12-12-2020

A Zero-Trust Federated Identity and Access Management Framework for Cloud and Cloud-based Computing Environments

Monjur Ahmed

Krassie Petrova

A Zero-Trust Federated Identity and Access Management Framework for Cloud and Cloud-based Computing Environments

Monjur Ahmed[1]

Centre for Information Technology, Waikato Institute of Technology,

Hamilton, New Zealand

Krassie Petrova

School of Engineering, Computer & Mathematical Sciences, Auckland University of Technology,

Auckland, New Zealand

ABSTRACT

Identity and Access Management (IAM) is an important aspect of information security. The deployment of cloud computing (CC) and cloud-based computing (CbC) creates a complex information security scenario involving multiple global stakeholders and geographically dispersed infrastructures. Therefore, implementing IAM in CC/CbC requires the consideration and consolidation of multiple factors. A trust-based approach towards information security may not be a credible option for the CC/CbC environment as trust-based relationships among different architectural elements and including human beings may pose an additional security threat to the cloud space. In this paper, we propose a zero-trust framework for federated IAM in CC/CbC. The proposed framework incorporates a decentralised approach towards IAM that aims to minimise any single entity's controlling power over the digital assets in the CC/CbC space. The critical component of the proposed framework is the decentralised audit log.

Keywords: Access management, identity management, zero-trust framework, federated security, cloud computing.

INTRODUCTION

Identity and Access Management (IAM) and access control is a critical component of distributed computing approaches such as Cloud Computing (CC) and Cloud-based Computing (CbC) including Internet of Things (IoT), Fog Computing and Edge Computing (Ahmed et al. 2020; Guo et al. 2019; Fan et al. 2017). Where CC/CbC services are offered on a commercial basis, the computing platforms are normally provided by a cloud service provider (CSP). A number of CSPs may pool their resources together in order to better manage cost and customer demand, forming a federated cloud (Ahmed, Nahar, Urmi, & Taher, 2020; Mashayekhy et al. 2019).

A CSP serves and communicates with a number of different customers (individual or corporate). In the cloud environment, customer data and other digital assets reside within the CSPs' physical infrastructure (i.e., in the CSPs' computers known as cloud servers). Therefore, the mechanisms for managing access to customer resources has remained mainly CSP-centred (Indu et al. 2018). With CSPs responsible for IAM, cloud customers have become significantly CSP-reliant with respect to ensuring the safety and security of their

[1] Corresponding author. monjur.ahmed@wintec.ac.nz

entrusted digital assets (Sen and Tiwari 2017). From a privacy and security point of view, customer over-dependency on the CSP as the custodian of customer digital assets is a major concern (Indu et al. 2018; Zhou et al. 2017). Even though service level agreements (SLAs) and legal considerations may help prevent a CSP from unauthorised 'looking into' into the spaces on their Cloud servers where clients' digital assets are kept, the CSP may still retain the capability to perform unauthorised operation(s) on its clients' data (Rizvi et al. 2020). Applying a less CSP-centred approach towards the deployment of cloud-based security and privacy protection would reduce significantly CSPs' capability of sneaking into rooms allocated to clients (as a preventative measure), or at least make it nearly impossible for CSPs to hide their actions if they decide to do so (as a demotivational measure).

Federated identity management is one of the foundations of digital identity management (Hamlen et al. 2011). However, in a traditional federation, the participating entities must maintain a level of trust as they exchange information about user authentication and authorization credentials (Chadwick, 2009). Conversely, in a zero-trust security model, participants such as network or networking elements are not trusted but are always verified (Assunção, 2019; Samaniego & Deters, 2018). In this paper, we propose a zero-trust federated IAM framework for CC/CbC that aims to prevent CSPs from gaining unauthorised access to customer digital assets placed under a CSP's management and residing within the CSP's infrastructure. This goal is achieved by ensuring that a CSP is not sufficiently motivated to use any available 'backdoors' to tamper with clients' digital assets, for example by performing unauthorised Create-Read-Update-Delete (CRUD) operations, or any other unauthorised actions. The proposed framework focuses on authentication, as part of IAM. It enables the creation of an auditable trail of access attempts including ones originating from the CSP within whose infrastructure the digital assets of the customer (individual or corporate) are stored.

