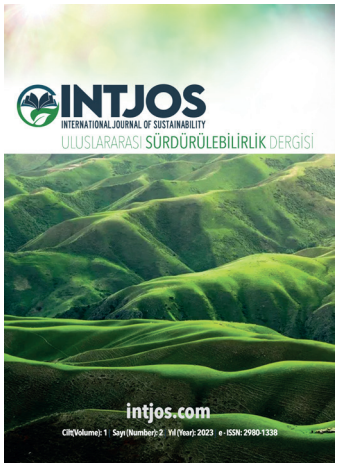

INTERNATIONAL JOURNAL OF SUSTAINABILITY
DOI: https://doi.org/10.5281/zenodo.8380593
INTJOS 2023; 1 (2) : 289 - 301

The Post-Implementation Effects of Aan Identity Management Platform on Risk and Regulatory Compliance

Risk ve Mevzuata Uyum Üzerindeki Bir Kimlik Yönetimi Platformunun Uygulama Sonrasi Etkileri

- Wayne A. SZOT
  Dept. of Computer Science,
  Sam Houston State University, Huntsville, TX, USA
  was012@shsu.edu

- Yeşim ÜLGEN SÖNMEZ
  Dept. of Software Engineering, Faculty of Technology,
  Fırat University, Elazığ, Türkiye
  phdyus@gmail.com

ABSTRACT

Why should a company focus on Identity Management? The risks of not doing so are great and many compa-nies do not realize the amount of benefit that can be achieved from doing do. This study attempts to quantity and measure how much benefit can be had by committing to a proper Identity Management platform and solu-tion to give confidence and arm the Information Security department with data to present when it comes time for funding decisions.

Kaynak gösterimi için:
WAYNE A. S. & ÜLGEN SÖNMEZ Y. (2023). The Post-Implementation Effects of an Identity Management Platform on Risk and Regulatory Compliance; International Journal of Sustainability -INTJOS, c.1 **s.2 ISSN: 2980-1338**

Keywords: Audit, Identity Management, RBAC (Role Based Identity Management) Risk, SOX

ÖZET

Bir şirket neden Kimlik Yönetimine odaklanmalı? Bunu yapmamanın riskleri büyüktür ve birçok şirket bunu yapmaktan elde edilebilecek fayda miktarının farkında değildir. Bu çalışma, güven vermek ve Bilgi Güvenliği departmanını finansman kararları zamanı geldiğinde sunacak verilerle donatmak için uygun bir Kimlik Yöne-timi platformu ve çözümü taahhüd ederek ne kadar fayda sağlanabileceğini ölçmeye ve desteklemeye çalışmak-tadır.

Anahtar Kelimeler: Denetim, Kimlik Yönetimi, RBAC (Rol Tabanlı Kimlik Yönetimi) Risk, SOX

INTRODUCTION

The Information Security world has paid a lot of attention to securing networks and avoiding malware, as it should, but relatively little has been mentioned about managing user access which is arguably just as (if not more) important than the aforementioned areas. Improperly managed access that is not kept up-to-date and adheres to the concept of least privilege leaves attackers a very broad and easily accessible attack surface. It would do organizations good to invest in and pay attention to the area of identity management for risk reduc-tion and regulatory compliance. In the time since SOX was passed, many items have been added to the check-list for compliance that have to do with user access to systems and making sure that companies pay regular attention to re-certifying access and removing unneeded access to keep the environment as clean as possible. Users should only have the least amount of access needed to perform their job duties and nothing else, super-fluous access leaves areas for attackers to gain a foothold in the environment and ultimately escalate their ac-cess so they can perform progressively more damaging attacks putting the data and reputation of the company at risk.

This study will focus on the benefits that can be achieved by focusing on implementing a properly planned identity management system with proper controls surrounding it to assist and automate many of the functions needed for proper identity management. The risk and audit perspectives will be considered when designing the proper items around IDM and the controls that will be needed to maintain the environment going forward to ensure risk does not creep back in over time after the solution has been implemented. Once identity manage-ment is under control, many other areas in Information Security will also benefit, such as the number of vul-nerabilities, needing remediation will be reduced and the resources needed to chase these down will be freed

up to study on other areas of importance.

