An Assessment on Integration of Single-Sign-On Technologies for Military Environment: A Fit- Viability Model

LK Alahendra[1], WMIL Wasalage[2], SPP Pakshaweera3, Nandana Pathirage[4]

[1,2,3,4]*Kotelawala Defence University, Sri Lanka,*
[1] kdu-29-ict0129@kdu.ac.lk, [2] kdu-29-ict0121@kdu.ac.lk, [3] hoditm@kdu.ac.lk,[4]nandana_pat@yahoo.com

Abstract*—With the creation of web-based technologies, single sign-on has emerged as an important and central architecture solution for enterprise applications. As security breaches become increasingly more frequent, Minimizing user access to back-end systems and web applications without impacting legitimate usage is more important than ever before. As more web-based applications are deployed, Single Sign-On (SSO) solutions that have the capabilities to provide authentication, management, access control, and logging across the complete front- and backend e-business chain will become increasingly more important to Information Technology (IT) professionals. Furthermore, arrival of networking and internet has necessitated the use of numerous authentication techniques as password inflation has severely undermined the protection offered by a single password. Writing down and sharing passwords, use of regular passwords and similar practices greatly undermines the security of a network. Password issues also hinder productivity of the workplace and create redundant costs to the organization.*

Even though, SSO is a two-edged sword. SSO will degrade the security if it has not being deployed properly and SSO isn't a security panacea in and of itself, it can make positive contributions to an enterprise information security program. Since SSO can have positive impact on the secure systems, establishment of SSO for military environment based organizations can be taken into consideration with the aim of enhancing the productivity and secureness by eliminating the issues in using several usernames and passwords for separate systems. In this research, the feasibility of using SSO technology for military environment was investigated and potential risks were identified in the prevailing system authentication.

The research was conducted using a mixture of quantitative and qualitative methodologies within an overall inductive framework. To elicit quantitative values necessary for the research, questionnaires, and document reviews were used. To elicit qualitative values, interviews, observations and case studies were used. Then, inductive and deductive reasoning were used to theorize the findings appropriately and to generate outcomes.

The feasibility of such integration was analyzed from technical, financial, operational and organizational perspectives and based on the findings; a model has being developed for the integration of SSO technologies for military environment with appropriate security measures using a mix of available SSO technologies, would be productive and successful in military environment.

Keywords**:** Single-Sign-On, Military Environment, SL Army

I. INTRODUCTION

In the past, when a computer user wanted to work with the required resources he had just to remember one password. The increasing of networks, the development of the internet, and the ability connect different systems through expanded servers caused for a number of individual authentication necessities. It's a bad situation that when the systems and applications were increasing, there occurred problems in using passwords, as today most of the users have a habit to write down their passwords, to create passwords which have a risk of identified by others. The worst thing is the reuse of old passwords and to share them with others causing security problems in the organization.

In recent times, for example, research organizations including Gartner (2006), Giga Information Group, and Meta Group have shown that anywhere from 15 percent to 45 percent of all help desk requests are related to forgotten or expired passwords (Bigler and Mark 2004). Moreover, the Securities

Industries Association, a Wall Street trade group, discovered that users spend an average of 44 hours a year logging onto an average of four applications a day, further harming productivity (Safarulla and Kavitha D 2005)

A. An Overview to SSO

Figure 1. Legacy Approach Vs SSO Concept
Source: (Oracle, 2008)

Historically, SSO is quite an old concept that was developed to reduce the number of logins between various systems. According to single sign-on design the multiple logins a user needs to perform are turned into a single operation. In practice this will probably never be the case, but ideally a user should be able to log on once and further authentication requests would then be serviced automatically by the software rather than the user. Here, the user is relieved of needing to memorize multiple passwords (Credentials) as an application is presented with the data needed during a login, like passwords and username, email, or intranet proxy logins.

SSO has become increasingly famous in recent years, especially in establishments that employ web portal interfaces to facilitate third-party and backend systems like enterprise resource planning and consumer relationship management. There should be a stronger authentication for the SSO software when working with higher risk applications and information, like payroll system which includes digital certificates, security tokens, smart cards, biometrics or combinations.

Given the expanding use of this technology, internal auditors should consider familiarizing themselves with SSO and understand how it alters the authentication process. Auditors should also examine the potential risks associated with this type of authentication in the event of an SSO implementation at their organization.

B. SSO Architecture

The SSO software on a user's PC enters logins and passwords on behalf of the user. But where does the software find that information. In the latter case, data resides in a secure location outside the user's PC, basically for reasons of control (it should be possible to deny or grant access remotely) and user mobility. Following depicts the main three architectures to get SSO information like logins, passwords and access rights (Jerphanion 2008).