The rest of this paper is organised as follows: a brief overview of related research is presented in the next section. The proposed framework is described and discussed in the remaining sections, including research limitations and envisioned further work.

RELATED WORK

An IAM system can be viewed as a framework that provides both policies and technologies to enable authorised access to CC/CbC resources (Carnley and Kettani 2019). Deploying an efficient IAM system may have a positive impact on individual and corporate customers' adoption and continued use of CC/CbC services (Ahmed et al., 2020)

In CC/CbC, computing resources are distributed, with remote access provided by communication networks (e.g., the Internet) (Khalil et al. 2014); therefore, prior research has considered a number of different approaches towards developing a distributed IAM that meets user security and privacy protection expectations (Bendiab et al. 2019; Hamlen et al. 2011; Indu et al. 2018; Patel et al. 2013). For example, Horrow and Sardana (2012) propose an IAM framework that authenticates IoT users through an identity manager which in turn collaborates with a service manager within the IoT architecture. Bendiab et al. (2019) propose a trust model for a federated cloud IAM and note that existing federated IAM systems may not be well suited to the highly dynamic and open nature of the CC/CbC environments. Sharma et al. (2016) propose developing an IAM system as a cloud service (security-as-a-service, SECaaS). Gupta and Quamara (2018) propose an identity-based access control and a mutual authentication framework for a distributed cloud-based IoT that includes the use of smart cards as a means to access cloud-based services (in the case of a single-CSP deployment scenario).

Despite the significant technology advancement, security breaches such as insufficient control over personal data dissemination and customer data leakage continue to occur (Eludiora et al. 2011; Werner et al. 2017). The integration of IAM and the CC/CbC environment may face further technical challenges such as the need to conduct a large-scale penetration testing to validate the robustness of the proposed IAM (Chang et al. 2016), and organisational challenges related to the requirement to add a security dimension to the business processes of the organization adopting IAM (Everett 2011; Uddin and Preston 2015). Reed, Sporney, Longley, Allen, Grant, Sabdello and Holt (2020) propose Decentralised Identifiers (DIDs) which is a decentralised approach that enables verifiable, decentralised digital identity.

As pointed out by Noor et al. (2013), an effective trust management approach may alleviate CC/CbC customers' concerns about distributed digital asset security, and data privacy. In cloud federations in particular, the concept of 'trust' implies the existence of trust relationships between the participating entities and sharing the responsibility of maintaining a secure CC/CbC space (Mashayekhy et al. 2019). However, establishing trust is still a major concern in cloud federations where differing perceptions of shared responsibility may lead to fatal gaps in cybersecurity (Ahmed et al. 2019). A zero-trust approach helps to overcome this obstacle (Scott, 2018). In a zero-trust model, no trust-by-default is the standard premise (Ahmed et al. 2020). Eliminating the need to develop and maintain trust relationships removes a highly significant factor from the CC/CbC security space which should result in a better integrated and better secured CC/CbC architecture.

A ZERO-TRUST IAM FRAMEWORK FOR CC/CbC

As part of IAM, authentication and subsequent authorisation remain at the core of securing a distributed computing system (Sharma et al. 2016). Authentication allows the different parties involved to mutually ascertain each other's identity before commencing actual communication across the distributed environment (Wang et al. 2020). Cloud-based resources are complex to both manage and protect as the distributed environment widens the doors to cyberattacks. However, malicious activities may go unnoticed as in the CC/CbC environment, it is often a significant challenge to identify a security breach. First, the cloud service customer may not have a complete knowledge of who the active IAM parties are, especially in a federated trust-based computing environment. Second, to trace down the activities of all parties involved in handling an organisation's digital assets in the cloud space may be quite complex both legally, and technologically (Patel et al. 2013; Suganya and Sujatha 2020). To compound the issue, in any CC/CbC architecture, the distributed digital resources may not even reside under the management of a single entity. This adds to the challenges of providing reliable authentication and authorisation services across the CC/CbC plane (Porambage et al. 2016).

