ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 3, No. 5, 492-500 (2018)

www.astesj.com

Special Issue on Multidisciplinary Sciences and Engineering

ASTESJ

ISSN: 2415-6698

Towards Adoption of Authentication and Authorization in Identity Management and Single Sign On

Ujjwal Joshi*, Sangwhan Cha, Saeed Esmaili-Sardari

Computer Science, Harrisburg University of Science and Technology, Pennsylvania, USA

ARTICLE INFO

Article history:
Received: 10 September, 2018
Accepted: 04 October, 2018
Online: 25 October, 2018

Keywords:
Authentication
Authorization
Single Sing On
Identity Management

ABSTRACT

Identity and Access Management (IAM) and Single Sign on (SSO) are two security concepts that are related to each other. IAM governs the user access in an organization whereas SSO facilitates the user by authenticating to one centralized application and not having to re-authenticate when trying to access other applications. This paper addresses the different benefits that an IAM and SSO tool can provide to reduce the security risk within an organization. Since, authentication and authorization are one of the major concerns in the cyber security; this paper analyzes common problems that are faced during authentication and authorization. We have also analyzed prior researches that have been done in the IAM and SSO space along with conducting a survey to understand the different issues and benefits of IAM and SSO. From the survey that has been conducted, we have addressed different issues when implementing IAM and SSO solutions along with understanding the architecture, in which these solutions have been deployed into. The surveys conducted have been compared with prior researches done in IAM and SSO space to understand the benefits that the solution provides. The results from the survey have been analyzed to provide the best practices when implementing IAM and SSO solutions along with the benefits provided by the solution.

1. Introduction

Identity Management also commonly known Identity and Access Management (IAM) refers to the set of processes that can be applied to grant right access to the right people within any corporate enterprise environment [1]. Businesses today, implement IAM solutions so that it provides them with the framework that can manage user IDs and passwords along with solving problems related to the challenges associated with managing accesses and permissions of multiple user IDs [2]. IAM solutions also provide different auditing capabilities that enable the managers and higher officials within organization to keep track of the different accesses that their employees have [2]. A terminated employee still having access to the organization resources can cause certain damage to the organization so having an IAM system can reduce the risk associated while manually removing or adding users to different systems. Today, architectures within an organization can be categorized based on whether their applications are deployed in the cloud or within their own network also known as on-premises [1]. This increases the complexity of managing users and granting accesses to them due to increased privacy and security risk [3]. Although IAM systems can remove and create access, the user still needs to enter their user name and password to access the systems that they were provisioned to by the identity management systems. Remembering passwords and usernames can lead to issues where the user can forget their credentials or lose their credentials for certain system, which might fall into the hands of an intruder. Single Sign On (SSO) provides a better functionality for managing authentication and authorizations to applications, by not having the user re-enter the credential every time they need to login [4]. SSO provides a single source of authentication mechanism which provides the user a single platform to enter their credentials to access different applications and also discourages the need to maintain multiple credentials to access different systems [5]. IAM and SSO solutions provide a secure way for businesses to manage and authenticate their users. This research explores the authentication and authorization mechanism that IAM and SSO provides with the view of providing better security while implementing these solutions. The research also explores the different models of architectures that an enterprise environment can have to recommend the best practices that can be followed while implementing IAM and SSO solutions.

*Ujjwal Joshi, 696 Fox Ave, Lewisville, TX, USA, 469-451-9885
ujoshi@my.harrisburgu.edu

https://dx.doi.org/10.25046/aj030556

Security is one of the major concerns that an organization faces today, as risk from cyber-attacks can damage an organization [6]. As business today are growing bigger and faster than anticipated, they are looking for new technologies that can provide a simplified solution for them to manage their user's accesses and resources. A user within an organization needs to have the right set of access to do their work and manually managing user accesses is not a suitable practice for an organization since there can be gaps such as assigning wrong or incorrect accesses [1]. Moreover, manually adding and removing accesses can lead to issues such as forgetting to remove accesses when users leave organization or adding accesses when users join organization.

Since authentication and authorization are one of the major components of IAM and SSO, the need to provide access and manage user authentication are highly in demand. Corporate environments today are complex because they have users and data scattered in different applications and servers. Therefore, there is always a need to manage users efficiently so that the organization is less vulnerable to intrusions and outside attacks. Most organizations today need the security knowledge that can help them to investigate the security solutions that are available. Business always makes mistakes by believing the vendors or service providers rather than understanding their own infrastructure for their security purposes.

Lack of security knowledge and security principles are one of the common problems that organizations face today. By tradition software applications within an organization were supposed to be deployed within the organization boundaries [1]. However, today an organization cannot restrict itself to the traditional views and are deploying applications outside an organization boundary. Any application that is outside the organization boundary is not within the organization trusts zones and organizations do not have complete control over it. Since some applications are within the organization boundary and some are maintained by service providers, the complexity to sync users between application increases. As technologies are rapidly changing today, IAM is gaining a popular momentum as it is one of the key components when managing users on applications deployed within organization boundaries and outside organizations boundaries [3].The problem still lies on how business and organizations can securely manage users and their credentials for applications that are inside the organization and outside the organization boundaries. Since service provider's applications are managed by service provider's resources and application within organization boundaries are managed by organizational resources, manually adding the users and creating credentials can lead to gaps where the user may not have the right access. The complexity also increases when users try to access service provider's applications with different credentials which can lead to forgetting or losing passwords. Such complex situations can be managed by using SSO for authentication and authorization along with IAM for managing user accesses. However, not all the SSO and IAM may be feasible for an organization. Depending of the complexity of the organization infrastructure there is a need to do research which provides guidelines to business so that they know the check and balances that is required when implementing IAM and SSO solutions.

