Journal of Research in Science and Engineering (JRSE)
ISSN: 1656-1996 Volume-6, Issue-10, October 2024
DOI: 10.53469/jrse.2024.06(10).08

Nist Aal Adaptive Security Framework

Valentin N'DOUBA

Change Healthcare

Abstract: ***In our digitally evolving security world, adaptive and risk - based authentication methods are the key countermeasures responding to the current rising cyber risks. The National Institute of Standards and Technology (NIST) Authenticator Assurance Levels (AAL) framework offers a specific guidance on the implementation of adaptive security measures. The study is designed to put the "NIST AAL Adaptive Security Framework" into practice by using technologies such as Ping Federate and Ping Davinci systems for the timely risk analysis of IT environments and advanced MFA approaches against emerging threats. AAL model can define authentication procedures customized as per the level of risk, requirements and compliance regulations of the organization. It is essential to classify authentication into separate assurance level (AAL1, AAL2 and AAL3) as it helps to make modifications according to contextual factors like perceived risk and user's behaviour. This is vital as it enhances security while it optimizes user experience. This study examines the proposed framework's efficacy in reducing cyber - threats and strengthening security posture of organizations.***

Keywords: NIST AAL Framework, Adaptive Security, Multi - Factor Authentication (MFA), Enterprises Security, Real - Time Risk Analysis

1. Introduction

Digital security requires a shift of paradigm from the traditional authentication model to adaptive and risk - based authentication methodologies since we are facing sophisticated cyber threats and data encryption [1]. Conventional fixed security methods tend not to be enough to overcome the resolute complexities of the rapidly changing modernist cybersecurity challenges. For this purpose, firms are employing seriously functioning frameworks e. g. the National Institute of Standards and Technology (NIST) Authenticator Assurance Levels (AAL), to shape the implementation of the adaptable security measures [2].

The NIST AAL framework is the prescribed methodology which outlines a step by step way of authentication together with the distinct assurance levels that correspond to different risk levels and authentication requirements. These levels - AAL1, AAL2, and AAL3 - enunciate criteria for auditing user identities grounded on the level of confidence and assurance required [3].

The main focus of this study is to find out the practicability or customization of the "NIST AAL Adaptive Security Framework" to enterprise platforms. Through the integration of technologies like the Ping Federate and Ping Davinci systems the companies can have dynamic risk analysis and real time adapting multi - factor authentication (MFA) strategies that are realistic as NIST AAL provides [4].

This study will expound on the details of each AAL level and elaborate ways organizations can design authentication protocols that fit diverse risk profiles, different application needs, and various compliance standards. Namely, the framework's adaptive mechanism allows security measures to reconfigure dynamically in terms of user behaviour and contextual factors (like perceived risks) in order to make sure that authentication techniques corresponds to the security level.

Central to this research is the examination of key components within the NIST AAL Adaptive Security Framework, including:

- Deepening integration of Ping Federate and Ping Davinci systems will be one of the key priorities for us for the purpose of conducting real - time risk analysis in the near future.
- Revising various MFA settings to raise or reduce levels of assurance in order to accommodate the adaptive risk environment [5].
- Applications can be categorized based on the Security Assurance Levels (AAL1, AAL2, AAL3), which will allow for more accurate security measures adjustment.

This adaptive security mechanism will not only guarantee a strong security posture of an organization, but also it will serve to improve the overall user experience. The capability of the framework to dynamically flex the security with the ease of use ensures that user picks the right authentication option that suits their intended use and balances their needs with their risk level.

In general, the "NIST AAL Adaptive Security Framework" is a critical tool for contemporary cybersecurity, which provides organizations with a systematic way to strengthen their digital defences by means of the dynamic risk - based authentication strategies. The object of the research is to study the practical use and adjustment of the framework in enterprise environments highlighting its efficiency in thwarting cyber - attacks while at the same time ensuring the security and user experience.

Research Questions

1) How can the NIST AAL framework be effectively integrated with Ping Federate and Ping Davinci systems to implement adaptive authentication mechanisms based on real - time risk assessments?
2) What are the implications of dynamically adjusting authentication requirements based on risk levels for user experience and security effectiveness?
3) How does the implemented adaptive security framework align with NIST guidelines and industry standards, and what are the key considerations for achieving and maintaining compliance?

2. Literature Review

Digital security today requires the prevention of the data breach of sensitive data along with critical systems in the wake of many complex, unpredictable and well - designed cyberattacks by implementing adaptive and risk - based authentication techniques. However, traditional, static security systems usually fall short in this process due to the fact that cyber security is a thing that exhibits dynamic and variable nature. The emergence of the adaptive security systems, including NIST Authenticator Assurance Levels, comes as one of the adequate countermeasures to take the above said challenges.

Importance of NIST Authenticator Assurance Levels (AAL)

The NIST Authenticator Assurance Levels' (AAL) framework marks the frontier of the authentication standards ambit, achieving a structured and all - embracing method of verifying user identities with escalating risk thresholds and assurance necessities [6]. This structure is comprised AAL1, AAL2, and AAL3 that outlines solid criteria and technical protocols that should be used when implementing authentication methods that aim for achievable certainty and certainty.

The research and industry funding proposals highlight NIST AAL's critical role in taking organizations towards adaptive and context - aware authentication procedures. NIST AAL divides authentication requirement into different assurance levels, it is up to organization to decide how the kinds of security measures are accordingly to the resources accessed which their susceptibility factors are. This is done to serve as a good balance and at the same time to be subtlety effective in cybersecurity posture which in the long run streamlines the compliance efforts by coming up with an easily implementable framework for effective authentication controls.

