Cloud Security Standards

Vidushi Gupta, *Carleton University*

The security provided by cloud computing should be better or equal to security level of non-cloud IT environment. Hence, it is crucial that cloud customers subscribe to cloud service providers that support cloud security standards. The advantages of adhering to standards are several:

- Hybrid cloud computing can be realized as it becomes easier to merge local security technologies with those of cloud service providers
- Standards encourage interoperability as it is easier to switch between cloud service providers following standard practices
- Cloud security policies with standard practices are easily described and understood
- Regulatory compliance is uncomplicated

(Baudoin, et al., 2017) describe ten steps for cloud service customers to evaluate and manage security and privacy of cloud service providers. Some of these steps are described in detail below:

A. Manage people, roles and identities

It is important to manage access to customer data and application in the cloud computing environment. People are grouped into three different roles – employees of cloud provider, service administrators and customers or of cloud service and the rest (Cloud Standards Customer Council, 2016).

For employees of cloud service provider, it is necessary to have proper access controls so only suitable people have access to customer services and related software and data. Information security management standards such as ISO/IEC 27002 (ISO, 2013) and ISO/IEC 27017 (ISO, 2015) describe necessary controls for provider employees. It is important that cloud customers subscribe to cloud service from providers with certification in these standards. Likewise, service administrators and customers or of cloud service should be authenticated prior to using the cloud service. Since administrators have more responsibility and consequently further access to potentially sensitive data, they must be authenticated strictly (Naik & Jenkins, 2016). To manage authority and

authentication of these identities based on their attributes, Identity and Access Management (IAM) Systems are used. Here are some IAM standards and protocols in use today:

1. *Federated IDs*

Federated IDs connect electronic identities of users between different identity management systems in an organisation. A user stores their credentials on assigned federated ID. Each user with a single federated ID prevents managing multiple credentials to access services (Wikipedia, n.d.).

2. *Privileged Identity Management*

In instances when privileged access is required to be given to system administrators, a privileged identity management system is used. Such a system allows time-bound and approval-based access to administrators. By allowing authenticated access to few people for a specific period, accountability increases, and threat of hacking is reduced. A common application of this concept in seen in Microsoft's Azure Active Directory (Azure AD) Privileged Identity Management (PIM) (Microsoft Corporation, 2019).