In this paper, we evaluate different criteria that an organization can have from the infrastructure and architecture perspective. The architecture depends on the number of applications that are hosted within and outside the organizational boundaries. The infrastructure is based on the number of employees that an organization has and the different kinds of policies that is applicable to each employee. Then, we categorize the organization based on architecture and infrastructure that the organization has. Depending on the categories that the organization fits into we analyze the different process that an organization can undergo to select the suitable IAM and SSO solutions. We also provide the guidelines on some of the best practices that the organization can follow to implement those solutions. However, this research does not recommend any solution that exists in the market today but provide more of a guideline that the organization needs to take into consideration while implementing IAM and SSO solutions.

The remaining of this paper is organized as follows. Section 2 presents related work. Section 3 describes the proposed approach. The experiments for the proposed approach are described in Section 4. Section 5 provides the concluding remarks.

2. Related Work

Authentication and authorization are one of the mechanisms used in computer security to validate if the user has the right credentials and permission to access a system. However, authenticating and authorization also known as identification, is one of the common problems in computer security [4]. Although many researches have been done to improve the authentication standards, passwords is still common authentication mechanism [4]. Using passwords as an authentication mechanism increases complexity in an enterprise environment since forgetting passwords from time and again can lead to inefficiency while accessing systems. Organizations today are also demanding systems that help them manage users so that end users can manage their private information more efficiently [7]. Identity management is one of the key components of an organization since it plays an important role in authentication and authorization [3]. Identity management refers to the process of managing identities so that each identity has the right set of accesses that is needed for them to do the required work in an enterprise environment [1]. Identity management consists of four major modules which are Authentication, Authorization, User Management and Central User Repository [1]. The authentication module deals with validating user credentials where the user can authenticate themselves by providing username and password or through other different authentication mechanisms such a Kerberos, SAML and so on [1]. The authorization modules provide the functionality of validating a user access to different systems. The user access can range from the group of permissions or roles that a user has to access the system [1]. The user management module provides functionality such as provisioning and de-provisioning of users, life cycle management to manage the user accesses, when the user joins the company till the time the user leaves the company. The central repository module delivers a one stop place for reviewing users and different access they carry along with different systems that IAM is integrated to and reading information from different other managed systems [1].The proper deployment of the four modules of identity management can result in building robust enterprise environment where processes can be automated and limited manual intervention is required.

An enterprise environment today, is not just restricted to application deployed within a particular network, but also includes various other applications on different vendor systems. Enterprises now are also moving their resources to cloud and are exploring the different cloud models. There are three cloud concepts which are gaining popularity such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [8]. The concept of SaaS, PaaS and IaaS has also changed the way different authorization and authentication mechanism worked. The mechanism to store identities across different systems using SaaS, PaaS and IaaS is also known as federated identity management [4]. With cloud-based applications and the need to access applications anywhere at any time has brought in changes in the traditional authentication mechanism and developed different standards that are also known as SSO standards. However, enterprise still use username and passwords as a common authentication mechanism and these can lead to certain problems. In password-based authentication the user passes in a username and password to prove they have the right credentials to access the system. So every time a user needs to access a system they need to enter the password. The use of password-based authentication and classical authorization techniques are described below

- Alpha numeric passwords are used which sometimes can be easy to guess so an unauthorized user may also access the system [4].
- Since different system may have different passwords the user has to memorize all the password or maintain a list somewhere else which can be stolen or lost
- Some system with password-based authentication allows grammars in passwords which provides a way for attacks like dictionary attacks [4]
- Two factor authentications can be a better approach but not all the systems follow two factors authentications.
- Once the user is able to authenticate the next process that happens is authorization which allows the user to access certain resources in the system.
- The authorization techniques for classical system are assigning permissions directly which is difficult to manage [4].
- RBAC (Role Based Access Control) is one of the mechanisms used in various systems to grant access to users for authorization [4].
- The RBAC solves the issues with permissions since permissions are assigned within the roles and roles are assigned to the users [4]. This reduces management risk since they only need to be aware of the roles that the user has.

SSO provides enterprises with a mechanism to authenticate and authorize users with a single password. Once the user logs into one system and authentication happens the users does not need to login again to access other applications [4]. This prevents user from having to remember multiple passwords for different applications. However, since there are many different standards that provide single sign on for users, there is a need to understand and analyze how different single sign on systems works and suits for a particular enterprise environment [4].

Today, there are different SSO and IAM solutions that are available in the market. Organizations need to understand how these solutions work for them based on their architecture and infrastructures design. Some of the commonly used identity management systems that exist today are Sailpoint IdentityIQ, Oracle Identity Manager, RSA lifecycle and governance and so on. SSO tools that exist today are Okta, IdentityNow which have the capability of creating and removing users and also providing single sign on for the enterprise users. Rather than focusing on the tools that exists, it is necessary for the organization to understand the protocols that these tools use and choose the right one that fits their organization. Some of the protocols that are widely use and accepted are OAUTH, OpenID, and SAML etc.

