously stored in the computer itself thus the problem associated with the theft of cookies or unauthorized access of them is avoided. It provides two factor authentications which is more reliable. Smart is also protected by a pin itself. For SSO smart will generates a pin based on its certificate used for one time only. The system starts operating when user requires authenticating himself against the system. At the time of registration the user sets its id, password and enters the device into the system. The server verifies the user's information and generates a certificates and other log based details holding files and transfer them to this device. Now each time the user demands the login the devices updates these records and the cached files.

Components of System

(i) **Smart Card Pen drives Device:** Store Certificate (X 509), Digest (MD5), One Time Pin, Cache Data, and Self Erasable Unit (SEU).

(ii) **SSO Authentication System:** Browser with Integrated Service, Key Generation, Verifier, Auditor, Logs Generator

(iii) **Authentication Server:** Tokens and Certificate Generator, Digest Matcher (MD5), Request Analyzer, Card Verifier, Identity Manager.

By the above component analysis the system can operates completely with integrated SSO and the smartcard device. For developing this system there are different algorithms needs to be implemented which works at different

layers of security control. The proposed system is capable of providing the more secure way of authentication. It were satisfying the property of authentication, authorization, provisioning, centralized identity management, cache manager, single point of control, password protection and proliferation handler etc.

VII. EXPECTED BENEFITS

The advantages of the Proposed SSO approach include:

- *Reduction of the time spent by the users during log-on operations to individual domains.*
- *Reduction of the failed log-on transactions.*
- *Reduced time for log-on to secondary domains.*
- *Reduced costs and time used for user's profiles administration.*
- *Improved security since the number of username/password each user has to manage is reduced.*
- *Simplified administration because with a centralized administration point, system administrators reduce the time spent to add and remove users or modify their rights.*
- *Enhanced ability of system administrators to maintain the integrity of user account configuration including the ability to change an individual users access to all system resources in a co-ordinate and consistent manner.*
- *Higher services usability because the user has to interact with the same login interface.*
- *Uniform interface to user accounts management thus enabling a coordinated and synchronized management of the component domains.*

VIII. CONCLUSION

Security of information is one of the major process of getting the higher trust and reliability of users over the system and prevents the unauthorized access and activities to disrupt the normal operations. Authentication is one of such process that provides high security of information. When a user claims to have an access for the protected operations of network then the user's identity should be checked. The process of verifying the identity is known as authentication.

After this process, authorization is taking place for giving limited permission to each authorized user to access the applications inside the network. As it known, username and password is the first oldest solution for authentication, but typically that is not enough to have a secure environment. At the analytical level of evaluation the approach is satisfying all the preliminary security constraints related with authentication. Later on result parameters will prove the effectiveness of the proposed approach.

REFERENCES

[1] Michael Fleming Grubb and Rob Carter"Single Sign-On and the System Administrator"published in the Proceedings of the Twelfth Systems Administration Conference (LISA '98) Boston, Massachusetts, December 6-11, 1998

[2] Lawrence O'Gorman"Comparing Passwords, Tokens, and Biometrics for User Authentication "Proceedings of the IEEE, Vol. 91, No. 12, Dec. 2003, pp. 2019-2040 2003 IEEE

[3] Ravikanth Ponnapalli"Secure implementation of Enterprise single sign-on product in an organization" paper is from the SANS Institute Reading Room site.

[4] Si Xiong, Stockholm, Sweden"Web Single Sign-On System For WRL Company"

[5] "Best Practices for Integrating Kerberos into Your Application" MIT Kerberos Consortium. Ver. July 23, 2008

[6] "A More Secure Front Door: SSO and Strong Authentication" report by Improvita.

[7] Khalid Bashir And Saman Asif"Important Considerations For Single Sign-On Solution"In International Journal Of Multidisciplinary Sciences And Engineering, Vol. 1, No. 1, September 2010

[8] Bernardo Machado David, Anderson C. A. Nascimento, Rafael Tonicelli "A Framework for Secure Single Sign-On"

[9] Kirstie Hawkey, Konstantin Beznosov, University Of British Columbia" Investigating User's Perspective Of Web Single Sign-On:Conceptual Gaps, Alternative Design And Acceptance Model" in ACM 2012

[10] Arul Princy "A Survey on Single Sign-On Mechanism for Multiple Service Authentications" IJCSMC, Vol. 2, Issue. 12, December 2013

[11] Prashant Kumar Gajar, Arnab Ghosh And Shashikant Rai "Bring Your Own Device (Byod): Security Risks And Mitigating Strategies "Volume 4, No. 4, April 2013 Journal Of Global Research In Computer Science

[12] C. Ramakrishnan, S. Dhanabal" Security Analysis of a Single Sign-On Mechanism For Distributed Computer Networks ",IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. III (May-Jun. 2014)

[13] Yaser Fuad Al-Dubai & Dr. Khamitkar S. D"Kerberos: Secure Single Sign-on Authentication Protocol Framework for Cloud Access Control"Global Journal of Computer Science and Technology: B Cloud and Distributed Volume 14 Issue 1 Version 1.0 Year 2014

[14] Madhavi A. Indalkar ,Ram Joshi "Efficient and Secure Single Sign on Mechanism for Distributed Network "International Journal of Computer Applications (0975 – 8887) Volume 99– No.8, August 2014

[15] Manoj V. Thomas, Anand Dhole, K. Chandrasekaran "Single Sign-On in Cloud Federation using CloudSim" I. J. Computer Network and Information Security, 2015

[16] Daniel Fett,Ralf Küster,Guido Schmitz "SPRESSO: A Secure, Privacy-Respecting Single Sign-On System for the Web" in ACM 2015