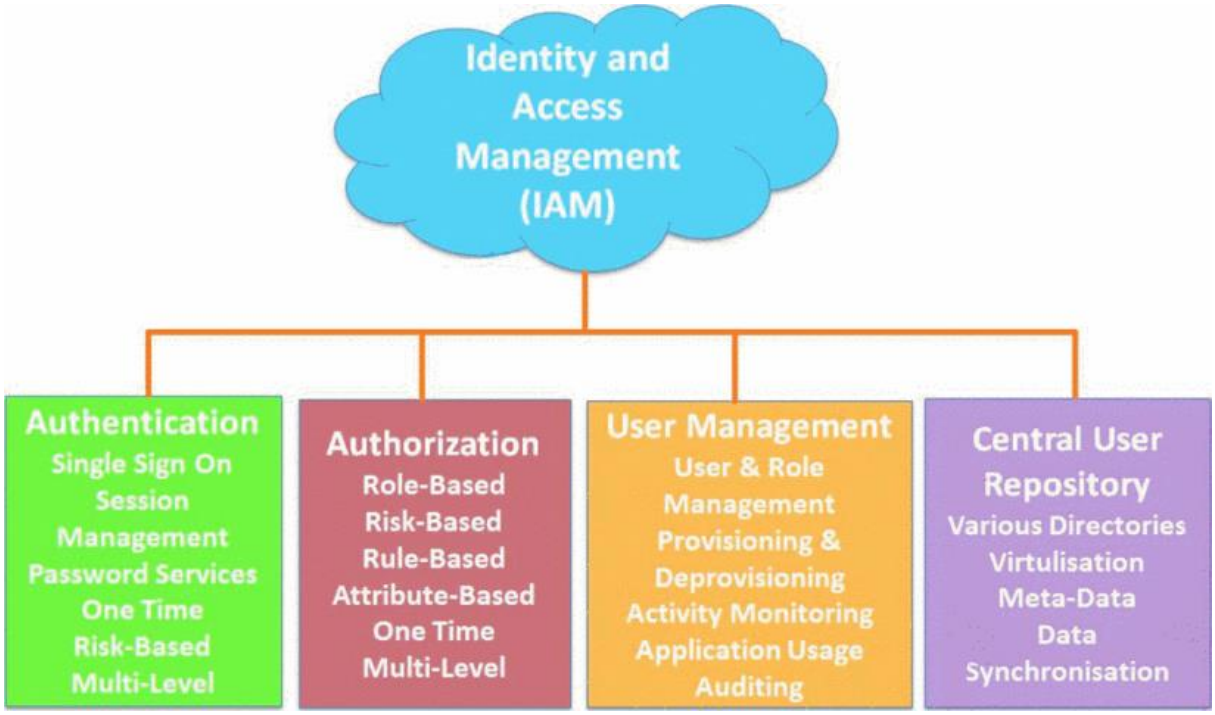

Fig 1. Identity and access management components (Naik & Jenkins, 2016)

3. *Single sign-on*

To assign different credentials for different services lowers security as users might use similar passwords (Revar & Bhavsar, 2011). Therefore, single sign on allows logging into multiple services

using the same credentials. This way there is reduction in number of passwords and IDs to manage and hence more security. One harmful affect of this service is that once a malicious user has right credentials, they might gain access to many services all at once. Thus, there needs to be increased security to protect leakage of credentials. Multiple levels to authenticate the identity of a user is also important. Below are some protocols and associated standards that strengthen single sign-on capability.

4. *LDAP Lightweight Directory Access Protocol (LDAP)*

LDAP allows access to directory servers which store authentication passwords and other sensitive information. Directory servers allow detailed access control mechanisms which decide user's access to information based on entries and attributes. An LDAP entry contains information about an entity. Each entry has a distinguish name (DN), related attributes and object classes (Basic LDAP concepts, n.d.). A TLS is established between client and servers in a LDAP session. This is to increase authentication as a client certificate may be demanded by LDAP server, server identity is verified using NDS names, IP addresses as attributes to be authenticated. This authentication method is set between client and server using bind authorization method where state of authorization is set. The authentication method can be simple BIND or SASL (simple authentication and security layer) authentication bind. In LDAP, there are policies in place that don't allow users to choose weak passwords and have strong encoding mechanisms (Internet Engineering Task Force (IETF), 2006). It is also possible for two-factor authentication with one-time passwords. Some may be standardised. IETF does this but asks for comments which they may used to change it.

5. *Active Directory Federated Services (ADFS2)*

This is a single sign on service made by Microsoft. Microsoft creates a dedicated domain in the cloud for office 365 subscription. When a user logs in, Microsoft will check their identity information with its active directory accounts. This way, users can access any Microsoft applications and systems with different organisations (Microsoft, 2019).

In comparison, while active directory is database of directory services where organisational credentials are stored, authentication is done, LDAP is a protocol used to communicate with an active Directory.

6. *Security Assertion Markup Language (SAML)* (OASIS Open 2005, 2005)

"SAML is an XML-based framework that allows identity and security information to be shared across security domains**."** (Campbell, Mortimore, & Jones) SAML provides security by using a public

key infrastructure to protect identities of users logging in. It is used for providing privacy and authenticity. It has single sign on capability through which one set of credentials can be used to access many platforms (Khodabacchus, Soyjaudah, & Ramsawock, 2017). Use of SAML fulfills three different functions:

- Allows end user to use their credentials to login
- Identity provider verifies identity of end user
- After identity is verified, the service provider authorises end user to login

An implicit trust is established between identity provider (IP) and service provider (SP). If this data is breached, security is lost. There is a need to provide security improvement on this language, so this data is not breached.

6. *OAuth 2.0*

OAuth 2.0 is also used in single sign-on service. It is an open standard that, according to (Hossain, Hossain, Hossain, & Sohag, 2018) allows third party applications a way to access users' resources (such as their photos and videos) without sharing their login credentials and in a away that helps improve user's experience of the application. More generally, The OAuth 2.0 authorization framework allows a third-party application to obtain restricted access to an HTTP service after being granted access by the resource owner. Here the client application obtains authorization from resource owner (entity capable of granting access to protected resource). After receiving authorisation, client communicated with an authorization server to be authenticated and obtain access token (Hardt & Microsoft, 2012). (Fett, Kuesters, & Schmitz, 2016) show that OAuth 2.0 is implemented without proper cryptographic security, like encryption keys, hash functions and digital signature.