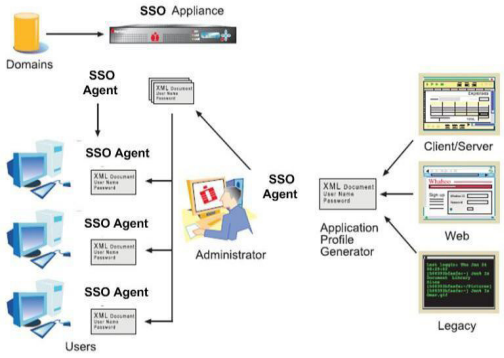


Figure 2. SSO Enrollment and Deployment
Source: Imprivata official website 2009

- SSO server

The information is stored on a server, for instance a Windows or Unix server, that is generally dedicated to this task. The client on the PC queries the server whenever necessary. This server is often duplicated for high availability, although cache mechanisms on the PC can compensate for temporary unavailability. Therefore, start-up costs must be taken into account: servers (but you can dedicate an existing server) and software installation. In a distributed architecture, the number of these servers may be high.

- SSO appliance

With a combination in software and hardware this is introduced as a variation of the SSO server solution, which decreases the costs in Software deployment. On the other hand, it is not possible to install the software on an existing server, which may increase the deployment costs. Finally, not like in server, it is often impossible to add memory and disk on an appliance.

- Enterprise directory

SSO data is simply stored, in encrypted form, in the directory that already exists in most companies. For instance, the Active Directory base through which user's access Windows. Therefore, you do not need to install any server or appliance. Your PCs are already configured to access the information, since they already access the directory. Deployment costs are reduced significantly.

In such architecture, the directory is typically completed with some administration stations and a database in which the log of activities is stored (for audit). But these modules are not an obligatory and critical passage point for the entire system, unlike "server" and "appliance" architectures.

C. Research Question

The research question around which this research is based is presented below:

How can the SSO technology integrate with military environment with concentrating on high security procedures and to increase the productivity?

II. LITERATURE REVIEW

A. Single Sign On Technologies

The idea of reducing the number of logins for a user has been addressed differently by manufacturers of SSO products. Unfortunately there is no set standard or ideas on how to tackle the issues of SSO consistently; since today's modern production environments tend to be diverse in their requirements.

Some of prominent technologies used to produce SSO products and their suitability to different network environment are discussed below.

a. *SSO with Lightweight Directory Access Protocol (LDAP)*

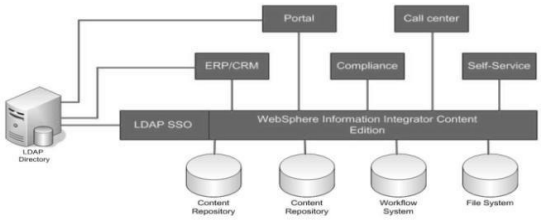


Figure 3. LDAP architecture

Source: IBM 2005

SSO systems mostly use LDAP authentication. The enterprise user logs on in the morning and sees normally a form based enterprise login screen. The user enters in their id and password. Through an encrypted link, the SSO software sends these data to a security server. By submitting user ID and password, the security server log on to the LDAP server on behalf of the user and continue with any other authorization and permit the user access to required resources.

The above figure shows the way a LDAP SSO system may correspond with extant LDAP architecture of an organization. In above example, users can access one or more applications which necessitate access to different repositories. To access dissimilar workflow systems and repositories these applications authenticate to enterprise or departmental LDAP directory which contains the encrypted user credentials.

- Use of LDAP Directories in LDAP Authentication

LDAP directories and LDAP authentication is one of the enterprise user infrastructure cornerstones. As the enterprise has digitized and opened itself up to customer, vendor, wide-spread employee and business partner access to pieces of most enterprise applications, the need to identify who the user is has significantly increased from a security viewpoint. Who is the user trying to entrée an applications? What is the potency of authentication by which the applications can trust the user trying to entrée the applications? What are the user's approval privileges?

The frequency of user authentication has also been increased making it normal to have thousands of identity look-ups per minute in large enterprise. The above are the reasons why LDAP directories and authentication have taken on such a dominant role in enterprise authentication.

- How LDAP Authentication Works

LDAP is formed on a client-server model. Information about people, organizations, and resources accessible to LDAP clients are made by LDAP servers. It defines operations that clients use to search and update the directory. An LDAP client can perform these operations, among others:

- searching and retrieving entries from the directory
- adding new entries in the directory
- updating entries in the directory
- deleting entries in the directory
- renaming entries in the directory

As an example, to update an entry in the directory, an LDAP client put forward the distinguished name of the entry with updated attribute information to the LDAP server. The LDAP server uses the distinguished name to find the entry and performs a modify operation to update the entry in the directory.

To perform any of these LDAP operations, an LDAP client needs to establish a connection with an LDAP

server. The LDAP protocol specifies the use of TCP/IP port number 389, although servers may run on other ports.

The LDAP protocol also defines a simple method for authentication. LDAP servers can be set up to restrict permissions to the directory. Before an LDAP client can perform an operation on an LDAP server, the client must authenticate itself to the server by supplying a distinguished name and password. If the user identified by the distinguished name does not have permission to perform the operation, the server does not execute the operation.

b. *Public Key Infrastructure and Digital Certificate*
Public Key Infrastructure (PKI) is the most popular, guaranteed and assured authentication technology used in most SSO products as the key authentication method.