Organizations today have also started a centralized authentication mechanism where the user does not have to remember their entire password and maintain a sticky note or list, attached to their computer [5]. This authentication mechanism when configured properly provides security where users do not have to worry about maintaining sticky note of all their passwords to access different systems [5]. To attain a centralized authentication mechanism different standard can be followed and one such standard is Security Assertion Markup Language (SAML) which uses Extensible Markup Language (XML) based solution for exchanging information between service providers [5]. Another authentication mechanism that can be used is OpenID where an OpenID provider acts as an authentication provider to authenticate relying parties [9]. SSO systems such as SAML, OpenID are the first step in reducing the problem of using different password to log in different systems [4]. Aside from SAML and OpenID another SSO standard that is quite popular is Kerberos authentication. Kerberos provides single sign on through the generation of tickets [10]. These systems are also known as federated authentication standards and are used to authenticate users across different platform [11].SSO protocols like SAML, OAUTH and OpenID replaces traditionalauthentication by using a single source of authentication at the identity provider (IdP) [12]. However, each of these protocols also has their own advantages and disadvantages and based on the literature review there are different ways to attack these single sign on protocols. One of the attacks that is possible which using SAML based single sign on is by constructing a false SAML token [13]. Since SAML uses xml to authenticate the users the attackers can modify the xml to attack the system. One of the major concerns for organization today is how to remediate certain attacks that can occur within the organization. No systems today are free from attacks by attackers despite of the fact whether the organization is using identity management and single sign on solutions. Knowing and having information about different attacks can help organization to plan ahead to prevent those attacks. Some of the vulnerabilities and ways that an attacker can attack an organization involve:

- Injecting malicious endpoints: In this attack the attacker creates a malicious end which is used to force the user to enter their user name and password so that the attacker can retrieve the username and password. Once the credentials are retrieved the attacker uses the known credential to authenticate themselves [12].

- Redirect Attack: In this attack the attacker learns about the user credentials when the identity provider redirects that user by using wrong redirection code [14]. This is possible since neither OAUTH nor OpenID connect specify how the redirection works [14].
- IdP Mix up Attack: In this attack the attacker confuses the resource provider about the identity provider that the user chooses at the beginning of authorization or authentication process to impersonate as the user to access the data [14].
- State Leak Attack: In this attack the attacker forces the browser to be logged under the attacker name at the resource provider [14]. This attack is also called session swapping since it breaks the session integrity property [14].

One of the challenges that many organizations face today is to understand how single sign on works and the best practices to follow while implementing any single sign on protocols. Since most of the organizations are moving their application to cloud and each application are supported by different vendors the traditional authentication mechanism is not suitable. Also, since not every system is threat proof and analysis need to be done when using different authentication and authorization protocols. The literature and journals available do point out the different standards available for single sign on but do not take initiative on predicting how one relates in terms to other. Also understanding how authorization and authentication works with single sign is one of the major concerns that will be reviewed in this paper. The literature review provides information regarding different SSO standards such as SAML, Kerberos, and OpenID but analyzing how authentication and authorization works with the SSO standards is one of the major aspects that needs to be researched more on.

3. The Proposed Approach

In order to understand the challenges faced by different organizations while implementing IAM and SSO solutions it is necessary to interact, understand and analyze the insights of people working in that platform. Proceeding further, reviewing previous researches done in IAM and SSO provides great insights into the data gathering method and analysis. The research will use qualitative method for data gathering. Qualitative method of data gathering involves individual interviews, observations and research. This research will conduct interviews in phone and through online survey with the IAM and SSO resources that are working with different organizations. The research screening is not only limited to a particular organization within a certain region but will cover different regions and organizations inside United States. Aside from interviews we will also review different researches that have been done prior to this research and analyze the results and outcomes of those researches. The interviews to be conducted will be focused more on organizations that have recently implemented IAM solutions and SSO solutions. The interview methods will also look at organizations that are recently planning to implement some form of SSO and IAM solutions since those interviews can provide more insights into the challenges that the organization had to go through in picking the right solution.

Since interviews are the primary source of data for the proposed research, the interviews will help us to build recommendations and guidelines that can be followed while implementing identity management and single sign on solutions. The interview questions are to be more focused on the steps that were taken before finalizing the IAM and SSO solutions and the challenges faced with those solutions. We tend to use these questions to analyze the different circumstances within the organization prior to building the recommendations. The interviews to be conducted will also have questions that are related to the architecture and infrastructure of the organization and the effectiveness of IAM and SSO solutions to provide enterprise security. The response received from interviews is than compared with the different concepts and researches that have been done prior to this research. Different concepts regarding SSO and IAM are also explored by reviewing journal articles, books and prior researches to build a foundation on the existing solutions. The research will also do a comparative study on the prior researches to fill in the gaps that has not yet been covered. The interviews related to the research have questions related to the impact of SSO and IAM in risk management. The risk management section of the questionnaire will be directed towards understanding how SSO and IAM solutions helped in mitigating risk and vulnerabilities within an enterprise environment.