7. *OpenID Connect* (Sakimura, Bradley, Jones, & Jay, 2014)

OpenID Connect works in conjunction with OAuth 2.0 protocol. It allows a client to obtain basic profile information about resource owner or end-user after a client application has been authenticated by an authorization server. After becoming a standard in 2014, OpenID connect is the latest single sign on (SSO) protocol. It is used in large companies like Amazon, Google, Microsoft and PayPal. The OpenID connect specification presents libraries that support OpenID's integration into a web application including specifying libraries that manage security for this protocol (Mainka, Mladenov, Schwenk, & Wich, 2017). This protocol can withstand ID spoofing, wrong recipient, Replay, signature

bypass and other such single phase attacks as is shown in (Mainka, Mladenov, Schwenk, & Wich, 2017). Single phase attacks are where one message is changed in one phase of SSO protocol. As mentioned, phases in SSO involve SP registration, end-user authentication on IP and end-user authentication on SP. On the other hand, it is unclear if this protocol addresses cross phase attacks. The issuer confusion attack is resolved by providing verification steps. However, these steps are scattered over the whole specification and not written in one specific place.

Comparison between Oauth2.0, SAML, OpenID connect

Oauth2.0 is used for authorisation while SAML and OpenID Connect are used for authentication.

A use case for Oauth2.0 is when in an application downloads contacts from Facebook or our phone. Here, an application is securely accessing to another application(Facebook) on behalf of a user. After user approval, the identity provider (IP) authorises access to a third-party application to download its resources.

A user case for *OpenID connect* is using a google account to login to YouTube or google photos or Gmail. This example of single sign on is relevant as users sign into IP and access other websites without sharing their sign in information with each of them.

SAML is more likely used in an organisation environment. Using work email one can sign into different services. This is because work credentials are shared securely between IPS and are authenticated to provide access.

8. *System for Cross Domain Identity Management (SCIM)*

System for Cross Domain Identity Management (SCIM) specification is designed to make it easier to manage user identities in the cloud. This involves automatically adding/removing user identity information between identity domains. Additionally, SCIM can be used for sharing information about user attributes, group membership which affects a user's permissions. Therefore, this has become useful in provisioning user account between applications, related servers, and file shares. SCIM layers is built on top of HTTP layer and therefore follows security policies of HTTP. SCIM resources record sensitive information. Hence, communication between SCIM clients and servers must be done over transport-layer security mechanism (Hunt, et al., 2015).

B. *Ensure Data Is Protected*

Increasingly, information security has become important for organisations across all architectures of communication and access to internet. The cloud has an added layer of vulnerability as data is distributed among different resources in multi-tenant environments. This creates shared responsibility

among cloud providers and users. Data security is required during storing data, data transfer, or data stored for use by applications (Cloud Standards Customer Council, 2016).

When evaluating security for cloud service providers, cloud customers should investigate types of risks such as:

- risk of theft or unauthorised disclosure of data,
- unauthorised modification of data,
- risk of loss or unavailability of data.
- risk of unauthorised use of data assets, such as application code or images (Chen, Xiang, Yang , & Chow, 2016).

1. *TLS (Transport Layer Security) Protocol Version 1.3* (Rescorla & Mozilla, 2018)

This protocol is responsible for security over communication networks on the internet. It was first designed by Netscape communication is 1992 with the aim of providing security on world wide web (Oppliger, 2016). It expects a reliable and in-order data stream from underlying transport channels. TLS consists of:

- Handshake protocol that allows authentication of server and client identities and decide cryptographic keys and encryption algorithm to be used before data is communicated through channel. Identity is authenticated using public key. Cryptographic key and encryption are secure from eavesdroppers. Additionally, reliability is ensured as attackers cannot modify connection without notifying parties.
- A record protocol that employs structures established by handshake protocol to secure traffic between communicating bodies. Traffic is divided into individual records, each of which are protected individually using traffic keys.