The collection of policies, people, procedures, facilities hardware and software that permit the issuing, management and distribution of public key certificates is called a Public-Key Infrastructure (PKI). A PKI manages relationships and establishes trust in a distributed environment. They achieve this by controlling and managing the utilization of cryptographic certificates and keys. Without a PKI, cryptographic-based security could not be employed to support most ecommerce applications (Lannerstrom, 2000).

- Integration of PKI Technology in an Application

Majority of PKI-technology elements operate in networks as application services. The developer's toolkit element is the exception. The treatment of protocols and cryptographic services in support of application programmers is done by the toolkit. The toolkit consists of a collection of local software providers who implement security criterion and a high-level interface permitting developers to PKI-enable the applications. The toolkit is important because (certicom, 2001):

- It takes burden of cryptographic operations away from application programmers and reduces resources and time required to incorporate security with applications.
- It allows regular security integration throughout all applications.
- It increases the flexibility of the developers to meet new requirements with the evolution of the application environment.
- Introducing Enterprise PKI

The every specific security needs of a business with online operations can be fulfilled by a thoroughly implemented PKI. PKI offers management of certificates, relationships and keys needed to make use cryptography in business. Now it is widely believed that cryptography provides the best security to online applications if they are PKI-enabled. The applications with access to PKI resources such as certificate directory certification authority and certification authority and capability of processing the objects which are usually exchanged within a PKI such as public-key certificates and digital signatures can be PKI-enabled.

A Thoroughly Implemented PKI Fulfills these Requirements of Online Businesses
- Authentication: to avert masquerading, substantiate the identity of entities (individual, organization, role, and device) before online exchanges, transactions, or permitting admission to resources.
- If an application has PKI facility, it uses public key certificate and digital signature processes to validate individuals, nodes, servers or any entity partaking in the business flow.
- Authorization: to avert unauthorized activity, validates whether an entity has authorization to partake in a transaction, an activity, or is permitted to access resources.

PKI-enabled applications have the ability of cross-referencing verified identity of an entity (which was validated through a public-key certificate) with a privilege (or policy-enforcement) list prior to authorizing (denies or grants) request of an entity for partaking or admission.

- Non-repudiation: offers the tools which easily prove that a person has partaken in a specific transaction. PKI-enabled applications binds participants to their activities and the time and date in which the activity transpired using their capability to process public-key certificates, authenticate digital signatures and keep a record of transactions.

- Privacy: averts unauthorized access or eavesdropping. In case of a heightened privacy concern, PKI-enabled applications can encrypt data.

Though the encryption services are not supplied by PKIs, the exchanging and managing of encrypting and decrypting keys are necessary services typically offered by PKIs.

- Integrity: averts data tampering, prevents accidental or purposeful data alteration in storage or during transportation.

Digital signature is a favored method of preventing data tampering. Positive verification of a digital signature means the transition integrity is still intact while if the transaction data has been modified, the digital signature will fail to yield a positive verification and the data will eventually be discarded. PKI-enabled applications can apply a digital signature to transactions, in order to verify the transaction integrity. These necessities are best fulfilled by PKI-enabled application which provision the services (access, audit and cryptographic) usually offered in operational PKIs.

- PKI Technology and Architecture

Good PKI architectures need to be openly documented, support standards and offer lucid application interfaces. The collection of PKI technologies consist of hardware and software which implement the operations of the

- End-Entity Application (EE)
- Registration Authority (RA)
- Certification Authority (CA)
- PKI Directory

- Basic PKI Architecture and Data Flow

The major technical components and operational flow of a PKI are shown in Figure 4.

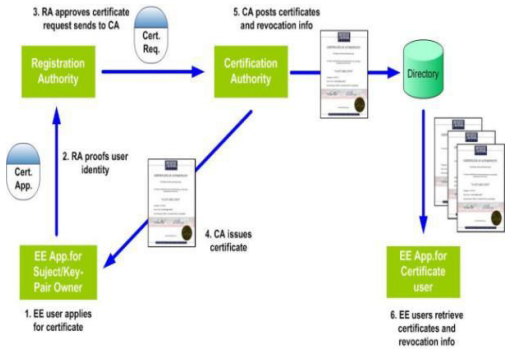


Figure 4. Basic PKI Architecture and data flow

c. *SSO Tickets*

Another Key technology associated with SSO concept is the use of SSO tickets.

In an office environment, where users interact with a range of applications and systems, the environment does not usually preserve the user context using multiple processes, computers and products. The need to verify the initiator of the original request makes user context crucial to offer single sign-on capability. To surmount this difficulty, Enterprise SSO offers an SSO ticket (not a Kerberos ticket) which applications could use to get credentials that match the user who made the original request. A SSO ticket is not enabled by default.

On a request, a ticket containing encrypted username of the concerned user, domain name and the expiration time of the ticket is issued to an authenticated Window user by the SSO system. A ticket is only issued to the user who made the request (cannot make requests for others) and by default a ticket has a life time of two minutes. The SSO administrators have the ability to modify the life time of tickets.

