Issues in Information Systems
Volume 24, Issue 2, pp. 22-32, 2023

DOI: https://doi.org/10.48009/2_iis_2023_103

Enhancing cybersecurity using a new dynamic approach to authentication and authorization

Abdur Rahim Choudhary, *Choudhary Associates, arc@choudharyassociates.com*

Abstract

This paper adopts a new dynamic approach towards user authentication and authorization to enhance security in Cyber Networks. The concept of user ID is generalized by embedding additional attributes incorporating detailed user profile, operational context, common operating picture, and situation awareness. This leads to a new paradigm that is formulated as a Computable Compound Identity Measure (CCIM). Using CCIM the existing authentication and authorization schemes are integrated and generalized to a process that also embeds access control. The CCIM scheme is risk-adapted and dynamically responsive to the operational need. This responsiveness is proportional to the operational information incorporated into the CCIM decision making, including its dynamic and variable content. The paper also presents a conceptual architecture to demonstrate how to deploy this new scheme using Policy-Based Management (PBM) technology. This technology is the operational enabler for the dynamic behavior of the CCIM scheme. A working prototype product does exist though its inner details are proprietary and cannot be shared in this paper. This CCIM based authentication and authorization technology is an important step towards a fundamental solution versus ineffectual patches, partial solutions, and piecemeal approaches. The technology addresses constantly changing threat environment with a cost-effective technology that evolves and adapts in a dynamic manner to offer operational responsiveness and risk aversion.

Keywords: computable compound identity measure, dynamic access control, contextual identity, multi-level passwords, policy-based management.

Introduction

The term cyber security is coined to represent the ever-expanding requirements, scope, and challenges of the information technology security. The challenge of its governance, risk aversion, and standardization is now becoming apparent. However, awareness of its extent is not fully appreciated because the community is lagging behind in the deployment of the available technology solutions and products. Even though the spectrum of technology solutions is sometimes taxonomized, it is done using the same type of thinking about the security threats and the technology approach in response to the threats. In this paradigm, there is a perpetual race where the attackers are always a step ahead of the defenders. The initiative remains with the attackers and the defenders are delegated to a position where they only can react.

A disruptive approach has not been so far envisioned to stop this perpetual race and the predicament of the defenders in it. In this paper, we propose a new dynamic technology that promises to snatch the initiative from the attackers and gives it to the defenders. This new technology breaks down the present-day barriers between separated technologies for authentication, authorization, and access control. These barriers are removed in technological terms as well as in terms of deployment topology and operational concepts. The technology uses a mathematically computable numeric measures for the risk of providing access and the cost of refusing it. These computed measures are not static; they dynamically adjust as the common operations picture and the situation awareness parameters change. They also adjust with the operational evolution over time, and can accept new modes for operational scenarios required by evolved business goals. The existing technologies can do none of these.

In the next section we introduce the case for the need of a paradigm shift. The following section presents the computable compound identity measure (CCIM) scheme. Next, we discuss policy enablement of an existing authentication application, and a conceptual architecture showing how the CCIM scheme is overlaid on an existing application. The common operating picture and situation awareness dynamics are discussed in section that follows. Major advantages of the CCIM solution over the existing practices are discussed next. Next, we discuss some elaborations about the CCIM, and finally present the main conclusions. We remind the reader that architecture and design details are withheld in this paper for proprietary reasons, though such details are obviously available since a working prototype product has already been developed.

Traditionally authentication depends upon user ID and password. Both of these are poor instruments in today’s high threat environment in cybersecurity. User ID is just a string. Currently the user ID does not play a significant role, and we will see how the technology presented in this paper changes this situation drastically. Consequently, the emphasis, in the current authentication process, is therefore placed squarely on the passwords. The password too is just a string. This situation inevitably leads to over reliance on passwords and consequent complexification of the string that represents the password. Enterprises go to great lengths at specification of the structure of the password string. For example, they specify the minimum length of the password string, and that it include lower and upper-case letters, numerals and special characters. Such requirements make it difficult for the user to remember the password, and to input it for authentication purposes. The current authentication process is neither user friendly nor is it effective to keep the systems secure.