Acronyms used in this study

- IAM/IDM – Identity and Access Management
- SOX – Sarbannes-Oxley Act of 2002
- SAML – Security Assertion Markup Language
- RFID – Radio Frequency Identity
- IoT – Internet of Things
- FIM – Federated Identity Model
- RBAC – Role-Based Identity Management

1. LITERATURE STUDY AND BACKGROUND

1.1. A Privacy-Preserving Approach for Identity Management as a Service

In this study, Nunez and Agudo outline a model for Identity as A Service (IDaaS) that preserves privacy and data protection. Their model is named 'BlindIdM' which complies with the IDaaS model and complies with data privacy laws and regulations (Nuñez & Agudo, 2014). Recognizing the importance of trust in the cloud provider and the security of their IDaaS services, the BlindIdM service will allow the cloud provider to supply identity services without knowing the information of the users in a blind fashion. This is opposed to current situations where the user must trust the cloud provider with their data and that the provider makes proper decisions and security methods around that data. Utilizing this blind privacy model allows the BlindIdM service to naturally comply with the privacy laws of several countries with no additional measures needing to be taken. Reduction in liability is also naturally the result of this blind approach, keeping in mind that the cloud provider does not hold the decryption keys they cannot be held liable for breaches that would necessitate the decryption of the user's data.

The BlindIdM model consists of the following technical elements and stages:

- Generation of public and private keys
- Encryption of identity information and outsourcing
- Trust establishment and generation of re-encryption keys
- Identity information interaction by the user (how does the user retrieve their data?)

While the authors do a good job of outlining a new technical solution to a defined problem, there is not much data analysis to back up their claims. Implementation of such a proposal would take time and cost a lot of money in resources and capital outlay, but in reading the study I would not be confident from the outset that my investment would be worth it. The authors should have prepared a case study (or two) with data before and after implementation to indicate whether there would be any benefit, and if so, how much?

1.2. Data minimization in communication protocols: a formal analysis framework and application to identity management

Veeningen et al. propose a framework that compares communication protocols in the identity management world with an eye to data minimization as a venue to protect privacy (Veeningen, Weger & Zannone, 2014). Outlined are protocols that use cryptographic primitives that ensure participants learn as little as possible and cannot correlate information from different sources. Many different applications have been cited to which this study would apply including electronic toll collection, e-voting, and RFID systems. The framework defined here gives precise, verifiable results that obtains insight into privacy differences between the protocols and applications. Four identity management systems are presented for analysis and comparison to determine a range of relevant privacy requirements. Two assumptions are relied upon for this formal model to function correctly:

- Discrete information – there are a finite number of data points for each data subject that can be analyzed on a Boolean level.
- Discrete knowledge – subjects themselves may or may not be able to learn the pieces of information that are attributed to them, but uncertainty in this situation is not allowed.

Analysis of a Personal Information model is analyzed such that all personal information present in the system at any point in time can be described. PI information is a specific string that holds specific meaning about a person and can be distinguished between identifiers and data items. Identifiers are unique keys that index to the data items to ensure uniqueness. Actors within the system only have partial knowledge about the totality of personal information within that system. The model assures that each actor only has knowledge of their own space and cannot induce or deduce any information about any other actor. In addition, the model analyzes the messages that are exchanged between actors to determine if any additional personal information is obtained via this method. Session keys, nonces, and any non-personal data that can be collected to deduce personal data is modelled and prevention proposed. The model then goes on to define the states the knowledge is bundled into and traces each bundle back to a point in time and an analysis can begin on how that state was constructed.

The study then examines a case study of an online service provider and the Identity Management system they use. The parts of the IdM that comply with the model are identified and analyzed, and the parts that do not comply are broken down as to the reason for non-compliance, however like the last study there is not a lot of real-world data to compare. The authors do give a case study, but this study is not broken down into Key Performance Indicators that would indicate any improvements over non-implementation of the framework.