A connection with two peers is called a TLS session. During a TLS session, cryptography parameters containing information about session is shared between these two peers. Some of these parameters are session identifier, a peer certificate, an algorithm to compress data for encryption, a cipher spec consisting of Message Authentication Code (MAC), a pseudo random function (PRF), a Master key. (Ferst, Figueiredo, Denardin, & Lopes, 2018) . TLS is application protocol independent and can be layered on any transport protocol. However, TLS standard does not specify how transport protocols can communicate with TLS for handshaking and verifying authentication certificate.

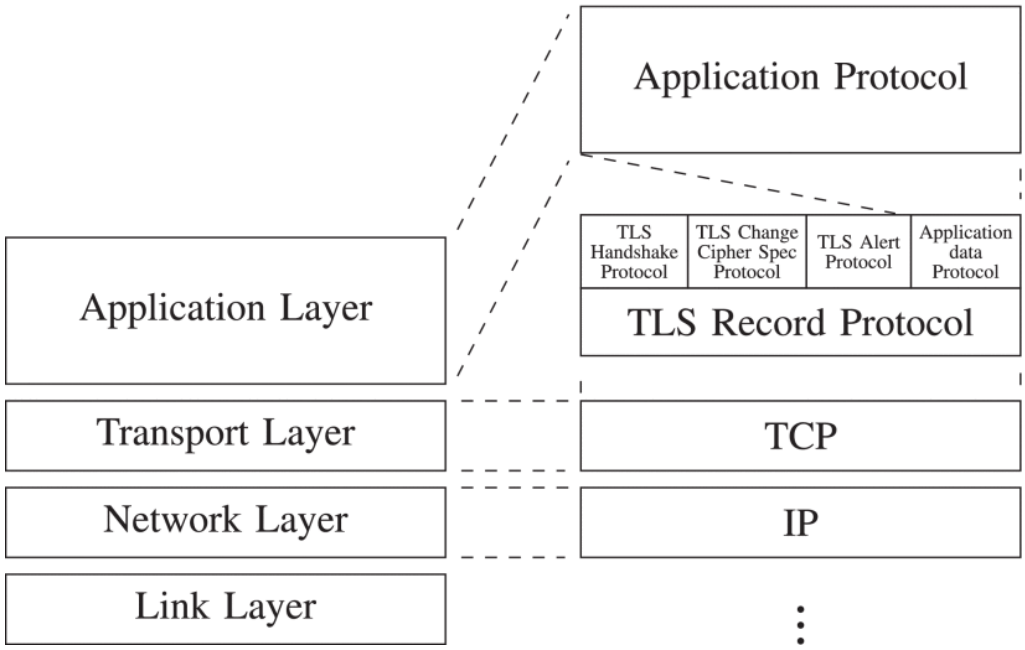

Fig 3. TLS protocol layered in between transport and application layer

2. *Hypertext Transfer Protocol Secure (HTTPS)*

HTTPS is HTTP but over TLS (transport layer security). HTTPS provides authentication, data confidentiality and integrity to visit sites on the internet. (Rescorla, 2000). Usage of this protocol is useful when cloud service customer is trying to connect to cloud service provider. HTTPS prevents man-in-the-middle attacks by validating the server's identity with server's certificate message. However, there is no method to check identity of client by the server unless client has its own security certificate (Rescorla, 2000)

3. *Secure File Transfer Protocol (SFTP)*

SFTP is a file transfer protocol run over secure socket shell (SSH). It works easily over single, reliable, secure duplex byte stream connection (SSH). Unlike using a remote command to specify file name to be transferred, SSH uses ssh-2 subsystem request to initiate SFTP server on remote host. This shields the client from information about how SFTP is implemented on the server instead of adding SFTP-server pathname in the command (which might change). The command line does not mention information about files to be transferred inside SFTP protocol. (Barrett, Byrnes, & Silverman, 2005). Fig. 2 shows how sftp is implemented on client and server side.