If applications authenticate the requestors' identity, they redeem tickets to acquire the requestor's user credentials. The tickets are redeemed by applications from SSO systems in these ways (Microsoft, 2004):

- Redeem only: a request to redeem a ticket initiated by an application need to contain the ticket and the affiliate application name to which a connection is desired. Application administrators of the particular affiliate application, SSO administrators, or SSO affiliate administrators can only redeem tickets. The use of redeem only is only recommended in the cases where there exists a secure sub-system between the applications which issues and redeems the ticket. Only application administrators of specified affiliate applications can redeem tickets for user.
- Validate and redeem. Tickets carry information about the requestor. Here, the SSO service substantiates that the message sender and the ticket user are the same prior to the redemption of the ticket.

Though ticket time-outs can be disabled by SSO administrators on a per-affiliate application basis, it is not advisable because, for these applications, tickets would never expire. In situations that require disabling ticket time-outs, a secure sub-system between the front and end of the SSO system

where the ticket is issued to the adaptor and is redeemed is a must.

SSO affiliate administrators could specify that a ticket is allowed and substantiation of the ticket is required on a per affiliate application basis but if the SSO administrators specify at the SSO system level that the ticket validation is necessary; the SSO affiliate administrators are not able to deactivate this option at the affiliate application level.

B. *SSO and Military Environment*

SSO systems are often based on complex systems management applications. As any organization's systems enlarges and multiplies, requirement of having each of its own username and password emerges. As a remedy, SSO eases the burden of having to spend time logging on to each system individually. But at the same time, if SSO is compromised, it gives the keys to the castle to a malicious user.

Military environments are having much credential information which is important in all aspects. Therefore secureness of the information system must be at a higher level.

Implementing SSO for a military environment has its own consequences. But the emerging drawbacks can be reduced and can be obliterated by deploying the system under secure SSO architecture.

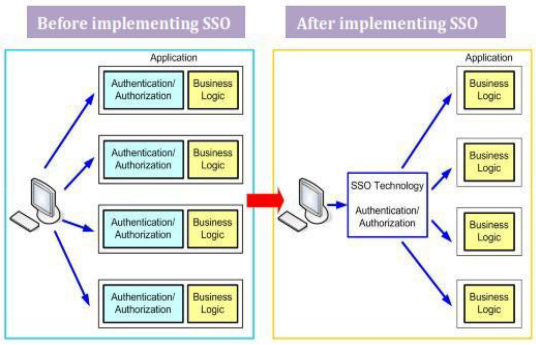
C. *Major Benefits and Drawbacks of implementing a SSO in Network Manager Perspective*

Network manager should fully contribute to achieve business objectives of their organization. When Organization plan to implement a Technology like SSO, then Network Manager, need to think how these newly introduced concepts are beneficial to business and their suitability to existing environment. Following are the major areas a network manager has to mainly concentrate on when implementing a SSO,

1. Need of reducing development time & man-hours

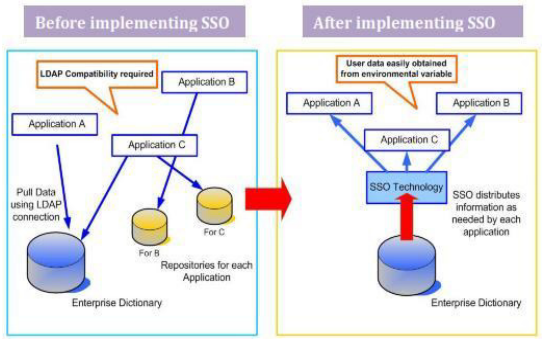
- *With the use of SSO, we are able to consolidate authentication &authorization*

SSO technologies reduces the overall development time and man hours and streamline the organizational applications by consolidating authentication and authorization processes of an organizational network.



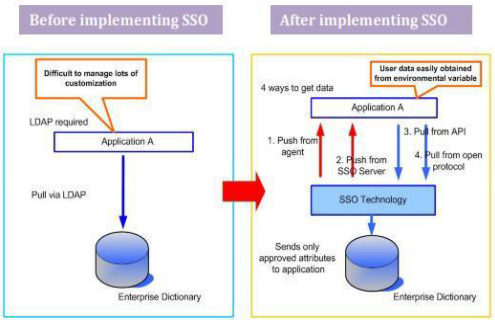
- *With the use of SSO, we are able to distribute user attributes*

Another advantage of SSO technology is its user attribute distribution function which gives the organizational network the luxury of not needing a repository while reducing the application development time.



- *With the use of SSO we can makes maximum of our Enterprise Directory.*

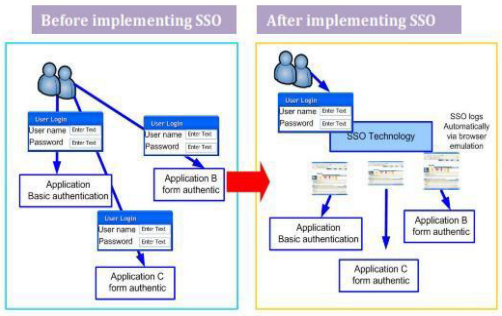
Normally, Most of the organization applications work with LDAP feature, which needs a great amount of customization. Not only that there is also the risk (to enterprise directory) of direct access, & Directory performance is constantly a concern. With the use of SSO, we're able to pull Enterprise Directory data right from the environment variable, quickly & in a using of different varieties of formats.