3.1. Methodology Design

Interviews are the primary source of data for this research topic. The interviews questions are designed to help us understand how IAM and SSO solutions are functioning within an organization. The questions presented are within the understanding of people working in different IAM and SSO solutions or people who have some cyber security knowledge. The research questions are designed to understand the different systems of environment an organization has, different SSO protocols used, examine the IAM and SSO concepts within the cyber security space, number of resources that organization has for IAM and SSO and understand the easiness or efficiency provided by using different IAM and SSO solutions. Visual representation of the data collected and gathered is presented in the experiment results section to analyze and understand the feedback from the survey conducted.

In this paper, we classify the data collected into three different architecture models that an organization can have. The models are based on the different applications and users that the organization has. The models are categorized as small, medium and big and analysis is done projecting the different models and evaluating the differences that each model has in compared to another.

The result obtained from data gathering and reviewing different articles is reviewed to understand the impact and various factors that are involved within an organization. It is expected that the research methodology used above will provide us with the information that is needed to understand the organizations limits and their issues in following the best practices that are required. The result obtained from the research is used to build a set of best practices that is needed for any organization while implementing IAM and SSO solutions in cyber security space. This research evaluates how IAM and SSO solutions can help to mitigate risk in an enterprise environment when best practices are followed.

3.2. Data Rubrics Classification

The data rubrics classification is used to classify organization based on the users, applications, size of the team that an organization has. The recommended practices to be followed can vary based on each organization architecture and model.

3.2.1. Architecture Design Model

The organization architecture is based on small, medium and big based on the number of users that the organization has

Small
- Number of users less than 10000
- Number of applications less than 50

Medium
- Number of users less than 25000 and more than 10000
- Number of applications less than 150 and more than 50

Big
- Number of users more than 25000
- Number of applications more than 150

Size of IAM and SSO team (Team Classification)

The team classification is based on the number of employees and contractors that are directly and indirectly involved in IAM. Indirectly involvement may include employee and contractors that are aware of the IAM system and need to coordinate with the IAM team for different enhancements that needs to be done.

Small
- Less than 5 employees and Contractors directly involved in IAM and SSO
- Less than 10 employees involved indirectly involved in IAM and SSO

Medium

- More than 5 and less than 10 employees and contractors involved in IAM and SSO
- Less than 20 and more than 10 employees and contractors indirectly involved in IAM and SSO

Big
- More than 10 employees and contractors involved in IAM and SSO
- More than 20 employees indirectly involved in IAM and SSO

Complexities with IAM and SSO solutions

5 The system is reliable
4 The system has issues but has helped organization to function better
3 The system is fairly designed and has space of improvement
2The system is poorly designed but can be improved
1 The system is not reliable and needs to be replaced

3.3. Population and Sampling

The data is collected based on the survey that is conducted and evaluated based on the data rubrics classification mentioned in the previous section. The data analysis process is as described below

- Understand the current architecture of the organizations surveyed and classify them based on the classification rubrics
- Analyze the problems and issues that can be potentially faced by different organization who have implemented IAM and SSO solutions
- Analyze the security issues reduced with IAM and SSO solutions
- Analyze the recommended practices that can be followed with IAM and SSO solutions through survey and prior researches
- Compare and contrast the feedback from the survey and other past researches that has been done
- Build set of recommended practices based on the survey or prior researches

User Population Sampling

The interview process involves 20 different people who are working in IAM and SSO and the analysis is based on their feedback and literature reviews. The user population consists of different people with different background on IAM and SSO.

4. Experiment Results

The experiment results are based on the survey that was conducted with 20 participants that are working in the IAM and SSO security space. The experiment results presented below has been analyzed and compared with prior researches to reflect IAM and SSO practices that are being followed. It also looks at the complexity involved with IAM and SSO solutions and the role they play in mitigating security risk.

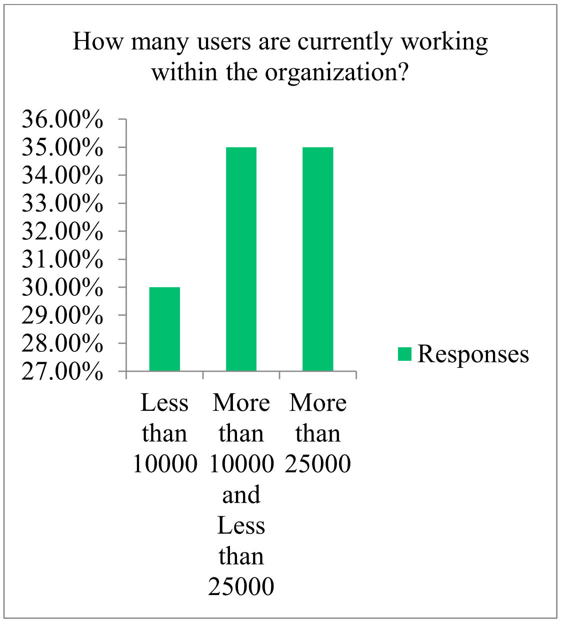

Figure 1: Users currently working within the Organization

4.1. Organization size and Architecture

Based on the survey conducted it can be concluded that most of the organizations that were surveyed had more than 10000 users that was needed to be managed by SSO and IAM solutions. Figure 1 and Figure 2 describes the numbers of users and applications currently managed or needed to be managed by SSO and IAM solutions. 40 percent of the respondents admitted that the number of applications that has been integrated with IAM and SSO systems is more than 150. Based on this result it can be predicted that the survey data fall under the medium or big tier. From the survey conducted it can also be concluded that most of the organizations engaging with IAM and SSO have a bigger infrastructure and architecture to manage.