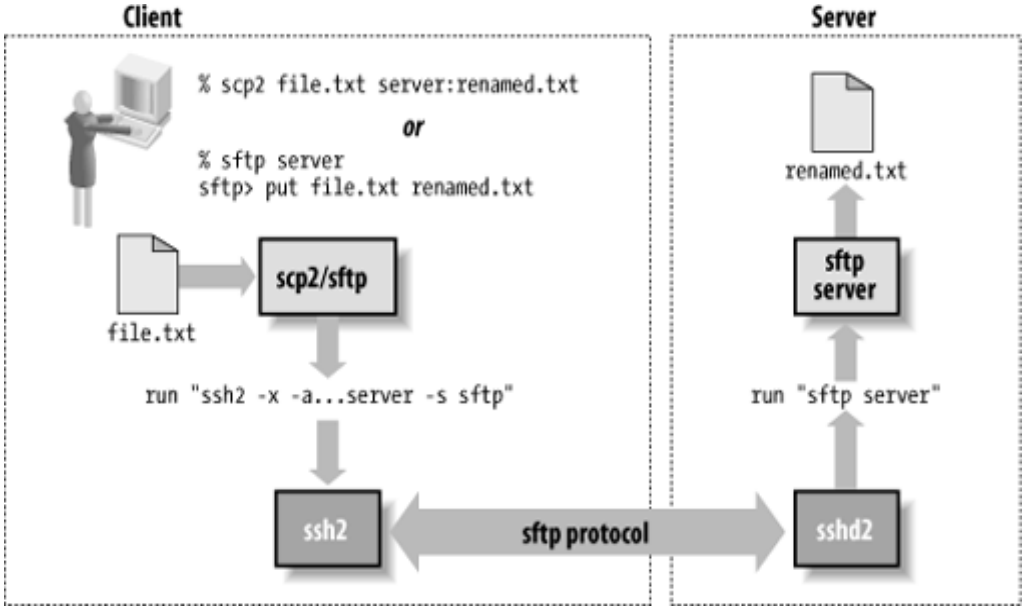

Fig. 2: Illustration of how SFTP operates (Barrett, Byrnes, & Silverman, 2005)

4. VPN using IPsec or SSL

VPN technology allows using cryptography in open and public network to form a virtual private network (VPN)., SSL VPN operates in secure sockets layer while IPsec VPN functions at the network layer. As explained in (Fei, Kehe, Wei, & Qianyuan, 2013),with a VPN connection, an encryption technology is used to design a dedicated and secure network in the normally open and vulnerable network of the internet. This way, resources do not need to be spent in constructing a private network physical line. This involves making a “security tunnel” to connect users, encryption technology to encrypt and decrypt data, key management technology that keep keys that help in encryption and decryption of data and authentication technology for verifying identification and/or digital signature.

SSL is responsible for offering secure channels between two communicating machines on a network. SSL uses x.509 digital signature technology and public key system to fulfill those requirements. During connection, server and client use MAC password and MAC key to authenticate identity of client and server and a Master password to protect data flow. Established VPNs connect using SSL in VPN SSL (Fei, Kehe, Wei, & Qianyuan, 2013).

In VPN IPsec, security features such as data encryption, data certification and data verification are provided on network layer. However, IPsec is unable to achieve the access control without which a network is vulnerable. This is unlike SSL where access is controlled based on a user identity.

C. *Ensure Effective Governance, Risk and Compliance Processes Exist*

Governance are guidelines that members use to make decisions about providing IT services to fulfill needs of their organisation. It is important to have governance to guide management processes and decisions that affect IT services according to business goals of the organisation. Standards to provide guidelines for governance of IT services have been developed for years and are followed around the world. These governance practices or standards are not specifically about cloud computing, but general so they can be applied to process of cloud computing. The International Organization for Standardization (ISO) had a standard in place called ISO/IEC TR 20000-9:2015 published in 2015. (International Organization for Standardization, 2015) This standard provided guidelines to manage cloud services. However, this guideline has been withdrawn after review. Some standards worth mentioning are COBIT 2019 (ISACA, 2019) by ISACA (ISACA, 2010), The Payment Card Industry Data Security Standard (PCI-DSS) (PCI Security Standards Council, 2006), SSAE (Statement on Standards for Attestation Engagement) 16 (SSAE 16, 2011). Some key standards have been described below.