The decentralisation of the framework is inspired by the decentralisation approach to secure system proposed by Ahmed (2018). A multi-CSP authentication process lies at the heart of the proposed zero-trust framework. Multiple CSPs participate in a dynamic federation which provides an authentication service on request. The authentication process is not associated with any specific technology or tool. It works on the principle of decentralisation. The end-user to be authenticated is a customer of one or more CSPs but not of all CSPs involved in the CSP federation. For any authentication request, each of the CSPs acts either as a 'native-CSP' or as an 'audit-CSP'. A native-CSP stores digital assets belonging to the end-user and may also store some of their credential information. An audit-CSP contributes to the authentication process; it stores part of the end-user credentials but does not store any end-user digital assets. An audit-CSP must not be a native-CSP, and can be any of the foreign CSP. An audit CSP is a regular CSPs or a purpose built CSPs offering Auditing as a Service (AaaS).

An example illustrating the concept as presented in Figure 1. Here, CSP-a is a native-CSP while CSP-b and CSP-c are audit-CSPs. Assuming CSP-a does not store any part of the end-user credential information, this CSP federation comprises the minimum number of CSPs required (i.e., three different CSPs). The CSP configuration can be expanded to include any number of CSPs.

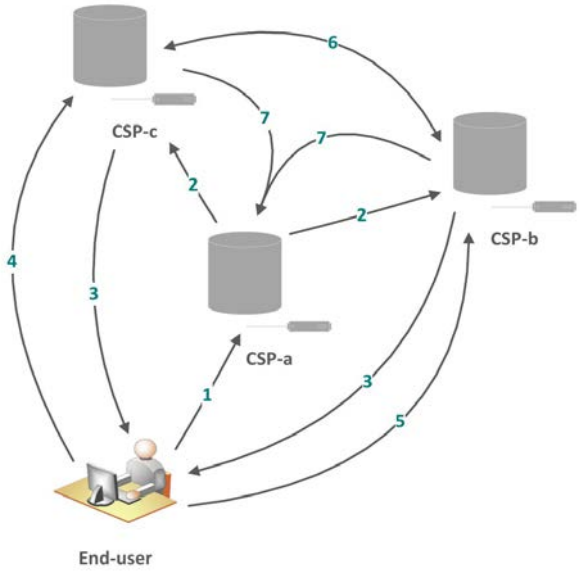

Figure 1. A Zero-Trust IAM Framework for CC/CbC

More generally, the distribution of CSPs can be represented as

$\forall q \in n, \{(CSP_A+1) > CSP_N\} \wedge CSP_N=>1)$ ..... (i)

where:

n = Total number of CSPs, CSP_N = Total number of Native-CSPs, CSP_A = Total number of Audit-CSPs, and q = a CSP.

This implies that there needs to be at least one native-CSP, and that the total number of audit-CSPs must be greater than the number of native-CSPs. The example in Figure 1 also shows how the flow of the authentication events reduces the opportunity of a CSP tampering with the authentication process or with the log. The steps of the authentication process are outlined and explained below. (Note: it is assumed that the partial end-user's credential sent to audit-CSP-c in step 4 is different from the one sent to audit-CSP-b in step 5.)

1. End-user initiates a login request to a native-CSP (in this example, CSP-a).
2. Native-CSP (CSP-a) informs the relevant audit-CSPs (in this example, CSP-b and CSP-c) about the login request.
3. Audit-CSPs send an authentication (credential) request to the end- user.
4. End-user sends a partial credential (e.g., a username) to an audit-CSP (in the example, CSP-c).
5. End-user sends a partial credential (e.g., a password, or an access token) to an audit-CSPs (in this example, CSP-b).