2. Need of improving usability

- *Cut down on IDs & passwords with the use of SSO*

Another key advantage of using SSO is that it reduces the number of IDs and passwords users have to use in performing their tasks on the network. Thus, this greatly reduces the exposure of passwords to unwanted individuals as users do not need to write down the Passwords they need to remember.



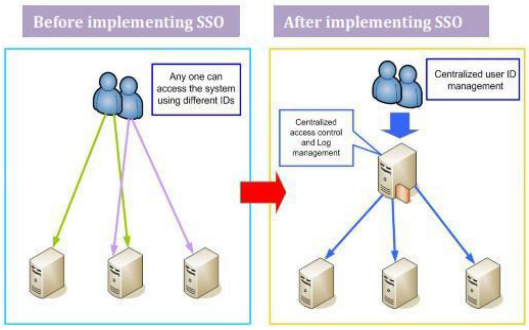
- *With SSO's dynamic menu, user access privileges are clear*.

SSO can present application menus dynamically, depending on the access privileges of the group to which the user belongs. Further, by installing the Dynamic Menu Portal (a standard feature), you can also generate content user by user.

3. Need of strengthening our security level

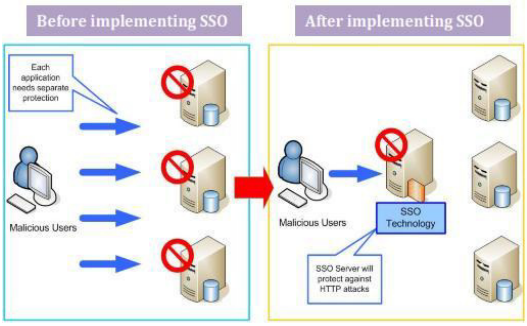
- *By Centralizing ID and log management, makes it easy to concentrate on the issues of unauthorized access and private information leaks.*

Id management is vital to overall network security. By implementing SSO, management of user IDs can be centralized, providing more time to focus on measures to prevent unauthorized (illegal) access & disclosures of private information.



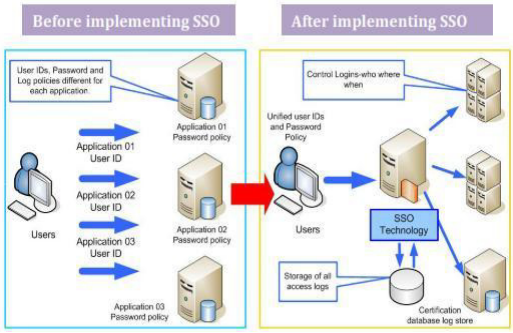
4. Need of simplifying our management task

- With the implement of SSO, we can assure protection against HTTP attacks and can be consolidated, instead of being implemented one application at a time.Because a firewall can't give exact protection against HTTP attacks, it's requiring to perform measures at the Web application level. With the implement of SSO in front of our Web applications, we are able to consolidate implementation of those measures in one place.



- *SSO provide feature of creating uniform user ID, password & log policies*

With each application which is relates to our organization carrying its own user ID, password, & log policies, management can become grandly complex. With the implemented of SSO, user ID, password, & log policies are centralized, making management easy.



Although there were benefits in considering the SSO implementation; as a network manager, from a management perspective several challenges of using SSO technology can be detected. These challenges need to identify with the business objectives of the organization.

The main disadvantage of the SSO technology is the time delay it incur when login in to an applications with SSO technology. One password is sufficient to log in to multiple applications. When needing to log in to one application, with SSO technology, Users have to wait until SSO software authenticates with all the applications it can log into creating considerable time delay. It may directly effect to the users efficiency.

Another disadvantage of the SSO technology is the inability to find local support in case of system disruptions. SSO technology is globally acclaimed technology but it is difficult to find local support in case of software failure. For an example due to a technical problem if users could not log in to any application, there needs to be either local or global support from vendor to solve the problem. Most of the time we cannot fixed technical issues locally definitely we have to get assistance from our product vendor as soon as possible unless it would definitely affect the productivity and performance of entire process.

It Adherence to LDAP principles is one of the challenges in using SSO technology. Though LDAP have many extensions, most vendors do not implement all these parts of a LDAP hindering the optimum performance of a LDAP and causing scalability. But sophisticated enterprise web environments needs strong LDAP support to make the full use of LDAP capabilities.

Firewalls and VPNs offer important security protections, but they have not been optimized for customer, partner, and reseller utilization on the extranet. Firewall protection and authentication services are geared towards employee usage scenarios and, in order to create comparable extranet user sign-on privileges, require individual set-up by the firewall administrator for each user or user group. As important as firewalls and VPNs are, however, they do not address SSO and 3A capabilities, so cannot be considered as user-friendly portal security solutions by themselves.

III. METHODOLGY

Considering the nature of the research, as the chosen research methodology for the research, a mix of quantitative and qualitative methodologies was used within an overall inductive research paradigm. The characteristics of the quantitative and qualitative methodologies and the variables of the research necessitate a coherent synthesis between these two methodologies.