1. *ISO/IEC 38500 – IT Governance* (ISO, 2015)

ISO is an independent non-governmental international organisation that gathers experts from different countries of the world to establish standards or world-class specifications in technology, food safety, agriculture and healthcare. They were founded in 1947 and have published 22942 standards since (International Organization for Standardization, 1947). They have members from national standards bodies of 164 countries. They work closely with International Electrotechnical Commission (IEC) and International Telecommunication Union (ITU) (International Organization for Standardization, n.d.).

ISO/IEC 38500:2015, published in 2015, replaced ISO/IEC 38500:2008 after a standard review cycle of 5 years. By providing guiding principles, this standard allows governing groups of organisations (partners, directors, executive managers) to make effective, efficient and acceptable use of information technology within their organisation. It also helps those that who are counselling or informing these executive decision-making bodies (legal or accounting specialists, technical specialists, auditors etc.) It aids in governance of current and future use of IT on an organisation. It is useful for both public and private organisations, government, not-for-profit organisations. Additionally, adopting this standard helps in providing a vocabulary for IT management. (ISO, 2015)

ITIL (Information Technology Infrastructure Library) (IBM Cloud Education, 2019)

The name was coined in 1980s by the British government's Central Computer and Telecommunications Agency (CCTA) when it printed best practices in IT service management.

One of the most important part of ITIL is the configuration management database (CMDB). It provides authoritative principles for all components in an IT service, such as software, IT components, documents, users, and hardware. CMDB keeps track of changes in these resources and their location so its easier to trace and manage them. ITIL framework is updated by AXELOS (Axelos, 2019). Newer versions of ITIL add new processes to service management. Version 3 introduced Business Relationship Management (BRM) process (Terra, 2019), and became easier to read with fewer inconsistencies compared to previous version. The latest version of ITIL is version 4 emphasises digital transformation, artificial intelligence, cloud computing, and DevOps. The ITIL framework lays out five key stages of providing an IT service. It lists best practices in those areas. These areas are:

Service strategy: provides guidance on how to design, develop and implement IT service management. This can involve awareness of service costs and budgeting, strategies on managing feedback and improvement of IT services.

- Service design: describes how to design services and processes. This can involve optimizing service capacities, managing suppliers among others.
- Service transition: provides guidance on how to manage implementing new service or altered service while making sure that service management process operates smoothly.
- Service operation: states best practices to ensure that services run properly, and new features are delivered effectively.
- Continual service improvement helps ensure that IT services keep updating in a manner that help continually changing business goals

2. *ISO/IEC 20000*

Another service management guide that may be used in conjunction with ITIL is ISO 20000. From ISO/IEC 20000 :1 to ISO/IEC 20000 :13 provide guidance on applying a service management system to the organisation and integrating it with other service standards such as ITIL and COBIT (ISO, 2020). ISO/IEC 20000 contains essential requirements organisation must meet to display compliance and competency. ITIL supports implementation of ISO/IEC 20000 by providing more detailed information on processes. ISO/IEC 20000 Part 11 specifically describes how to integrate both standards in an organisation (ISO, 2020).

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) (Federal Government of United States of America, 2019)

In February 2013, an order was issued by President of United states with directive to develop a framework to reduce cyber risk to critical infrastructure. Based on current standards and existing guidelines, this developed in collaboration with industry and government. The framework consists of three main components: the core, implementation tiers and profiles.

- The core mentions cybersecurity objectives for an organisation based on cybersecurity risk management which are divided into further subcategories such as asset management, data security, response planning, recovery planning etc. There are a total of 23 such categories split across five functions of identification, protection, detection, response and finally recovery (Government of United Stated of America, 2019).
- Implementation tier illustrates the level of integration of an organisation with principles of cybersecurity framework of NIST. Adoption of these practices into risk management is dependent on choice of the organisation based on their business goals (Federal Government of United States of America, 2019)
- Profile is a way for an organisation to track their cyber security strategies that are in place currently and assign target cybersecurity strategies. This allows an organisation to prioritise areas that are important and analyse gaps (Federal Government of United States of America, 2019).

3. *Canadian Centre for Cyber Security's Cryptographic Module Validation Program (CMVP)* (Canadian Centre for Cyber Security, 2019)

For procuring IT products, the CMVP certifies cryptographic modules against Federal Information Processing Standard (FIPS) 140-2 standard (NIST: Computer security resource center, 2019) and ISO/IEC 19790 Information technology. CMVP is joint effort between Canadian Centre for Cyber Security and NIST. Vendors can get their products certified in an accredited CMVP lab.