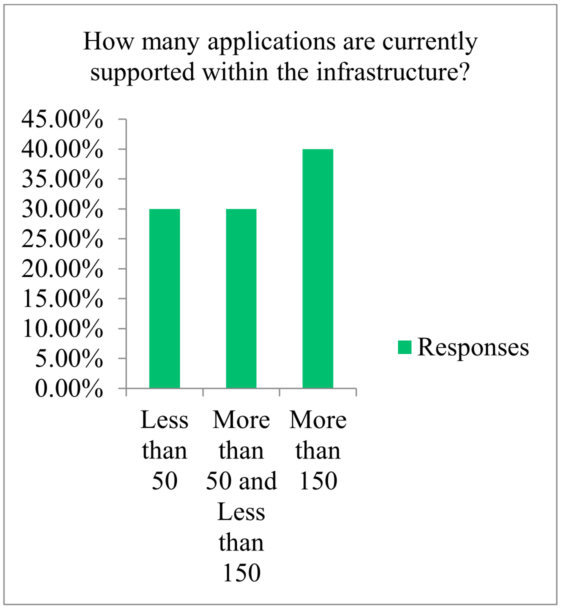

Figure 2: Applications currently supported within the Infrastructure

4.2. Compliance and Auditing Policies

Compliance and Auditing can be described as one of the major reasons that require organization to purchase IAM and SSO solutions. The compliance and auditing policies may differ based on the different domain that the organization is associated with, however the two most popular of those are SOX and HIPAA [15]. Based on the survey gathered majority of the respondents agreed that the organization has some compliance and auditing policies that they need to follow. Figure 3 shows the responses from the participants that were involved in the survey.

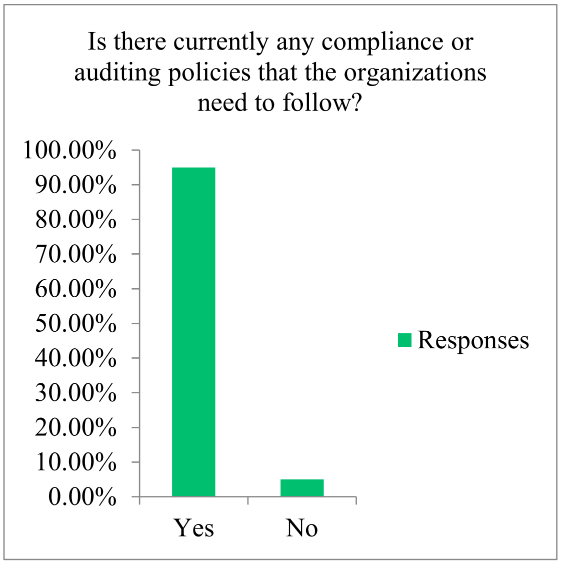

Figure 3: Compliance and Auditing Policies Enforced

4.3. Complexity

Based on Figure 4 most of the respondents responded with already having an IAM and SSO solution in place. Based on this data finding it can be argued that the responses provided to other questions in the survey are more inclined with organizations that have implemented IAM and SSO.

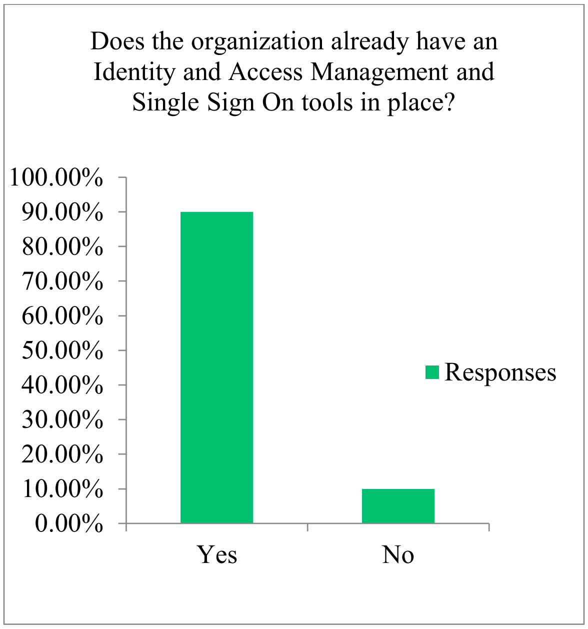

Figure 4: Already having IAM and SSO in place.

The data gathered from the survey also identifies that organizations had reviewed the IAM and SSO solutions before implementing them. The bar graph below shows that most of the respondents responded with the organizations efficiently studying or analyzing the IAM and SSO solutions prior to implementation as shown in Figure 5.