6. The audit-CSPs involved in steps 4 and 5 authenticate the end-user to the native-CSP (CSP-a).
7. Audit-CSPs advise native-CSP on the outcome of authentication and all CSPs log the authentication details.

The framework ensures that the full set of credential components (i.e., the complete information required for the successful authentication of the end-user) is not held by any participating CSP). Secret (challenge) end-user credentials are distributed across multiple audit-CSPs (or across multiple groups of audit-CSPs). To achieve the purpose of not allowing any single entity (or a single group of entities) to have control over the end-user authentication credentials, the two audit groups should not overlap, and should never share with each other the end-user credential they store. Furthermore, the secret credential stored by one of the groups should not be interchangeable with the secret credential stored by the other group. As shown in Figure 2, if the end-user has two different pieces of secret authentication credentials A and B, and a non-challenge credential C, at least two audit-CSPs (or two groups of audit-CSPs) will be required for successful authentication.

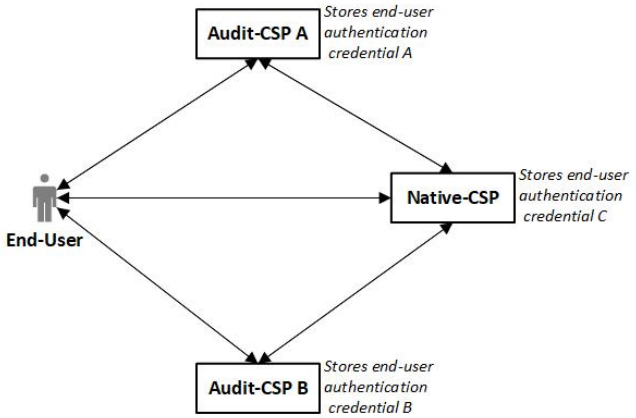

Figure 2. Parties Involved in the Authentication Process

A native-CSP may store a non-challenge part of the full set of credentials (e.g., the username), or may store only some of the challenge part of the credential set (e.g., one of the factors in the case of multi-factor authentication, or part of an access key but not the whole key). In the example in Figure 2, the participating native-CSP uses their knowledge of the non-challenge component C in order to complete the end-user authentication. For best results, the challenge part of the credential set (i.e., the user's secret) should not be stored by a native-CSP even partially. Ideally, it should be stored is a decentralised manner by the audit-CSPs.

The general rule of distribution of the user credential information can be represented as

$$\forall D\ \exists\ (n \in N) \wedge (\text{Auth-CSP}_A > \text{Auth-CSP}_N \mid \text{Auth-CSP}_A \notin \text{Auth-CSP}_N) \quad \text{..... (ii)}$$

where:

n = Total number of credential components, N = Natural numbers, Auth-CSP_A = Credential information stored in audit-CSPs, Auth-CSP_N = Credential information stored in native-CSPs, and D = Distribution of credential information among CSPs.

The above implies that the distribution of the end-user credentials must ensure that authenticating audit-CSPs hold more pieces of credential information than authenticating

native-CSPs, and that a native-CSPs should not act as an authenticating CSP since native CSPs may store only a non-challenge part of users' credentials.

The proposed framework requires an audit log where each activity related to the authentication of a particular end-user is recorded as a separate transaction. Thus, the audit log provides a map of the authentication process flow and makes available for inspection the full audit trail of login attempts. Importantly, in order to support the provision of a robust federated and decentralised user authentication process, the audit log should not be fully stored by any participating CSP. In other words, the audit log should be maintained and managed in a decentralised manner, with any participating CSP storing only a part of the resulting distributed login transaction database.

Second, to ensure that audit log records already made are not modified, the decentralised audit log should never be updated except for adding new transactions (i.e., the audit log database should allow only 'read' and 'append' operations). To avoid losing its credibility in the case of any integrity breach affecting the audit log, the framework should have a 'healing' capability, such as keeping backup copies that would allow the system to 'roll back'. However, maintaining multiple redundant copies of the audit log database may present a challenge due to its decentralised nature.