Conclusion

In this paper, we have looked at three important aspects of cloud security, namely, access management, protection of data through secure connections and regulatory standards to ensure compliance. We explained common standards and protocols under each of these aspects and explained the relationship between them. We have also highlighted some drawbacks in these standards and procedures that show potential for improvement. Our future work involves evaluating cloud security standards and comparing them.

References

Axelos. (2019). *What is ITIL*. Retrieved from Axelos official website: https://www.axelos.com/best-practice-solutions/itil/what-is-itil

Barrett, D. J., Byrnes, R. G., & Silverman, R. E. (2005). *SSH, The Secure Shell. The Defininite Guide.* O'Reilly Media, Inc.

Basic LDAP concepts. (n.d.). Retrieved from https://ldap.com/basic-ldap-concepts/

Baudoin, C., Chen, E., Dotson, C., Edwards, M., Gershater, J., Harris, D., . . . Koumpam, E. (2017). *Security for Cloud Computing Ten Steps to Ensure Success Version 3.0.* Cloud Standards Customer Council.

Campbell, P., Mortimore, C., & Jones, M. (n.d.). Retrieved from https://tools.ietf.org/html/rfc7522

Canadian Centre for Cyber Security. (2019, April 3). *Cryptographic Module Validation Program (CMVP)*. Retrieved from https://cyber.gc.ca/en/cryptographic-module-validation-program-cmvp

Chen, F., Xiang, T., Yang , Y., & Chow, S. S. (2016). Secure Cloud Storage Meets with Secure Network Coding. *IEEE Transactions on Computers*, 1936-1948.

Cloud Standards Customer Council. (2016). *Coud: Cloud Standards Customer Council.* Retrieved from https://www.omg.org/cloud/deliverables/CSCC-Cloud-Security-Standards-What-to-Expect-and-What-to-Negotiate.pdf

Federal Government of United States of America. (2019, November 18 2019). *NIST Background on Framework*. Retrieved from https://www.nist.gov/cyberframework/new-framework#background

Fei, C., Kehe, W., Wei, C., & Qianyuan, Z. (2013). The Research and Implementation of the VPN Gateway Based on SSL . *2013 International Conference on Computational and Information Sciences.* Shiyang, China: IEEE.

Ferst, M. K., Figueiredo, H., Denardin, G., & Lopes, J. (2018). Implementation of Secure Communication With Modbus and Transport Layer Security protocols. *2018 13th IEEE International Conference on Industry Applications (INDUSCON).* São Paulo, Brazil, Brazil: IEEE.

Fett, D., Kuesters, R., & Schmitz, G. (2016). A Comprehensive Formal Security Analysis of OAuth 2.0. *CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, (pp. 1204-1215).

Government of United Stated of America. (2019, October 8). *cybersecurity framework*. Retrieved from https://www.nist.gov/cyberframework/online-learning/components-framework

Hardt, E., & Microsoft. (2012, October). *The OAuth 2.0 Authorization Framework.* Retrieved from Internet Engineering Task Force (IETF): https://tools.ietf.org/html/rfc6749#section-1.2

Hossain, N., Hossain, M. A., Hossain, M. Z., & Sohag, M. H. (2018). OAuth-SSO: A Framework to Secure the OAuth-Based SSO Service for Packaged Web Applications. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).* New York, NY , USA: IEEE.

Hunt, P., Oracle, Grizzle, K., Sailpoint, Ansari, M., Cisco, . . . Salesforce. (2015, September). *System for Cross-domain Identity Management: Protocol*. Retrieved from Internet Engineering Task Force (IETF): https://tools.ietf.org/html/rfc7644#section-7.1

IBM Cloud Education. (2019, May 22). *IT Infrastructure library*. Retrieved from IBM Cloud Learn Hub: https://www.ibm.com/cloud/learn/it-infrastructure-library

International Organization for Standardization. (1947). *About us: International Organization for Standardization*. Retrieved from https://www.iso.org/about-us.html

International Organization for Standardization. (2015). *Information technology — Service management — Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services*. Retrieved from ISO official website: https://www.iso.org/standard/65671.html