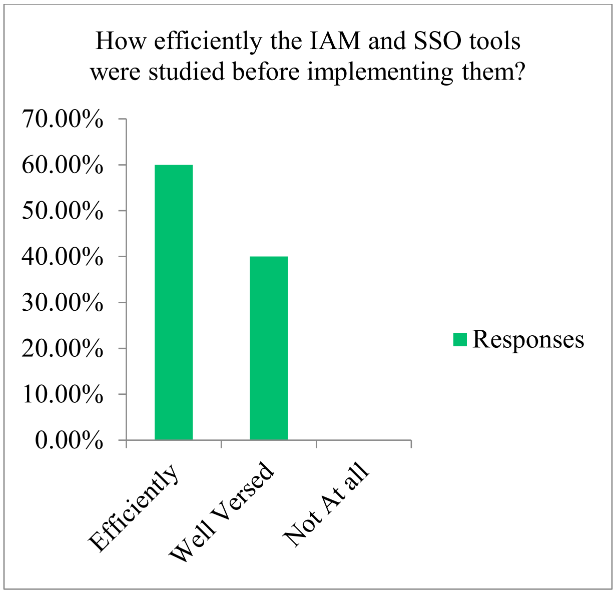

Figure 5: Review of IAM and SSO solutions

Some of the other restriction that was related with the IAM and SSO solutions is shown in the Figure 6.

The Figure 6 defines some of the restriction that is there when using the IAM and SSO tools. Some of the restrictions that are there with the tool are mentioned below from top to bottom according to the data collected are as below:

1. More customization needed with the tool
2. Provisioning capabilities are limited
3. Compliance and Auditing capabilities not as needed by the organization

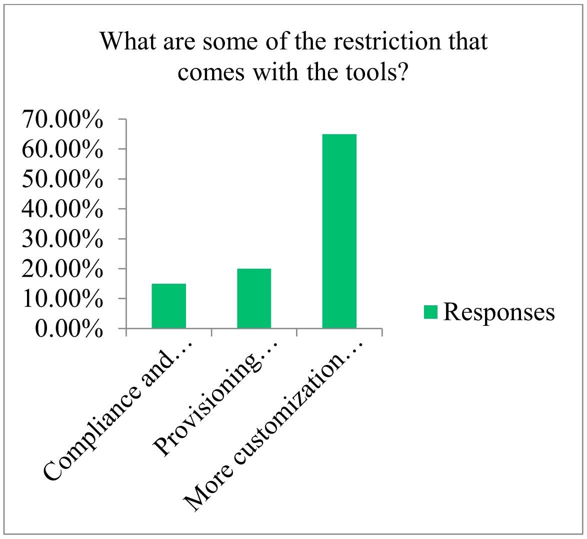

Figure 6: Restrictions with the Tools

4.4. Benefits provided By SSO and IAM solutions

According to the survey conducted and by reviewing the prior researches that have been done in IAM and SSO, we define the different benefits that are provided by Single Sign On and Identity and access management solutions.

4.4.1. Security

One of the major benefits that a SSO and IAM solution are able to provide is the extra layer of security that it adds to the existing infrastructure. IAM solutions ensures that each user in the organization has the right access to do their work so it decreases the risk of employees having more access than that is needed for them. SSO ensures that user do not have to remember their authentication credentials for every application that they need to login in. Removing the necessity of having to remember multiple credentials also reduces the risk of being easily targeted by losing their credentials to the intruders. SSO protocols make it tougher for attackers to easily extract credentials that are caused by server-side vulnerabilities and trying to trick the system to access a particular application which are managed by SSO solutions [16].

4.4.2. Privacy

An SSO solution also helps to maintain privacy within an organization, since employees do not have to re-enter their credentials for every application. Also SSO authentications techniques such as SAML and OAuth depends upon Identity Provider (Idp) and Service Provider (SP) for authentication mechanism the Idp does not have knowledge about the SP that the user is authenticating to which is also known as private browsing [16].

4.4.3. Automation

IAM and SSO solutions are able to provision users to other application without manual intervention or little manual intervention. This functionality helps organization to automate different provisioning, compliance and auditing activities that are needed which helps organizations to grant and remove employees' access faster and with reliability. An organization not using IAM and SSO solutions will need to rely on manual resources for provisioning, compliance and auditing activities which takes more time and effort.

4.4.4. Regulatory Compliance

Organizations within the United States are required to perform compliance activities based on the domain that they operate within [15]. The Sarbanes-Oxley (SOX) and Health Insurance Portability and Accountability (HIPAA) act are among the most popular act that organizations need to abide by. According to Sarbanes-Oxley act of 2002, the SOX act protects the interest of the investors and general public by diminishing fraudulent practices with the enterprise and improving the accuracy of the disclosures. The SOX act applies to all the organizations in US and the organizations are required to comply with the SOX [15]. The HIPAA act which provides data privacy and security within the health and medical domain. One of the major reasons of using IAM solutions at least in USA is also because of the Sarbox or SOX and HIPAA since organizations need to comply with that act [15].

4.4.5. B2B Collaboration

Most of the organizations today do not work alone but rather collaborate with other organizations as partners. This brings in the need for IT systems in one organization to collaborate with other organizations IT systems [17]. Collaboration with other organization needs resources of one organization to be able to access the systems available in other organizations. For this particular reason an employee within a particular intranet of one organization needs to access applications that are in a different intranet. An SSO and IAM tool makes this possible by centralizing their authentication and authorization mechanism and allowing their users login once and be able to access shared resources across multiple organizations [17].