DISCUSSION

The traditional centralised approach to end-user authentication may increase organisations' exposure to credential harvesting and identity theft (Abayomi-Zannu and Odun-Ayo 2019). The proposed framework addresses this concern by providing for a federated, decentralised authentication system. In contrast to the still prevalent trust-based approach to IAM (Keltoum and Samia, 2017; Bendiab et al. 2019), the framework applies a zero-trust principle, i.e., it removes' trust' from the operational context of the authentication process. The innovation of the proposed framework stands in it's using decentralised processing involving multi-party management of the authentication process in a zero-trust security environment. The framework facilitates the collaborative work of the CSPs involved in the federation but does not establish or require any trust-based relationships among them

The aim of the proposed framework is to discourage the malicious insiders (e.g., CSP, or any individual) through an unavoidable, non-erasable and traceable footprint. The IAM system is decentralised in such a way that no single participating entity 'owns' the total sum of a customer's credentials (and digital assets). This reduces significantly the power of any single CSP to control the authentication process or to commit any unauthorised modification (through bypassing standard authentication procedures) of the audit log. Therefore, participating CSPs will be unlikely to access client assets in an unauthorised manner, due both to their limited knowledge of the relevant client credentials, and the exposed nature of the shared audit log. Second, the proposed framework enables the detection of security incidents, as it equips the CC/ CbC environment with a mechanism to ensure that a breach cannot be kept hidden once it occurs.

The decentralised audit log described in the preceding section is a critical component of the proposed framework. While the inability to delete or update any existing information is a key requirement, an in-depth consideration of the design and deployment of an 'append only' mechanism for maintaining a decentralised audit log is out of the scope of this paper. The architecture for a distributed and decentralised security model for CC proposed in (Ahmed, 2018) and the related algorithm for preventing unauthorised data modification through decentralisation in (Ahmed & Sarkar, 2020) may provide some useful references. With its

strong support of decentralisation, blockchain technology (Nakamoto, 2017; Pilkington, 2016) may be also considered as a potential decentralisation mechanism.

A possible limitation of framework is the potential for implementation-related processing bottlenecks or other system performance issues. In addition, decentralised computing may incur operational overheads due for example to multiple instances of the same process running concurrently, or other redundancy requirements.

Directions for further work and research include the development of a reliable mechanism for achieving the decentralisation of the audit log and meeting its functional requirements (the audit log should be 'write-once' and there should be no way to modify any existing records). Carefully selecting an existing technology that may serve the purpose and developing a proof-of-concept system would be instrumental in demonstrating the benefits of the proposed framework in comparison to other approaches, and in addressing the limitations identified above. We also intend to further explore the feasibility of including (or excluding) native-CSPs from a security perspective.

CONCLUSION

The proposed zero-trust IAM framework is a conceptual one. It can be implemented using any technologies that can serve the purpose. While authentication (and subsequently, authorisation) is key to ensuring that legitimate users are provided with information access according to their legitimate privileges, it is equally important to ensure the existence of write-protected evidence of the login events. The proposed framework meets these requirements by employing a zero-trust approach that is complemented by a 'write-once' event log system. The decentralisation and the involvement of multiple CSPs is to ensure that there is no single entity in control of the authentication process and that all login attempts are securely receded and open to inspection. However, the framework requires the deployment of an additional mechanism to protect the trust-less model from unauthorised modifications of the shared audit log.

REFERENCES

Ahmed, I., Nahar, T., Urmi, S. S., and Taher, K. A. 2020, January. "Protection of Sensitive Data in Zero Trust Model," in *Proceedings of the International Conference on Computing Advancements*, New York: ACM Press, pp. 1-5.

Ahmed, M. (2018). Ki-Ngā-Kōpuku: a Decentralised, Distributed Security Model for Cloud Computing (Doctoral dissertation, Auckland University of Technology, New Zealand).