International Organization for Standardization. (n.d.). *Structure: International Organization for Standardization*. Retrieved from International Organization for Standardization official website: https://www.iso.org/structure.html

Internet Engineering Task Force (IETF). (2006). *Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms.* Retrieved from RFC 4513: https://tools.ietf.org/html/rfc4513#page-11

ISACA. (2010). *About ISACA*. Retrieved from ISACA Corporation website: http://www.isaca.org/about-isaca/Pages/default.aspx

ISACA. (2019). *COBIT 2019 Publications & Resources*. Retrieved from ISACA corportation website: http://www.isaca.org/COBIT/Pages/COBIT-2019-Publications-Resources.aspx

ISO. (2013). *ISO/IEC 27002:2013*. Retrieved from ISO official website: https://www.iso.org/standard/54533.html

ISO. (2015). *ISO/IEC 27017:2015*. Retrieved from ISO official website: https://www.iso.org/standard/43757.html

ISO. (2015). *Standard description*. Retrieved from ISO official website: https://www.iso.org/standard/62816.html

ISO. (2020). *35.020 INFORMATION TECHNOLOGY (IT) IN GENERAL*. Retrieved from https://www.iso.org/ics/35.020/x/

ISO. (2020). *Information technology — Service management — Part 11: Guidance on the relationship between ISO/IEC 20000-1 and service management frameworks: ITIL*. Retrieved from https://www.iso.org/standard/79025.html

Khodabacchus, M., Soyjaudah, K. M., & Ramsawock, G. (2017). Secured SAML cloud authentication using fingerprint. *2017 1st International Conference on Next Generation Computing Applications (NextComp).* Mauritius: IEEE.

Mainka, C., Mladenov, V., Schwenk, J., & Wich, T. (2017). SoK: Single Sign-On Security — An Evaluation of OpenID Connect. *2017 IEEE European Symposium on Security and Privacy (EuroS&P).* Paris, France: IEEE.

Microsoft. (2019, April 22). *ADFS Overview*. Retrieved from Microsoft website: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/overview/whats-new-active-directory-federation-services-windows-server

Microsoft Corporation. (2019, July 11). *What is Azure AD Privileged Identity Management?* Retrieved from Microsoft Azure Website: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Naik, N., & Jenkins, P. (2016). A Secure Mobile Cloud Identity: Criteria for Effective Identity and Access Management Standards. *2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud).* Oxford, UK: IEEE.

NIST: Computer security resource center. (2019, December 5). *Computer Security Resource Center*. Retrieved from Cryptographic Module Validation Program: https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards

Nom, p. d. (Année). Titre de l'article. *Titre du journal*, Pages de - à.

Nom, p. d. (Année). *Titre du livre.* Nom de la ville: Nom de l'éditeur.

OASIS Open 2005. (2005, March 15). *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0.* Retrieved from OASIS document website: http://docs.oasis-open.org/security/saml/v2.0/

Oppliger, R. (2016). *SSL and TLS: Theory and Practice.* Artech Hpuse.

PCI Security Standards Council. (2006). *pci_security*. Retrieved from https://www.pcisecuritystandards.org/pci_security/

Rescorla, E. (2000). *IETF RFC 2818: HTTP over TLS.*

Rescorla, E., & Mozilla. (2018, August). *The Transport Layer Security (TLS) Protocol Version 1.3*. Retrieved from Internet Engineering Task Force (IETF) : https://tools.ietf.org/html/rfc8446

Revar, G. A., & Bhavsar, D. M. (2011). Securing user authentication using single sign-on in Cloud Computing . *Nirma University International Conference on Engineering.* Ahmedabad, India.

Sakimura, N., Bradley, J., Jones, M., & Jay, E. (2014). *OpenID Connect Discovery 1.0 incorporating errata set.*

SSAE 16. (2011). *About Us: SSAE 16*. Retrieved from http://ssae16.com/SSAE16_overview.html

Terra, J. (2019, December 6). *ITIL 4 vs ITIL V3: What's New?* Retrieved from simplilearn: https://www.simplilearn.com/itil-4-vs-itil-v3-whats-new-article

Wikipedia. (n.d.). *Federated Identity*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Federated_identity