Hence, additional measures are invented for situations where security is of special concern. Passwords are, therefore, generalized to include onetime passwords, Secure ID devices, smart cards such as the Common Access Card (CAC) used by the Department of Defense (DoD), and biometrics such as iris and finger print schemes. With these schemes the reliance on passwords for the purpose of authentication keeps increasing, and the user friendliness of the process diminishes. The above steps still leave the security unsatisfactory. Therefore, they are augmented with additional operational constraints. These include various procedures. One such procedure is the concept of continued authentication that requires the user to periodically re-authenticate by providing the password again and again. This would detect an imposter who starts using an unlocked machine while the genuine user had stepped away. However, it imposes an inconvenience for the genuine user to have to periodically re-authenticate. Nevertheless, such measures still do not make the currently deployed authentication systems sufficiently secure.

The current authentication paradigm is rather limited and inflexible. It also fails in the primary reason for which it is intended, namely to make authentication secure. What is needed is a paradigm shift. Knowing that both strings, user ID and password, are ineffectual to make the current authentication practices secure, the research presented in this paper generalizes the use of both these strings. This paper provides the needed paradigm shift by introducing an innovative new concept, namely, the Computable Compound Identity Measure (CCIM). In this paradigm the user ID string (Camp 2004) is replaced by an intelligent and rich construct that computes into quantitative measures. The CCIM therefore becomes at least as important in the authentication process as the password is in the current paradigm. For example, even if someone logs in with valid user ID and password, the CCIM can overrule that determination and deny access to that user based on the common operating picture and situation awareness parameters which are included in the CCIM and the authentication decision making. The reliance on passwords is thus reduced because password is now only one of many criteria that are used in making the authentication decision.

Moreover, there can now be multiple levels of passwords, each carrying its assigned credentials and relative weight in making the authentication decision. For example, a simple multi-level passwords scheme could consist of a lenient password and a stricter password; each password carrying its own relative weight and access credentials; and the lenient password can be more user friendly in ease of remembering and ease to input. As the user ID is generalized into a CCIM scheme, the password is generalized into a multi-level passwords scheme.

In generalizing the user ID into a rich CCIM scheme, the boundary between authentication and authorization is now eliminated. The required information, such as security clearance and operational role is incorporated into the CCIM scheme such that the same technology now serves for authentication, authorization, and access control. The processes, technologies, and practices that are currently three separated entities are integrated into one unified CCIM scheme. The detrimental boundaries, from security perspective, between these three entities are eliminated to provide one uniform CCIM scheme. Therefore, the CCIM scheme is a big paradigm shift and potentially a disruptive technology. The paper reports the laboratory development of this technology.

CCIM Technology

Basic ideas were presented in Choudhary 2006. Research has continued to develop those ideas to meet the Cyber Security needs of present-day business applications and network operations, especially the scenarios from the department of defense (DoD). The CCIM technology used in this paper is a substantial growth beyond the ideas in Choudhary 2006. Substantial further research was performed during work with Defense Information Systems Agency (DISA). A prototype product was developed though its details are not publicly releasable, because they are company proprietary.

Under CCIM, the concept of user ID is generalized into an elaborate scheme that is defined both at a qualitative level and a quantitative level. The qualitative generalization incorporates detailed information about the user that the enterprise possesses, more particularly an enterprise like the DoD. This information is organized into an elaborate profile for the user who seeks access. Examples of such pieces of information are as follows:

> name, user ID, organization, position within the organization, permanent office location and address, home address, current location of deployment, the remote office location to which the user is assigned on the tour of duty, security clearance, smartcard ID, device ID, security certificates, encryption keys, certification authority, mission to which he is assigned, the task within the mission, the owner (commander) of the mission, common operating picture about the mission theater, situation awareness about the task, user honorable awards and reprimands, occurrences of compromise of his password or smartcard or mobile device, known personal episodes, and travel and recreation etc.

The above list is only illustrative. Similar information is also compiled about the machines for machine-to-machine authentication.

In general, the parameters representing the information organize themselves into three broad categories, namely:

- the Static ID containing parameters like the user-name,

- the Contextual ID containing parameters like the security clearance, and
- the Global ID containing such parameters as the mission and the common operation picture in the mission theater.

The three different IDs are formulated into the computable compound identity (CCI) as is illustrated in Figure 1 below. The CCI is a unique descriptor for the user at a qualitative level.