1.3. Identity Management System Model in the Internet of Things

Athamena and Houhamdi have composed a study that defines many concepts and words associated with the Identity Management sphere as it pertains to the Internet of Things and guides

newer users to a level of understanding needed to approach many of the topics (Athamena & Houhamdi, 2020) This is an important topic as defined Identity Management systems in the IoT world is largely non-existent and is one of the reasons for the great concerns of IoT security and an area that desperately needs visiting. Several different components of IdMS systems as they relate to IoT devices are considered, including DNS, Cooltown, SAML, OAuth, OpenID Connect, oneM2M, MAGNET, MANETs for healthcare applications, and identity management in M2M networks. According to the authors:

Considering the technical and personal requirements and expectations of the end-users, there are two major user requirements influencing the STSO:

- End-users: They are part of the IoT ecosystem (it is a set of devices connected by networks that communicate with other devices, services, applications and people). Thus, their role is to inform their requirements, provide feedback and control the operators separately. The integrated IdMS should personalize the users' profile and accordingly provide a set of services.
- Continuous receptive services: The system should fulfill and support the users' requirements independently of location and time. The IdMS aims to provide continuous receptive services, depending on a particular user's environment and running time, by defining communication mechanisms between things in IoT.

While this study provides an essential service; the ground-level definitions needed to understand the problem and begin crafting solutions, that is precisely the work's weakness. It does not go into great depth into any one subject and cannot be used as an implementation manual or a set of best practices when considering solutions in your own environment. Further work needs to be performed in this field such that it can be a more useful guide to the Information Security practitioner in the field hoping to secure their environments.

1.4. Identity management using SAML for mobile clients and Internet of Things

Sobh summarizes in this study a new scaled-down version of SAML that can work in the environment of mobile client and IoT devices within a cloud context (Sobh, 2019). This version of SAML is easier to use and easier to parse since both mobile and IoT devices are smaller and require lighter-weight protocols due to their limited resources. This version of SAML uses JSON to reduce the SAML footprint by 28.99% and will present a way to bring these devices in to an IDM environment where they previously might not have been able to, thus increasing security.

Previous versions of SAML using XML are shown to have performance problems due to:

- Redundant syntax: escalating the high costs of applications due to additional resource usage.
- Parsing algorithms are too complex: good XML parsers must be streamlined to process

data subjectively settled and implement extra tests to detect syntax errors and invalid data formats.

- XML takes up too much processing power: of which on mobile platforms and IoT devices, processing power is at a premium.
- XML requires specialized editors to properly edit keys and writing expressions.

Due to the increased concerns of privacy while in a cloud environment, it is even more necessary to ensure that the proposed SAML algorithm is not only lighter weight but maintains or even increases the amount of privacy protection while utilizing mobile and IoT devices in the cloud infrastructure. This study focuses on JSON as an aspect of SAML instead of XML that will speed up request generation and reduce processing power. JSON will not scale as well as XML, however in a mobile and IoT device environment this is less of a concern due to the lighter weight nature of the devices.

While this study does a good job at focusing on the mobile and IoT worlds and indeed proposing solutions that will further the security paradigm for devices that are notoriously bad at security, it only focuses on the use of JSON in a SAML context and does not provide alternative lightweight solutions. While Java is indeed platform independent and widely adopted, it is by no means the only solution out there and there are times when Java will not work. Additional protocols could have been presented as backup options in the event JSON is not appropriate for certain situations and these secondary protocols could have been presented with strengths and weaknesses compared to JSON.

1.5. Definition of an advanced identity management infrastructure

Tormo, et al. propose an identity management solution based on SAML, XACML, and XKMS standards to provide finer user access control for administrators and greater privacy benefits for users. Included in the study are performance figures to flush out the feasibility of the model they propose (Tormo, López Millán & Pérez, 2012). The architecture of their model is named MISTRAL and is where an end user interacts with the Service Provider/Identity Provider, but the end-user is abstracted from the functionality of the algorithm. An Attribute Provider is also introduced such that the Identity Provider only needs to oversee the authentication process while the Attribute Provider serves user attributes and controls access to them. SAML 2.0 is used for communication between all the parts of the model by requesting and responding to authentication requests, attributes and authorization decision statements. The SAML messages are digitally signed by the message issuer to verify the integrity of the message in the event it is intercepted. The Public Key Infrastructure controls the trust relationships between all the components binding different organizations and domains into one security domain.