The main stimuli behind using such a combination is that the research demands the predictive generalization of the feasibility of integrating SSO technology for military environment and develop an understanding of socio-economic dimensions of SSO technology and military domain by studying the problem environment first hand and interprets related phenomena in terms of meanings employees bring to them.

Therefore, this combination made the research more in-depth and productive. Within the larger frame work of selected methodology, several research techniques were employed to gather the necessary data.

Finally, to theorize and reach conclusions, an inductive approach which uses data to formulate theories was applied to the qualitative data and a deductive approach which applies a tentative hypothesis to the concerned data to ascertain its validity was applied to the quantitative data.

The selection of a sample for the research was done based on the non-probability sampling technique. The reason for selecting non-probability sampling technique for determining the sample population is that the entire research population consists of a limited number of individuals. Therefore, members of the sample could be selected based on subjective judgment of the researchers. This ensured the accuracy and applicability of the data gathered from the sample.

Following this line of reasoning, the authorities of the SL Signals Core, SL Artillery, SL Engineers, SL Service Core located at Panagoda, SL Military Academy at Diyathalawa and SL Singha Regiment at Ambepussa were the primary data spotlights. In selecting members for the sample population from the authorities, their characteristics and attributes such as, experience, authority level and the

knowledge, the position in the commanding chain, amount of hands on experience and the willingness to participate in the research were considered.

IV. DISCUSSION OF DATA

In the data collection process, mainly the employees' methods of managing user accounts, willingness to adapt to SSO technologies, their experience and the understanding on SSO technology were questioned. Feedbacks from the employees lead to the conclusion that integration of SSO technologies in military environment will come in handy to improve their efficiency since day by day number of logins that employees has to deal are increasing.

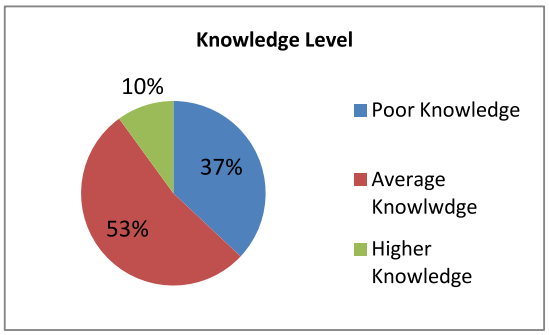


Figure 5. Knowledge Level

As shown in Figure 5, most of the users had an average knowledge about the use of SSO technologies. They had an understanding about the basic idea on how SSO work and some benefits of integrating it in their military environment. Since majority of users had sound knowledge about SSO technology, it leads to a conclusion that they will be comfortable in using this technology in their environment.

Figure 6 represent approximate values for number of accounts that a user access within a day. It was noticed that users generally access 0 to 10 accounts mostly. This may include internal applications to the organizations as well as web applications accessed via internet. When the number of accounts to access increases it is difficult to manage usernames and passwords for each account.

Another issue occurred when the number of user accounts are increasing is; every user may not enter each account. Therefore those account details can be easily forgotten and lost. It may also lead to auto deactivation of accounts.

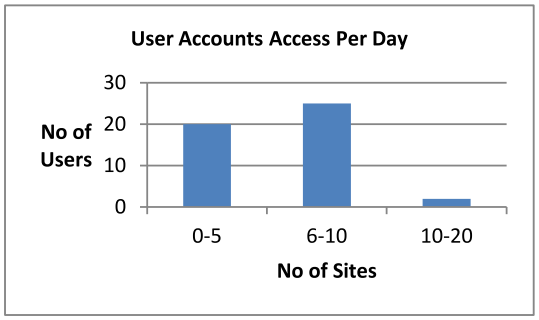


Figure 6. User Accounts Access Per Day

In addition, normally a single user has to have multiple numbers of authentication methodologies to sign in for the particular systems/sites that they use. The most prominent mode of authentication technology is the username/ password methodology. Without the SSO implementation, system users have to enter their credentials several times when they logging to particular systems. The Figure 7 depicts how the system users initiate their username and password combination for the systems that they use. Several combinations how the users use were identified. It was clearly visible that most of users use the same password for different systems or sites with different usernames.

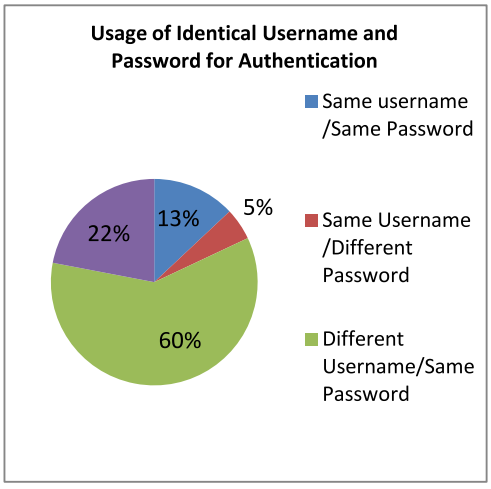


Figure 7. Use of Identical Usernames and Passwords

Most of the internet based systems are enabling with the browser option "Save Password". Usage of this option is very rarely (3%) can be seen in the office environment. Considering the home environment system usage, most of the system

users are using the browser option for their convenience. But about 5% of the home users are not using the browser option since they are not afforded with their own personal computer for system logins.