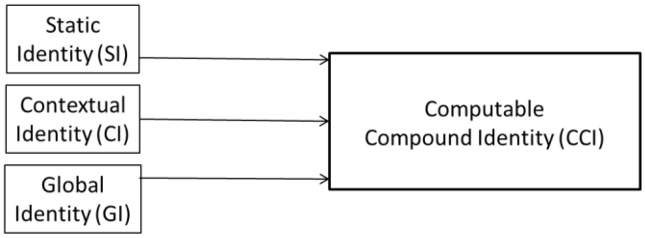

Figure 1: Generalizing the current paradigm of User ID into a Computable Compound Identity

At the quantitative level, CCI Measure (CCIM) is generated from the CCI by applying a compounding scheme which itself may incorporate additional parameters such as the relative weight factors. More precisely speaking, the equation below is an example of the compounding scheme that generates the CCIM from CCI.

$$\mathbf{CCIM = \{\sum wnvn\}/\{\sum WnVn\}}$$

Here n runs over all the applicable parameters that define the CCI, vn is the value assigned to the nth parameter for the user whose authentication is sought, Vn is the maximum possible value for the same parameter; wn is the corresponding weight factor assigned to the nth parameter and Wn is the maximum possible weight factor for it. The denominator is for normalization of CCIM so that the maximum possible value for CCIM is the value one. The CCIM measure is a probability.

This CCIM compounding scheme allows implementing the enterprise authentication policies and their operational intent in a qualitative as well as quantitative manner. The qualitative aspect is specified through the parametric variables included in the definition of the CCI, as shown in Figure 1; and the quantitative aspect is specified through the numeric computations using the assigned parametric values and the associated weight factors used in computing the CCIM, as shown in the equation above.

Thus, the CCIM scheme also provides an explicit mechanism to deploy the Intent Based Operations (IBO) through the assignment of parametric values and the associated weight factors (Choudhary 2022). The Policy Based Management (PBM) technology further finetunes this IBO capability of the CCIM scheme through the specification of enterprise operations digital policies via the choice of policy parameters, policy conditions, and policy actions (Choudhary 2004).

An example of the intent-based operations aspect of the CCIM scheme is to override an authentication decision made by the existing traditional authentication mechanisms, as is shown in Figure 2 in the next section. This happens dynamically in response to an overarching factor such as a raised Cyber threat level, variations in the common operating picture, and situation awareness conditions.

We have introduced the CCIM technology as a smart authentication technology. However, it is richer than each of the three existing technologies for authentication, authorization, and access control: richer than each individually and considerably more so in terms of their combined effect. Therefore, CCIM technology encompasses all three technologies such that it enhances the capabilities of and enriches the scope of each one of them. It integrates the three technologies under one framework, and unifies them such that the boundaries between them are eliminated. Nevertheless, for the purpose of this paper we will continue to refer to the CCIM technology as authentication technology.

Conceptual Architecture

The architecture for the CCIM scheme uses Policy Based Management (PBM). PBM basics are discussed in (Choudhary 2004) and some newer developments are in (Liu and Bi 2018) (Wu et. al. 2021). In this section we will rely on these references and not discuss how we deploy them in this conceptual architecture.

There is, however, one PBM aspect of special interest from the point of view of this architecture that we will discuss, namely the policy enablement of an application. This paper presents a non-intrusive approach in the sense that the existing authentication application is kept largely intact; it only needs to be policy enabled, so that the CCIM technology can be applied to it.

Policy enablement of the existing authentication application means that the authentication application can request policy decisions from the CCIM policy management environment, as well as to receive the decision and act upon it. In practice it means that a Policy Enforcement Point (PEP) is attached to the existing application and the application can communicate with this PEP, as shown on the right side in Figure 2.

The PEP in turn communicates with the CCIM Policy Decision Point (PDP) which represents the policy management and evaluation environment. It is shown on the left side in Figure 2. Therefore, the conceptual architecture for the CCIM scheme has two main modules: the policy enablement of the existing authentication application, and the CCIM policy management and evaluation environment. The architecture overlays the CCIM scheme on the existing application in a non-intrusive way such that the application and the CCIM are decoupled except for the policy enablement.

Common Open Policy Services (COPS) protocol (Walker and Kulkami 2005) is used for communications between the PEP in the application environment and the PDP in the CCIM policy environment. As is shown in Figure 2, the PEP requests service from the PDP by calling upon the method "PDP.evaluate()". This service requests CCIM for the policy decisions and receives the results of this request.