The MISTRAL framework depends on several databases as back-end stores to hold various groups of data involved in the running of the whole identity management system to keep things more efficient. The databases consist of:

- Authentication Database – maintains all pieces of information needed to carry out user

authentication including usernames, encrypted passwords and digital certificates.

- User Attribute Database – this database stores all the roles assigned, departmental information about a user, user personal data such as address and other such pieces of information belonging to a user.
- Attribute Release Policies Database – contains policies from each Attribute Provider that indicates which end-user attributes can be transferred to a requestor.
- Attribute Delegation Policies Database – maintains XACML policies permitting authorized end-users the ability to create new policies to delegate attributes to others.

This study struggles to define its audience in that a person who would want to implement this solution does not have enough real-world data to base a decision to implement on. What makes this framework any better than what the company already has and what would make it worth the time and effort it would take to implement. If the audience is intended for purely academic readers, the study struggles to give enough technical details upon which a proper critique can be built.

1.6. Inside the Identity Management Game

Lynch has focused on the evolution of authentication and authorization as it applies to current situations in online life such as social media, cloud-based services, and mobile platforms (Lynch, 2011). The current situation in identity management is compared to the past authentication schemes with local usernames and passwords and how that situation has changed, and new tools are needed such as single sign on, SAML, SOAP and AD Federation. SAML 1.0 was the early attempt at a federated identity management protocol that incorporated complex authorization patterns with data spread across multiple domains. Subsequent versions on SAML added features and functionality to extend its usefulness to a broader set of companies and situations. Today SAML serves education, government, and corporate interests and indeed is imbedded throughout much of the internet giving an environment of additional robustness in user authentication while at the same time making the user experience easier. Given this, however, SAML has not solved all authorization issues and additional tools are needed to accomplish these tasks. OpenID came during the Web 2.0 boom and social media to give users the flexibility to be identified across numerous different sites, much like SSO does in a single heterogenous environment, OpenID did the same among several disjointed sites giving a more seamless (yet secure) experience. In addition, OAuth extended the functionality of OpenID to give users the ability to delegate access to APIs acting on their behalf for a more automated experience.

While Lynch's study is valuable, it does not address the issues of authentication going forward. A look back at history does have its value, but the future is not addressed here. Perhaps a refresh of the article with an eye to the future would be in order.

1.7. A Smart Biometric Identity Management Framework for Personalised IoT and Cloud Computing-Based Healthcare Services

Farid, et al. propose an identity management framework for the Internet of Things and Cloud

Device space (Farid et al., 2021). IoT devices have historically suffered from a lack of security due to the remote and portable nature of the device. To be able to add a layer of identity management to IoT devices would help immensely in the securing of such devices. Biometric means are proposed as a measure of adding authentication to devices that would offer significant improvements where a user/password model would be difficult to implement. The study presents a healthcare scenario that utilizes IoT devices and proposes a framework including the following components:

- Gateway Layer
- Data Acquisition/Device Layer
- Cloud-Based Storage, Computations, Security, and Access Control
- Cloud API
- A multitude of different healthcare applications such as: Laboratories, Healthcare Professionals, and Outpatient Care

Within these different pieces and scenarios, the cryptography is worked out such that biometric traits and health data are kept of the utmost confidentiality. Functions are defined that outline all the different scenarios and how they may be imbedded within the IoT device.

While this study is a great resource for IDM applications, it is very narrowly focused and struggles to provide guidance to wider IDM applications. Pieces of this study can be gleaned for use in other applications, but the study as a whole only applies to the narrowly defined topic.