4.4.6. Simple Administration

Having a centralized system makes it possible for enterprises to have a single source where different access that the user has can be defined [17]. The IAM and SSO solutions provide interactive UI which makes it possible to be a one stop shop to view all the users and their accesses. The ease of being able to navigate through different users and revoke/remove certain access that the user should not be having provides organization with greater flexibility of managing their users.

4.5. Challenges Faced by IAM and SSO solutions

The challenges faced by IAM and SSO solutions mentioned below are derived based on the survey that was conducted and prior researches that describe the issues related to SSO and IAM.

Some of the common challenges are as follows:

- Lack of research done on the tool to study whether it meets the requirements for the IAM and SSO solutions
- Complexity of the architecture and applications that needed to be integrated with the IAM and SSO solutions
- Lack of proper documentation of the product and the tool
- Having incident management and change control in place.
- Understanding the vulnerabilities of the tools and how it can impact the infrastructure
- Sufficient and Knowledgeable resources needed to support the tool.

4.6. Best Practices to Follow

After analyzing the survey some of the best practices that can be followed during IAM and SSO implementation are as follows

- The organization should review the tool that they are implementing and understand the complexities associated with the tool
- The organization should have sufficient and trained resources to manage their tool
- The organization should maintain proper documentation for any changes or customization that is done to their IAM and SSO tool
- The organization should have incident management and change control activities in place for any changes that are done to the IAM and SSO tool
- The organization should understand the vulnerabilities that are with the tool and have teams and resources to mitigate the vulnerabilities with the tool
- There should be 24/7 support for monitoring and managing the tool like having an incident response team available

4.7. IAM Data Flow and Architecture

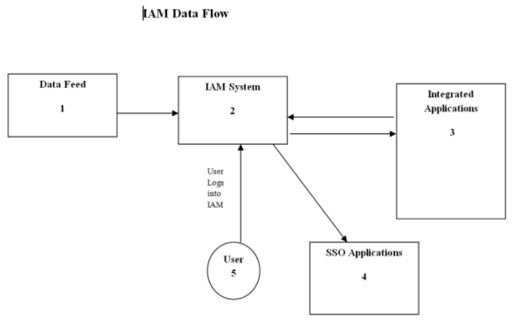

Figure 7: IAM Data Flow

Figure 7 represents the data flow of an IAM system. The bi-directional arrow between 2 and 3 represents the data flow from both the system where one system is the IAM and the other is the applications integrated with the IAM system. The IAM system reads in the user accounts, accesses that each user has in the integrated system but also has the capability to provision new accounts and access associated with users to the integrated system. The data-feed acts as a source of truth for the IAM system from where the IAM system reads in its primary data. The user in the figure represents the user who can log into the IAM system and make specific request for different accesses they need using the IAM system access request framework. If the IAM system supports SSO capabilities the logged in users into the IAM system can access applications without being prompted for username and password. The applications supporting SSO should be integrated into the IAM system to allow SSO functionality to the users. The SSO mechanism is handled by one or more of the SSO protocols that the IAM system is capable of working with such as SAML, OpenID etc.

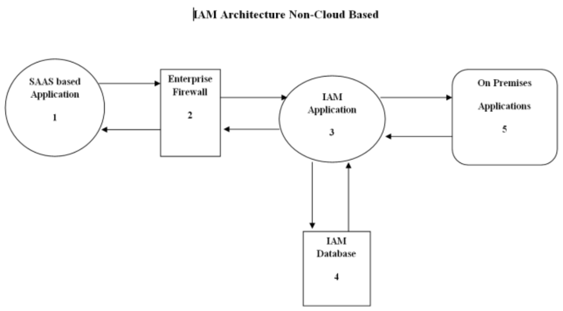

Figure 8: IAM Architecture Non-Cloud Based

Figure 8 represents the non-cloud based architecture of an IAM system. IAM architecture can be categorized as either cloud based or non cloud based. In the non-cloud based architecture the organization is responsible for maintaining the infrastructure needed to maintain the IAM system. The non-cloud based model can be integrated with both the on-premises applications along with cloud based SAAS applications. The architecture consists of an IAM database which is responsible for storing the data that the IAM system reads from integrated applications along with any specific capabilities or data modeling that the IAM system needs to function. On-premises applications are applications that are inside the enterprise network perimeter and the arrows between 3 and 4 represents that the IAM system can read and write data to on-premises application. Since SAAS based applications are not within an enterprise network an enterprise firewall might be present between the SAAS based applications and the IAM system. The firewall should be able to allow request to flow “to and from” SAAS applications to IAM system.