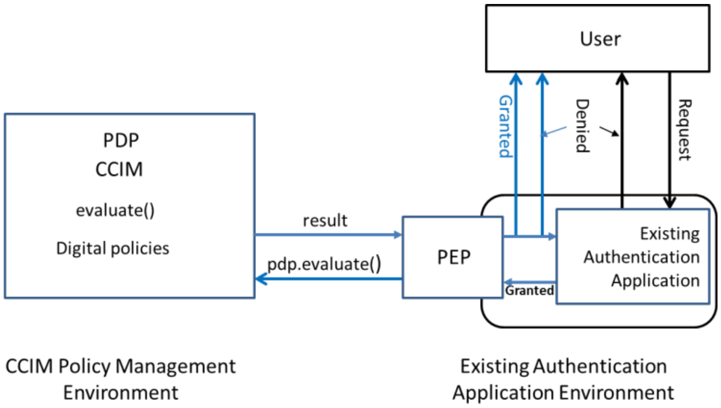

Figure 2: Policy enablement of the existing authentication application and conceptual architecture for CCIM based authentication.

The PEP request for PDP Evaluation includes the parameters that indicate the type of policies to be used, and the communication method to be used for this interface when more than one alternative is available. The PDP receives the request from the PEP, determines the applicable CCIM policies, evaluates these policies, integrates the CCIM policy results for risk assessment versus the operational need, and sends the authentication decision result back to the PEP. The PEP communicates the result back to the existing application using the mechanisms provided by the policy enablement.

The PEP incorporates a functional virtualization of the existing authentication application. This includes an understanding of the application configurations, the data that the application needs to run itself, the data that the application generates, and how to exchange data with the application. This happens along the lines of Network Functions Virtualization (NFV) (ETSI 2021), which is an integral part of policy enablement and related virtualization of security functions (Basile et. al. 2019).

As shown in Figure 2, the existing authentication application receives the user request, as it normally would. This interface remains unchanged, and CCIM mechanisms work non intrusively as an overlay. If the existing application determines that the request should be denied, that is communicated to the user, just as it would normally happen. The policy enablement comes into effect only if the existing application determines that it wants to grant the authentication. Unlike what would normally happen, this decision is not communicated to the user; rather, it is passed on to the PEP which invokes the "PDP.evaluate()" method to seek the final decision under the CCIM policy management and evaluation environment.

The CCIM decision may be "Request Denied" or "Request Granted" and the existing authentication application communicates the decision to the user via its interface with the PEP. Thus, the CCIM framework acts like an overlay on the existing authentication scheme and it can override the "authentication granted" decision arrived at by the scheme in the existing application.

The policy actions incorporated into the CCIM policy decisions results are executed by the PEP through its interface with the existing application. CCIM scheme issues a range of authentication decision actions, corresponding to the set of applicable CCIM policy actions, not just a binary yes or no decision. For example, CCIM scheme can grant authentication, grant authentication but simultaneously monitor the user activities, interrupt the previously granted authentication to re-authenticate as a result of user activity, terminate the previously granted authentication based on the user activity to avoid Edward Snowden type scenarios, send the user to a honey net, deny authentication, and lock the user account, etc.

The inner details of PDP are transparent to the existing application, and therefore do not influence the type of commercial platform for the application or the network provider. CCIM scheme can thus be cost effectively deployed for most platforms without customized development. Further, since the PDP details are transparent to the existing authentication application, these details can be changed at will.

The CCIM policy details and their computation can be transparently changed to accommodate future evolution in requirements and operational scenarios, without impacting the existing authentication application or the users. CCIM scheme strengthens the authentication decision in all cases, for example the cases for multifactor authentication and multilevel security. This means, for example, that an enterprise can save operational costs by using lower factor authentication and still achieve the same or better confidence in the authentication decisions.

Dynamics of Common Operations Picture and Situation Awareness

Common Operations Picture and Situation Awareness are concepts widely used in the Department of Defense (DoD) though their meaning, content, and applications are not well-defined. Moreover, the concepts are going through an evolution (Leedom 2003). We use the terms to represent the critical information regarding overarching operational environment. Examples include the various Defense Conditions (DEFCON), Alert Conditions (ALERTCON), Force Protection Conditions (FPCON), Emergency Conditions (EMERGCON), and Information Conditions (INFOCON), We include the parameters representing these factors into the definition of CCI, and we compute them into the CCIM decision engine to deal with the authentication requests under varying operations and scenarios.

In addition, we include network wide conditions that recognize the source network which originated the authentication request. Following five factors are routinely included in decision making: DEFCON like terror threat, Network Conditions regarding their security trust, Device Type as being enterprise provided or personal, Password Type in our multi-level password scheme, and Special Statuses in the enterprise operations context like normal or special (restricted or enhanced).

Inclusion of parameters that represent COP, SA, and special enterprise conditions, like epidemic related restrictions, makes the authentication decisions in accord with the business intent. They make them dynamically adjustable under varying operational scenarios. Such features are enabled via the formulation of policy parameters, policy conditions and triggers, and policy action sets.