1.8. A User Identity Management System for Cybercrime Control

Alese, et al. propose a system of identity management that focuses on relieving the user from password fatigue and at the same time increasing their security (Alese et al., 2021). This article focuses heavily on the use of biometrics to this reduction in reliance on password centric methods and explores many different algorithms of analysing facial images. The IDM system is broken down into the following parts: Service Provider, Identity Provider (with sub-phases of Registration Phase, Identification/Authentication Phase, Authorization Phase and De-Registration Phase).

For the facial recognition piece of the framework, the first step is training the different algorithms to recognize the facial patterns correctly. An initial dataset with images of the user needs to be built to initiate this training phase, of which a primary key of the user is attached to these images to keep them in order. The LBP operation breaks down the indexed images into 3x3 pixel chunks as a reference and chains these histograms together. The paper goes on to explain how the histograms of the indexed images are compared to the histograms of the authentication images to produce reliable comparisons keeping in mind that the index images and authentication images are most likely taken under different backgrounds and lighting situations that would normally make comparison difficult.

While facial recognition has proven to be a useful tool in the identity management tool chest, it has been shown to be easily circumvented through various means and should not be heavily

relied upon for robust security. This study adds to that tool chest, but the fear is that it may present facial recognition in too positive of a light such that some readers might come to rely too heavily on it and foster a false sense of security and not implement other controls to build a defense in depth strategy.

1.9. A modelling approach to federated identity and access management

Gaedke et al, focuses on creating an IAM system that will focus on federated defined profiles and the use of Security Assertion Mark-up Language (SAML) to identify and authenticate users across heterogeneous environments and applications and even different companies (Gaedke et al., 2005). The authors use these concepts to create a template that can be conceptually used when architecting an IAM solution that will be both robust and easy to integrate.

The Federated Identity Model (FIM) is an extendable modelling framework based on UML class diagrams that focuses on being platform agnostic and able to be implemented smoothly in a heterogeneous environment. The FIM also uses security token services that are passed from one service to another to create a security chain of identity to trusted entities. A block catalogue is built of different components such as Single Sign On, Self-Service Identity Management and Identity Federation of Enterprises. The Identity Federation System is the glue that holds all these pieces together into a workable framework.

This study is far too short to provide sufficient detail for any of the concepts it raises. In reading it, it is doubtful that many new concepts have been presented and even if so, the detail is far too abstract to be of any practical use. The question is, who is the audience of this paper? Those working in the identity management sphere within a company would not find is useful for any type of planning or implementation due to the limited scope presented here. Readers from academic backgrounds would find it of limited use as well due to the lack of detail and applicability of the protocols mentioned.

2. PROPOSED RESEARCH AND CONTRIBUTIONS

Companies must keep on top of their identity management to not only keep attacks at bay, but also to comply with regulatory requirements set out by congress and other governing bodies within the economy. This project will focus on a financial sector company that specializes in issuing and servicing mortgage loans. This company has put an emphasis on putting stringent controls around its user access to comply with SOX audits and enquiries as well as to protect its reputation from public data breaches. Before implementation, data providers and auditors struggled to gather and test data due to the manual nature of the performance of the controls. Spreadsheets with tens of thousands of people and untold entitlements assigned to these people were common, as well manual controls leave open lots of room for human error and incompleteness of the data. Users will also benefit from a more defined process to request access with clearly defined job flows and

approval chains. Previously, the company had a very ad-hoc provisioning system that often would involve different groups for different applications and even different processes for each of these groups, leaving the user to guess as to how to request access and often times the requests would get dropped because there was no defined job flow to see the request through to the end. To add to this confusion was the situation where access was mirrored since the managers did not know which permissions granted the desired access needed, thus users would often be granted all the access another similar user had leaving a problem since least privilege was not followed in this situation. In addition, users who had been with the company for a long time and have changed roles would gain new access without reviewing or removing the old access.