Ahmed, M., Sarkar, N. I. (2020). Privacy in Cloud-based Computing. in G. Cornetta, A. Touhafi, & G. Muntean (Eds.), Social, Legal, and Ethical Implications of IoT, Cloud, and Edge Computing Technologies. IGI Global, USA. (in-press)

Abayomi-Zannu, T., and Odun-Ayo, I. 2019. "Cloud Identity Management–A Critical Analysis," in *Lecture Notes in Engineering and Computer Science: Proceedings of the International MultiConference of Engineers and Computer Scientists*, pp. 170-175. Hong Kong: Newswood Academic Publishing

Ahmed, U., Raza, I., and Hussain, S.A. 2019. "Trust Evaluation in Cross-Cloud Federation: Survey and Requirement Analysis," *ACM Computing Surveys* (52:1) (doi: 0.1145/3292499).

Assunção, Pedro. (2019). A Zero Trust Approach to Network Security. Proceedings of the Digital Privacy and Security Conference. DOI: 10.11228/dpsc.01.01

Bendiab, K., Shiaeles, S., Boucherkha, S., and Ghita, B. 2019. "FCMDT: A Novel Fuzzy Cognitive Maps Dynamic Trust Model for Cloud Federated Identity Management," *Computers & Security* (86) (doi: 10.1016/j.cose.2019.06.011).

Carnley, P. R., and Kettani, H. 2019. "Identity and Access Management for the Internet of Things," *International Journal of Future Computer and Communication* (8:4), pp.129-133.

Chadwick, David W. (2009) Federated Identity Management. In: Aldini, Alessandro and Barthe, Gilles and Gorrieri, Roberto, eds. FOSAD 2008/2009. LNCS (5705). Springer-Verlag, Berlin, pp. 182-196. ISBN 978-3-642-03828-0. DOI https://doi.org/10.1007/978-3-642-03829-7_

Chang, V. Kuo, T.-H., and Ramachandran, M. 2016. "Cloud Computing Adoption Framework: A Security Framework for Business Clouds." *Future Generation Computer Systems* (57) (doi: 10.1016/j.future.2015.09.031)2016).

Eludiora, S., Abiona, O., Oluwatope, A., Oluwaranti, A., Onime, C., and Kehinde, L. 2011. "A User Identity Management Protocol for Cloud Computing Paradigm," *International Journal of Communications, Network and System Sciences* (4:3), pp. 152-163.

Everett, C. 2011. "Identity and Access Management: The second Wave," *Computer Fraud & Security* (5) (doi: 10.1016/S1361-3723(11)70051-3).

Fan, K., Wang, J., Wang, X., Li, H., and Yang, Y. 2017. "A Secure and Verifiable Outsourced Access Control Scheme in Fog-Cloud Computing," *Sensors* (17:7) (doi: 10.3390/s17071695).

Guo, S., Hu, X., Guo, S., Qiu, X., and Qi, F. 2019. "Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System," *IEEE Transactions on Industrial Informatics* (16:3), pp. 1972-1983.

Gupta, B.B., and Quamara, M. 2018. "An Identity Based Access Control and Mutual Authentication Framework for Distributed Cloud Computing Services in IoT Environment Using Smart Cards," *Procedia Computer Science* (132) (doi: 10.1016/j.procs.2018.05.185).

Hamlen, K., Liu, P., Kantarcioglu, M., Thuraisingham, B., and Yu, T. 2011. "Identity "Management for Cloud Computing: Developments and Directions," in F. Sheldon, R. Abercrombie, and A. Krings (Eds) Proceedings *of the 7th Annual Workshop on Cyber Security and Information Intelligence Researc*h, New York: ACM Press (doi: 10.1145/2179298.2179333).

Horrow, S. and Sardana, A. 2012. "Identity Management Framework for Cloud Based Internet of Things," in *Proceedings of the 1st International Conference on Security of Internet of Things*, New York: ACM Press (doi: 10.1145/2490428.2490456).