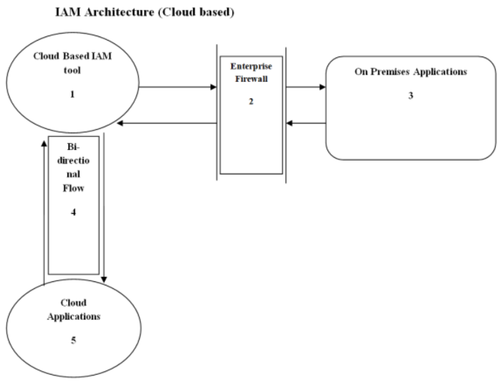

Figure 9: IAM Architecture Cloud Based

Figure 9 represent the cloud based architecture model of an IAM system. In this architecture the IAM system itself is a SAAS application that provides IAM services to the organization. The SAAS based IAM system also provides the functionality to read and write to both on-premises and other cloud based applications.

The arrow between 1,5 and 1,3 represent the flow between IAM system and the integrated applications.

5. Conclusion

In this paper, we analyzed how different IAM and SSO practices are being followed within several organizations. The survey looked at different architectures that the organizations has along with different practices that the organizations followed. In this paper we also analyzed different challenges that the organizations have while implementing IAM and SSO solutions along with the different benefits that an IAM and SSO solution provide. The research also reviewed other research that was done in IAM and SSO to analyze the best practices and comparing it with the survey conducted to understand IAM and SSO practice in organization based on their infrastructure and architecture.

However, we limited our scope to only twenty participants and prior researches to understand the importance of IAM and SSO in the cyber security space. The survey conducted was also limited due to the time and scope of the paper. The participants were only interviewed based on the survey questions and no other possible feedback or inquiry was done aside from the survey questions. Although the research and survey was limited, the responses from the participants helped to analyze the different aspects of IAM and SSO solutions.

Since, our research was only limited to 20 participants, the research scope can be expanded by increasing the number of questions on the survey and the number of participants for the survey. The survey conducted was more focused on understating the importance and benefits of IAM and SSO in the cyber security space, but it did not go in depth to really understand and analyze the IAM practice in different organizations. Since the method of conducting survey was online there was also a limitation on the questions that could be asked and responses that was received. Future work can also look into IAM and SSO practice more in depth from different risk management aspect and cyber security vulnerabilities that can exists. In this research we did not analyze into different cyber security vulnerabilities that can exists with an organization and how IAM and SSO solution can help in reduce each of those vulnerabilities that exists. Future, work can also take into consideration in focusing depth analysis on different SSO protocols that can be used within an organization considering their infrastructure and architecture.

References

[1] Manguic, D. M. (2012). CLOUD IDENTITY AND ACCESS MANAGEMENT–A MODEL PROPOSAL. Accounting and Management Information Systems , 11 (3), pp. 484-500.

[2] Peterson, B. H., Smedegaard, P., Heninger, W. G., & Romney, M. ß. (2008). Managing Multiple Identities. *Journal Of Accountancy* , 1-6.

[3] Nunez, D., & Agudo, I. (2014, 3 6). BlindIdM: A privacy-preserving approach for identity. International Journal Of Information Security

[4] Catuogno, L., & Galdi, C. (2014). Achieving interoperability between federated identity management systems:A case of study. Journal of High Speed Networks 20 , 209-221.

[5] Lewis, D. L., & Lewis, J. E. (2009). Web Single Sign-On Authentication using SAML. IJCSI International Journal of Computer Science Issues , 2.

[6] Andre, T. (2017). Cybersecurity: An Enterprise Risk Issue. Hfm Healthcare Financial Management , pp. 1-6.

[7] Tormo, G. D., Millán, G. L., & Pérez, G. M. (2012, 12 27). Definition of an advanced identity management infrastructure. pp. 173-200.

[8] Alston, A. (n.d.). Attribute-based Encryption for Attribute-based Authentication, Authorization, Storage, and Transmission in Distributed Storage Systems. pp. 1-20.

[9] Hsu, F., Chen, H., & Machiraju, S. (2011). WebCallerID: Leveraging cellular networks for Web authentication. Journal of Computer Security , 862-899.

[10] Pérez-Méndez, A., Pereñíguez-García, F., Marín-López, R., & López-Millán, G. (2012). A cross-layer SSO solution for federating access to kerberized services in the eduroam/DAMe network. International Journal of Information Security , 365-388.

[11] Shitamichi, T., & Sasaki, R. (2014). TECHNOLOGY OF FEDERATED IDENTITY AND SECURE LOGGINGS IN CLOUD COMPUTING. International Journal of Electronic Commerce Studies , 5, 39-62.

[12] Mainka, Christian; Mladenov, Vladislav; Schwenk, Jörg. (n.d.). On the security of modern Single Sign-On Protocols –Second-Order Vulnerabilities in OpenID Connect.

[13] Krawczyk, P. Secure SAML validation to prevent XML signature wrapping attacks.

[14] Fett, D., Küsters, R., & Schmitz, G. (2016). A Comprehensive Formal Security Analysis of OAuth 2.0.

[15] Heino, E. (2011). Evaluating financial benefits of an identity management solution CASE Logica. Retrieved July 9, 2018, from http://epub.lib.aalto.fi/en/ethesis/pdf/12500/hse_ethesis_12500.pdf

[16] Alaca, F., & Oorschot., P. C. (2018). Comparative Analysis and Framework Evaluating Web Single Sign-On Systems.

[17] Bazaz, T., & Khalique, A. (2016). A Review on Single Sign on Enabling Technologies and Protocols. International Journal of Computer Applications, 15 (11), 18-25.