Scoped within this study are 5 of the most critical applications the company hosts that are both business critical and in-scope for SOX compliance audits. 600 users access these 5 applications, and many users have access to multiple applications depending on their job functions. As a measure of risk, the company was issued an average of 15 findings by audit, 3 of which were labelled significant deficiencies. These are areas audit found to be of great concern and posed a great risk to the company and its investors. The measure of audit results after IAM implementation will be a key indicator of the implementation's success or not. The number of findings change from year to year as issues get remediated and new ones are found each year, but this will be a key indicator of risk for the organization. Can controls be put into place such that the number of potential issues to be found can be reduced significantly and the resources that would have been directed toward remediation could now be directed toward other areas of improvement.

Another indicator of risk is the fact that at any one time there are about 700 orphaned permissions per month. Orphaned permissions are those that are incomplete and do not have enough information to positively identify an individual owner with a proper reporting approval chain. Orphaned permissions are an indicator of sloppy data hygiene and lack of controls around how the data is managed, without which it is impossible to determine the current access picture of the environment, much less manage it. Orphans must be manually remediated and tracked down to find an owner, and if it is impossible to find the owner the permission must be removed.

These key indicators will be taken and measured again post implementation as a way of quantifying the amount of risk that was reduced after the implementation of the control structure. The implementation will commence in 4 phases: phase 1 has already been performed in that the pre-implementation data has been gathered and noted for processing later, phase 2 will be a role definition phase in which the business units will meet with information security representatives to determine which groupings of entitlements can be gathered into roles for proper role based access management (illustrated in Figure 2.1), phase 3 will be the IAM implementation which will include the technical aspects and the application connectors from the IAM platform, and phase 4 will be a post-implementation inspection to ensure proper environment configuration and that all defined controls are properly working. Once all 4 phases have been completed, a new set of data will be gathered for comparison.

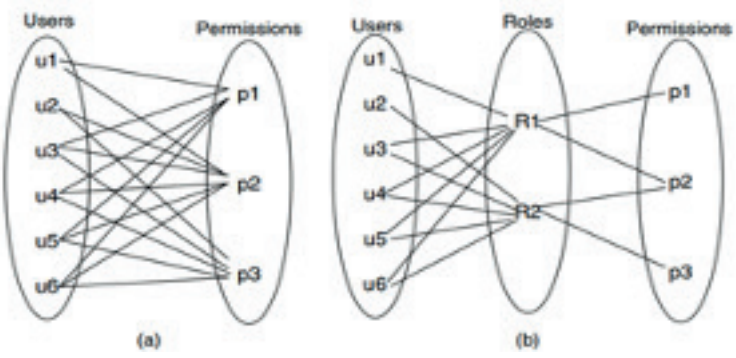

Fig. 2.1. Role Discovery and Assignment (Vaidya et al., 2008)

3. EXPERIMENTS AND RESULTS

Data gathering happened with the help of multiple teams and multiple sources such as the Data Services team that provided access and ensured the technical integrity of the data that came from each application and aggregated into the singular metrics. In addition to the applications themselves, user data also came from databases, active directory and even Azure for cloud applications.

Five different applications were chosen for this project, these applications were the most business critical and or had the biggest impact on SOX financial reporting. While there are several applications that support the environment, these five were the 'pilot' applications that would be used as a template for future projects involving the rest.

The first application is an Invoice Management ledger processing system that currently has 46 different assignable permissions, the second application is a customer support application with 73 assignable permissions, the third application is a loan origination system that has 15 assignable permissions, the fourth is a home valuation application used by the foreclosure department with 6 assignable permissions, and the fifth is a human resources application with 53 unique assignable permissions.

Phase 2 commenced with this data in hand to gather with the various stakeholders in the business that have functions in these applications to determine which roles can be defined to group these permissions into roles for easier management. After the meetings, it was decided that 26 roles can be defined that will hold all the unique assignable permissions that will ease the burden of provisioning or role transfer operations for the identity management team.

Phase 3 was the more technical of the phases including the infrastructure and network teams to get the particulars of the servers and connectivity installed and configured such that the identity management software and environment can run and communicate to all the different applications and environments needed for synchronization of user data. After the completion of phase 3, the automation of many of the identity management functions could commence such as provisioning

and de-provisioning (reducing risk that the immediate moment a user is marked as terminated their access is immediately and automatically removed, not needing to wait for a human to process the request).