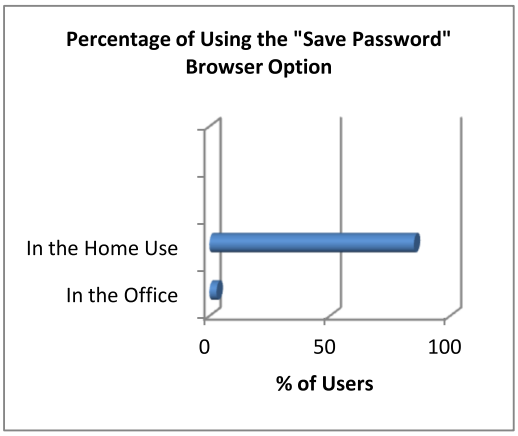


Figure 8. Percentage of Using the "Save Password" Browser Option

Figure 8 illustrates most of the users do not use the option “save password” in their office environment. This means that they are entering the same username and password multiple times for each site which may lead to several issues if the number of accounts to maintain is high.

Managing the username and password for separate sites/systems is one of the major problems which are faced through the traditional sign on concept. Therefore system users have taken different measures to manage the username and password. Over 50% of the users are using a notepad file to keep track of their user account details while a considerable percentage is keep remembering the details.

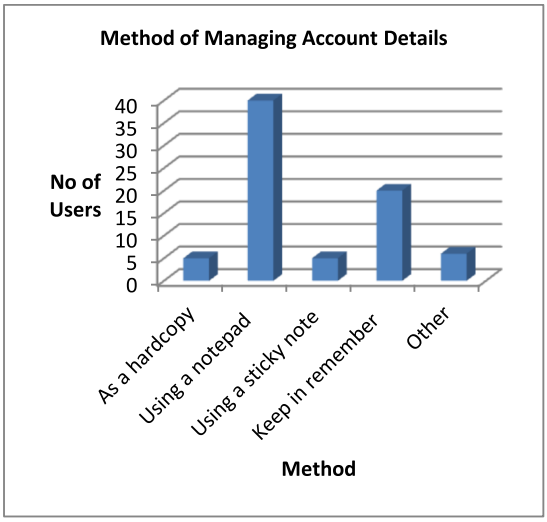


Figure 9. User Account Details Management Methods

A conclusion can be arrived that once the number of user account details are increasing people tends to keep the details of their accounts as softcopies in their own machines which is a security threat from their perspective.

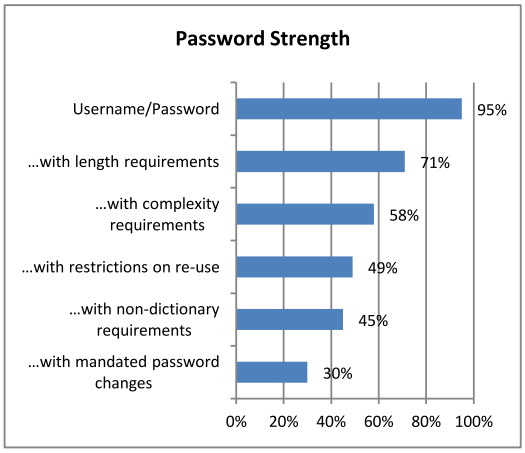


Figure10. Strengths of Passwords Implemented by users

Figure 10 indicates how the users considered about strengthening the security of the passwords. Even though these things improve the safety of the password, creates complicated to the end users. A disadvantage in passwords which are difficult to be guessed is difficult to remember. Creating problems in security natural copying mechanism take steps to write them down and get help from the help sector with unnecessary costs

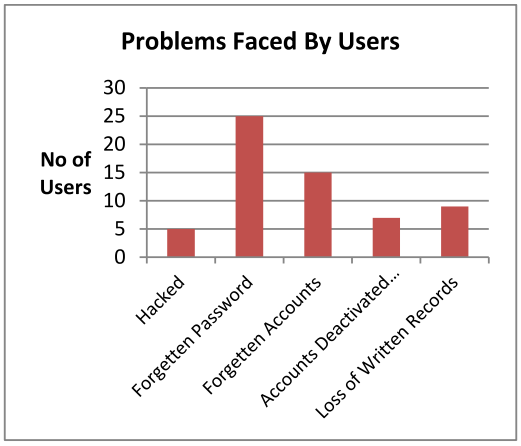


Figure11. Problems Faces by Users

As the Figure 11 depicts users of computer systems can face many problems with regard to personnel user accounts. It is also possible that when the number of accounts that a user has to maintain increase severity of above issues can be increased. In summary, it is evident that the current practices are time consuming and can lead to security problems as well as some inefficiency.