Most of the dynamic adjustments to operational situations are represented without changing any of the above-mentioned formulations or the code representing the policy logic. They are possible just by finetuning the numeric values assigned to the variables and the associated weight factors; and the numeric values of the parameters used in policy formulations.

Advantages of CCIM Technology

This section summarizes a detailed set of advantages of the CCIM scheme, as enabled by the qualitative definition of CCI, the quantitative measures of CCIM computations, and the conceptual architecture described earlier.

The CCIM technology significantly excels the current state of the art for authentication. That is because it incorporates the detailed information profile of the user. CCI incorporates the Static ID, the Contextual ID and the Global ID. The CCI Measure (CCIM) is explicitly computed as measures of the business intent and probabilities of operational situations. This yields numerical values for the authentication risk and its operational need. The authentication decision is made more objective and easier to make by comparing numeric scores.

Following are some of the explicit advantages that derive from these innovations.

1. The authentication decision can be any set of actions under the enterprise policies; for example, to authenticate but also to monitor the user activities, and to seek re-authentication when the user activities warrant. There is no limitation to what the CCIM policy actions can do within the scope of the enterprise business goals. This is a long way forward from the authentication practices that produce binary decisions in yes and no terms.

2. CCIM technology smarts make the authentication decisions risk adapted in the sense of the Risk Adaptable Access Control, RAdAC (Choudhary 2005) (Kandala et. al. 2011). This approach makes

the continual authentication as a special case of the risk adapted authentication, and thus integrates the two without any burden on the users.

3. The approach is more user-friendly because the CCIM smarts work transparently to the user.

4. CCIM significantly enhances confidence in authentication decisions because they incorporate the enterprise operational policies and their business intent in qualitative and quantitative ways.

5. The enhanced confidence in authentication decisions applies to all DoD operations, including those involving coalition and international partners. This is because separate CCIM authentication policies can be used for different classes of users, like US nationals in USA, US nationals abroad, NATO partners, Coalition partners, and international partners, etc.

6. The CCIM details are not embedded in user's smartcard or in mobile device. The corresponding risk due to theft or loss is, therefore, mitigated.

7. The CCIM information is contained in a server that acts as authentication policy execution point (PEP) which is logically centralized but can be implemented in a distributed mode. There can be multiple PEPs devised for different classes of users and different security classifications to enforce broad based authentication policies. Multiple PEPs can also provide scaling, performance, backup and redundancy.

8. Multiple PEPs enable scaling with respect to increasing number of users, increasing types of parameters in CCIM context policies, and increasing number and types of policies.

9. The technologies used to implement the CCIM are standard based to facilitate interoperability.

10. The information for the CCIM technology can be updated in the server without the involvement of the user, his smartcard, or his device. For example, the CCIM can be updated if the user is reassigned, relocated, or if his card or device are lost or stolen. This can often be done just by editing few CCIM policy attributes that correspondingly represent the user in the server.

11. The use of a policy driven approach brings significant additional advantages. For example, the behavior of the authentication application can be modified without changing the application software or even the policy management software. Rather, it can be done by editing a few policy parameters in the appropriate authentication policy, or by activating modified or new policies. Other advantages include (i) automation, (ii) operational flexibility, (iii) responsiveness to the situational changes in near-real-time, (iv) evolution of the authentication capabilities with the changing requirements and operational scenarios, and (v) cost savings due to the above factors.

12. The CCIM technology is non-intrusive in the sense that very little needs to change in the current authentication applications, namely only policy enablement is required. The technology is an overlay for the existing authentication schemes. This allows CCIM implementation for most commercially available platforms and networks.

13. CCIM technology applies to the mobile as well as the wired networks.

14. CCIM technology reduces the reliance on passwords.

15. The detailed workings of the policy management environment are decoupled from the authentication application. Therefore, the CCIM policy environment can evolve by introducing modified or new policies, without impacting the existing application.

16. The CCIM technology has adequate set of capabilities with a wide applicability scope such that it integrates the three traditionally separate areas, namely authentication, authorization, and access control.

One might wonder as to any issues in the CCIM technology. Since the technology uses PBM, which is well researched at the Internet Engineering Task Force (IETF), it is founded on International Standard and well investigated specifications. IETF has mitigated common issues like performance, scaling, security, management, and data structures, sizes, storage and retrieval. The prototype implementation did bear out these expectations. However, when the technology is deployed on an operational scale, some issues are likely to emerge based on the deployment topology and operational experience. More research is needed on these topics.