Phase 4 pulled in both internal and external audit to review the designs and results of implementation for control effectiveness. Of key importance is to make sure there are no ways to bypass the controls (such as being able to create new permissions on the systems, thus nullifying the role definition process) and undermine the integrity of the system going forward. In addition, tickets were reviewed to ensure that the approval job flow process is followed without exception, it would be catastrophic to the environment if a user can circumvent the process and create their own access to do what they like thereby penetrating the wall of defense.

Conclusions and Future Work

Upon conclusion of audit's review of the implementation, it was their determination that there were many areas of improvement. Since many of the tasks of provisioning have now been automated, the average time of fulfilment of an access request decreased to a day. Most of this time is spent waiting for the various approvals needed for fulfilment. In addition, de-provisioning also has been reduced to almost instantaneous once the account had been marked for termination due to automation.

Audit findings dropped to one finding per year, and no significant deficiencies. A significant development that measures the reduction of risk realized by the environment. After this finding was remediated, the free resources realized due to not having any other findings were diverted to other more important items that needed attention. In addition, there are now only about 12 orphaned permissions that need remediating per month. With the applications being directly connecting to the identity management platform, there are far fewer opportunities for corrupted and dirty data that usually lead to orphans. While these results are indeed exciting, the same work now needs to be done for the rest of the applications defining future work for this study. Once the rest of the applications have been brought in, and the procedures followed here are documented and reviewed these procedures can be used in future studies to benefit other environments and the identity management sphere in general.

Acknowledgment

The authors of this paper extend their appreciation to Dr. Cihan Varol for his contribution.

REFERENCES

Alese, T. Owolafe, O. Thompson, A. F. & Alese, B. K. (2021), A User Identity Management System for Cybercrime Control, Nigerian Journal of Technology, 40: (1), 129–139, doi: 10.4314/njt.v40i1.17.

Athamena, B. & Houhamdi, Z. (2020), Identity Management System Model in the Internet of Things, TEM Journal, 1338–1347, doi: 10.18421/tem94-04.

Dólera Tormo, G. López Millán, G. & Martínez Pérez, G. (2012), Definition of an advanced identity management infrastructure, International Journal of Information Security, 12: (3), 173–200, doi:10.1007/s10207-012-0189-y.

Farid, F. Elkhodr, M. Sabrina, F. Ahamed, F.& Gide, E. (2021), A Smart Biometric Identity Management Framework for Personalised IoT and Cloud Computing-Based Healthcare Services, Sensors, 21: (2), 552, doi: 10.3390/s21020552.

Gaedke, M. Meinecke, J. & Nussbaumer, M. (2005), A Modeling Approach to Federated Identity and Access

Management, ACM, 1–59593051-5/05/0005, 1156–1157.

Lynch, L. (2011), Inside the Identity Management Game, IEEE Internet Computing, 15: (5), 78–82, doi: 10.1109/mic.2011.119.

Nuñez, D. & Agudo, I. (2014), BlindIdM: A privacy-preserving approach for identity management as a service, International Journal of Information Security, 13: (2), 199–215, doi: 10.1007/s10207-014-0230-4.

Sobh, T. S. (2019), Identity management using SAML for mobile clients and Internet of Things, Journal of High Speed Networks, 25:(1), 101–126, doi: 10.3233/jhs-190606.

Vaidya, J. Atluri, V. Guo, Q. & Adam, N. (2008) Migrating to optimal RBAC with minimal perturbation, Proceedings of the 13th ACM Symposium on Access Control Models and Technologies - SACMAT 08. doi:10.1145/1377836.1377839.

Veeningen, M. Weger, B. & Zannone, N. (2014), Data minimisation in communication protocols: a formal analysis framework and application to identity management, International Journal of Information Security, 13: (6), 529–569, doi: 10.1007/s10207-014-0235-z.