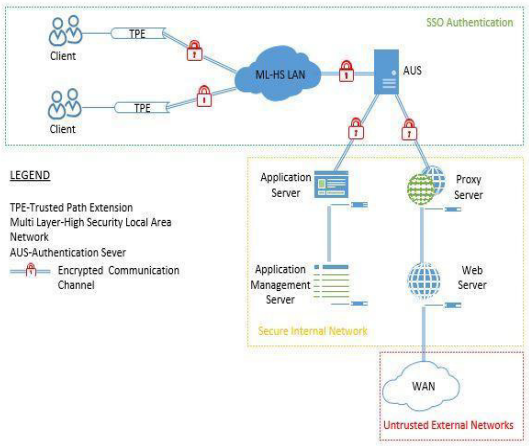
V. CONCLUSION

Based on the findings, a model has being developed for the integration of SSO technologies in military environment. Security and functionality were the main driving factors in developing the model. Others factors include performance, reliability, and the feasibility of integration into the existing military network.

In order to enhance the security, in the solution, a proper integration between SSO technology and military domain is required. More specifically, a high secure authentication protocol is facilitated by the SSO server through mitigating technological differences of different components. Therefore, structural diagram of integration architecture which facilitates the strategic improvements identified in above sections is presented in Figure 12.

According to the proposed model, users must authenticate to the Authentication Server (AUS) prior to accessing the network and any network applications. A Trusted Path Extension (TPE), attached to each client machine, creates a secure, unforgeable communications path to the AUS that is used for user authentication and other security services. TPE will communicate with AUS through high secure encrypted communication channels using RSA cryptosystem with strong 256-bit encryption, 2048-bit root.

Figure12. Proposed Model



TPE will establish a secure connection with the AUS and then AUS will request for the client username and password. TPE will send the username and password to the AUS server and the AUS server will confirm the authentication completing the authentication process.

After a user has successfully authenticated to the AUS, the user can access network applications running on the various Application Servers (AS) that are part of the ML-HS LAN.Security models such as the Biba model (for integrity) and the Bell–LaPadula model (for confidentiality) allow one-way flow between certain security domains that are otherwise assumed to be isolated.

After the initial authentication, for the security purposes AUS contains 2 main components Trusted Path Server (TPS) and Secure Session Server (SSS).TPS component creates a trusted path to a remote client through which identification and authentication, security session level negotiation, password modification, and other trusted path services are performed.

SSS process is used to launch untrusted application services (such as web servers or mail servers) running at the same security level as the client requesting the service.

As a conclusion, it is safe to say that if any military organization integrates with SSO technology following the suggested model; it would bring

security, productivity and financial benefits to the organization.

LIST OF REFERENCES

Administering Oracle AS Portal: Single Sign-On (2008), Oracle Technology Network, viewed 2nd February 2014, http://www.oracle.com/technology/products/ias/portal/getstart/1014/a_port04.htm

Bigler, M., (2004), Single sign-on: with SSO technology, managing user access across multiple applications can be a one-step process, viewed 4th February 2014, http://findarticles.com/p/articles/mi_m4153/is_6_61/ai_n8583698/pg_1?tag=artBody;col1

Gartner (2006), the value of Enterprise Single Sign On, Podcast for Business and IT Professionals - Gartner Voice Research Group, viewed 4th February 2014, http://www.gartner.com/it/products/podcasting/asset_145695_2575.jsp

IBM WebSphere Information Integrator Content Edition, 2005, Single sign-on overview, IBM Information center home, viewed 5th February 2014, http://publib.boulder.ibm.com/infocenter/wsiihelp/v8r3/index.jsp?topic=/com.ibm.websphere.ii.federation.security.content.doc/prod_overview/iiyva_ssover.htm

Jerphanion L.D., October 2008, Enterprise Single Sign On, Evidian Group, viewed 5th February 2014, http://www.evidian.com/iam/enterprise-sso/index.htm

Lannerstrom S., 2000, Basic elements of PKI, Sonera SmartTrust, viewed 7th February 2014, http://www.aukbc.org/bpmain1/PKI/elementpki.pdf

Microsoft.com 2004, Microsoft Host Integration Server 2004 SSO Tickets, viewed 7th February 2014, http://msdn.microsoft.com/en/us/library/ms945070.aspx

Safarulla A.N. and Kavitha D (2005), Win in the Flat World, Linux Single Sign On –Maximum Security, Minimum Cost, Infosys Technologies Limited, viewed 2nd February 2014, http://www.infosys.com/linux/knowledge/Linux-SSO.pdf

Sonia Bui,September 2005,SINGLE Sign-On Solution For Mysea Services, Naval Postgraduate School Monterey, California.

BIOGRAPHY OF AUTHORS

[1]Lashini Alahendra is a 3rd year undergraduate following Bsc in ICT degree program at General Sir John Kotelawala Defence University.

[2]Ishanka Lakshan is a 3rd year undergraduate following Bsc in ICT degree program at General Sir John Kotelawala Defence University.

[3]Suresh Pakshaweera is Head of the Department, Department of IT and Mathematics, KDU, Sri Lanka. His research interests include Information and Communication Technology, Geographical Information System and Remote Sensing. He has more than 20 year experience in IT infrastructural, product and service development in Sri Lanka Army.

[4]Nandana Pathirage is a lecturer of IT and Mathematics Department, KDU, Sri Lanka. His research interests include Strategic Information System Planning, Management Information Systems and Project Management. He is currently reading for PhD at KDU.