Indu, I., Anand, P. R., and Bhaskar, V. 2018. "Identity and Access Management in Cloud Environment: Mechanisms and Challenges," *Engineering science and technology, an International Journal* (21:4), pp. 574-588.

Keltoum, B., and Samia, B. 2017. "A Dynamic Federated Identity Management Approach for Cloud-Based Environments," in *Proceedings of the 2nd International Conference on Internet of Things, Data and Cloud Computing*. **(**doi: 10.1145/3018896.3025152).

Khalil, I. M., Khreishah, A., and Azeem, M. 2014. "Cloud Computing Security: A Survey," *Computer*s (3:1), pp. 1-35.

Mashayekhy, L., Neiad, M. M., and Grosu, D. 2019. "A trust-aware mechanism for cloud federation formation." *IEEE Transactions on Cloud Computing* (doi: 10.1109/TCC.2019.2911831).

Nakamoto, P. 2017. *Bitcoin: Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money*. Scotts Valley, CA: CreateSpace Independent Publishing Platform.

Noor, T. H., Sheng, Q. Z., Zeadally, S., and Yu, J. 2013. "Trust Management of Services in Cloud Environments: Obstacles and Solutions," *ACM Computing Surveys* (46:1) (doi: 10.1145/2522968.2522980).

Patel, A., Taghavi, M., Bakhtiyari, K., and Junior, J. C. 2013. "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review," *Journal of Network and Computer Applications* (36:1), pp. 25–41.

Pilkington, M. 2016. "Blockchain Technology: Principles and Applications," in F. X. Ollero, and M. Zhegu (Eds.) *Research Handbook on Digital Transformations*, Northhampton, MA: Edward Elgar Publishing, pp.225-253.

Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gorton, A., and Vasilakos, A. V. 2016. "The Quest for Privacy in the Internet of Things," *IEEE Cloud Computing* (3:2), pp. 36-45.

Reed, D., Sporney, M., Longley, D., Allen, C., Grant, R., Sabdello, M., & Holt, J. 2020. Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations. World Wide Web Consortium, Cambridge, MA. Available at: https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers

Rizvi, S., Mitchell, J., Razaque, A., Rizvi, M. R., and Williams, I. 2020."A Fuzzy Inference System (FIS) to Evaluate the Security Readiness of Cloud Service Providers," *Journal of Cloud Computing* (9) (doi: 10.1186/s13677-020-00192-9).

Samaniego, M., & Deters, R. (2018, July). Zero-trust hierarchical management in IoT. In 2018 IEEE International Congress on Internet of Things (ICIOT) (pp. 88-95). IEEE.

Scott, B. 2018. "How a Zero Trust Approach Can Help to Secure Your AWS Environment," *Network Security* (3) (doi: 10.1016/S1353-4858(18)30023-0).

Sen, A. K., and Tiwari, P. K. 2017. "Security Issues and Solutions in Cloud Computing," *IOSR Journal of Computer Engineering* (19:2), pp. 67-72.

Sharma, D. H., Dhote, C. A., and Potey, M. M. 2016. "Identity and Access Management as Security-as-a-Service from Clouds," *Procedia Computer Science* (79) (doi: 10.1016/j.procs.2016.03.11).

Suganya, R., and Sujatha, S. 2020. "Security Protocol for Cloud-Based Communication," *Design and Analysis of Security Protocol for Communication* (2020): 235-241.

Uddin, M., and Preston, D. 2015. "Systematic Review of Identity Access Management in Information Securit," *Journal of Advances in Computer Networks* (3:2), pp. 150-156.

Wang, L., An, H., and Chang, Z 2020. "Security Enhancement on a Lightweight Authentication Scheme with Anonymity for Fog Computing Architecture," *IEEE Access* (8) (doi:10.1109/ACCESS.2020.2996264).

Werner, J., Westphall, C. M., and Westphall, C. B. 2017. "Cloud Identity Management: A Survey on Privacy Strategies," *Computer Networks* (122) (doi: 10.1016/j.comnet.2017.04.030).