Discussion

The CCIM technology presented in this paper is unique in the sense that nothing exists in the current security technology space that offers the functional capabilities that it provides. It is disruptive in the sense that it puts the cyber defenders in the driving seat, unlike the current situation in which the attackers hold the initiative. It is also disruptive in the sense that it potentially can replace three existing but separate technologies, namely authentication, authorization, and access control.

Features like continued authentication are made much more sophisticated and affective; for example, by observing the usage behavior of the authenticated user, and disrupting the activity, like that of Edward Snowden, if and when the background monitoring system raises the corresponding flag. In this regard, the technology produces results akin to those in artificial intelligence, without, however, the undesirable consequences of the use of poorly understood techniques like the machine learning.

The CCIM technology provides capabilities over and above the best that is currently available. All enterprises that are vulnerable to cyber-attacks should seriously consider deploying it. It is an absolute necessity for big government departments like the Department of Defense (DoD): it is so for two main reasons; the technology was developed specifically under advisory from DoD, and it includes functionalities and future potential that DoD definitely requires but cannot find elsewhere.

The technology is at a prototype stage. Testing at deployment stage and operational stage can reveal issues. Therefore, more research and development are needed. Further, the technology should be tested in a larger scope. A big difficulty is regarding the needed budget, and this is where investors or grants have a role.

Conclusion

In this paper we have defined a new authentication paradigm that uses a new concept to generalize the traditional user id into rich mechanisms to calculate a Computable Compound Identity Measure (CCIM). The password too is generalized into a multi-level password scheme. The paper elaborates the definition and numerical computation for the CCIM. Conceptual architecture for the new technology is presented.

It is demonstrated how the CCIM scheme operates as an overlay technology for the existing authentication schemes; and how it can be implemented for most platforms and networks. It is shown how the existing authentication application can be policy enabled through the incorporation of a Policy Enforcement Point (PEP) which process uses an approach akin to Network Functions Virtualization (NFV). The new paradigm qualitatively and quantitatively represents variables to incorporate common operating picture, situation awareness, and overarching operational considerations in accord with the business-intent of the enterprise. The new technology offers a number of significant advantages over the best of existing technologies which do not provide the above-mentioned functionalities.

The new technology based upon the CCIM unifies three separate technologies, namely authentication, authorization, and access control. The three technologies are seamlessly integrated, eliminating the boundaries between them, and removing the gaps in the operational security that arise due to these boundaries.

References

Basile, C., Valenza, F., Lioy, A., Lopez, D. R., and Perales, A. P., "Adding Support for Automatic Enforcement of Security Policies in NFV Networks", IEEE/ACM Transactions on Networking, vol. 27, no. 2, pp. 707-720, April 2019, doi: 10.1109/TNET.2019.2895278.

Camp, J. L., "Digital identity", IEEE Technology and Society Magazine, vol. 23, no. 3, pp. 34-41, Fall 2004, doi: 10.1109/MTAS.2004.1337889.

Choudhary, A. R. (2008, November). Network management in net-centric systems. In MILCOM 2008-2008 IEEE Military Communications Conference (pp. 1-7). IEEE.

Choudhary, R. (2005, June). A policy-based architecture for NSA RAdAC model. In Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop (pp. 294-301). IEEE.

Choudhary. (2006, June). Compound identity measure: a new concept for information assurance. In 2006 IEEE Information Assurance Workshop (pp. 148-154). IEEE.

Choudhary, A. R. (2022). Business-intent-based IT management. Issues in Information Systems, 23(4), 317-327.

ETSI, “ETSI ISG NFV: Work Program and Releases Overview”, January, 2021.

Kandala, S., Sandhu, R., & Bhamidipati, V. (2011, August). An attribute-based framework for risk-adaptive access control models. In 2011 Sixth International Conference on Availability, Reliability and Security (pp. 236-241). IEEE.

Leedom, Dennis K., “Functional Analysis of the Next Generation Operating Picture”, 8th International Command and Control Symposium, National Defense University, Washington, DC, June 17-19, 2003.

Liu, W., Bi J., "Policy-Based Management Framework for the Simplified Use of Policy Abstractions (SUPA". RFC 8328, 2018.

Walker, J., & Kulkarni, A. (2005). Common open policy service (COPS) over transport layer security (TLS) (No. rfc4261).

Wu, Q., Bryskin, I., Birkholz, H., Liu, X., Claise, B., "A YANG Data model for ECA Policy Management" Internet Draft draft-ietf-netmod-eca-policy-01, August 2021.