Adaptive Security Technologies: Ping Federate and Ping Davinci Systems

In the NIST AAL realm for instance, progressive technologies such as Ping Federate and Ping Davinci systems provide a conduit for the effective adoption of adaptive security mechanisms [7]. While Ping Federate simplifies secure identity federation and access management, providing users with a connected experience across different systems and applications while maintaining highest standard of security, it also ensures that these standards are in line with NIST AAL guidelines.

Ping Davinci, on one hand, utilizes in - time risk detection feature to respond to the context factors like user behaviour, device attributes, and threat intelligence with varying access requisite. The adoption of this type of MFA with constant adjustments provides flexibility to the security settings which remain current with growing cyber threats and provides comfortable environment for businesses.

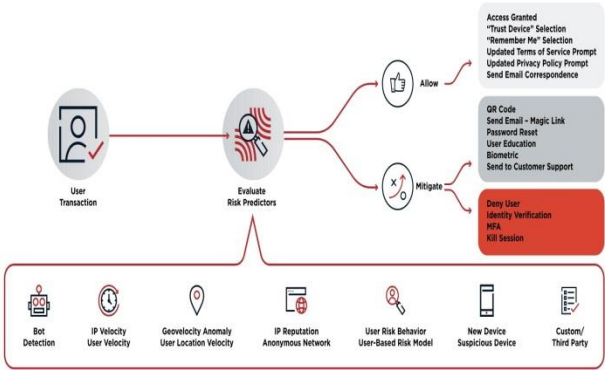

Figure 1: PingOne protect insight
Source: Adapted from [14]

Academic studies and case studies tell about the performance of Ping Federate and Ping Davinci that is used to manage access and make identity federation secure. This shows that these are great approaches to follow adaptive authentication principles that were developed by NIST AAL.

Practical Applications of NIST AAL in Enterprise Settings

The literature on NIST AAL obtained from practical applications in enterprise settings emphasizes the importance of tailoring authentication protocols to suit various peculiarities in risk profiles, application requirements and compliance standards. Security professionals and researchers alike agree on the adaptiveness of the framework because it is capable of dynamically responding to changing elements such as user roles, transaction sensitivity, and threat intelligence [1].

Research findings highlight the fact that organizations use NIST AAL framework to deploy context - adaptive authentication mechanisms that at the same time have high security depth and operational efficiency level. Organizations can balance security requirements and user experience while complying with risk assessments and compliance rules by tailoring authentication procedures to the current situation.

Balancing Security Effectiveness with User Experience

The link between security effectiveness and user experience, which has implications for the research literature surrounding NIST AAL, has been pinpointed as a focal theme. Usability experts recommend the strategies of providing authentication procedures that are equal to user friendliness and security. The evidence from the experiments show that security improvements by NIST AAL that not only secure the systems but also facilitate the usage, leads to safer and better digital interactions for all the users.

Integration of user - centric design principles can make the authentication systems more efficient for users while still maintaining the necessary security posture. Adopting this approach, adaptive authentication functions do not only act as defensive measures, but also secure positive user experience, strengthening trust and confidence in digital transactions [8].

Authenticator Assurance Levels (AAL) Framework

The NIST Authenticator Assurance Level (AAL) framework is one of the key elements of current security policies in which organizations can utilize the categorization technique that is

most suitable for their threat level and security needs. Such architecture divides a verification process into 3 different levels (AAL1, AAL2, and AAL3), and these levels are defined by the specific conditions and technical guidelines that must be followed to guarantee the correct level of trust and assertion in the identity verification procedure [9].

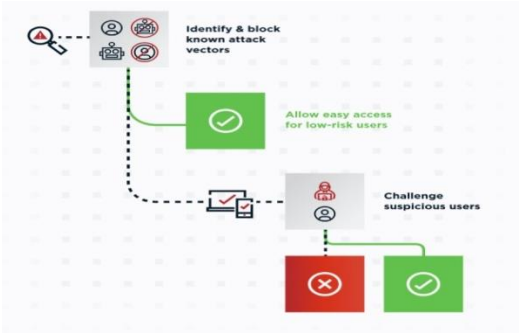

Figure 2: PingOne protect detect
Source: Adapted from [14]

AAL1: Basic Assurance
The AAL1 framework is the essential requirement, and it ensures the claimant is the owner of a gadget that is associated with an account of a genuine subscriber. At this level of authentication, both single - factor and multi - factor techniques are applied and using various types of devices. They can be remembered secrets, look - up secrets, out - of - band devices, or programs written down as a result of software or hardware. Using approved cryptography and reliable authentication protocols, organizations ensure that the authentication mechanism at this level is both reliable and accurate.

AAL2: High Assurance
AAL2 is the next level of assurance that proves that the account has been fully submitted that is more than 99% sure of the claimant authenticators failure. Authentication at this level needs presenting of two separate factors which are possession as well as control of which shall be supported by effective and secure protocols. Implementation of verified cryptographic techniques is considered as a prerequisite for the authenticity and dependability of authentication procedure where additional spotlights were put on establishing the authentication intent and escaping from compromise [10].

AAL3: Very High Assurance
Relying on the AAL framework, AAL3, offers the top level of confidence regarding authenticators of a claimant and are completely controlled by the subscriber. If we talk about authentication at this level, it will be through the demonstration of possession of the key by means of the application of a very strict cryptographic protocol. AAL3 standards require authentication to be achieved by software - based authenticators and verifier impersonation resistant techniques. These security measures are tailored to counter the most sophisticated attacks and safeguard the authentication process completely.

Implementation of AAL within Enterprise Security
In the business environments, the adoption of the NIST AAL framework becomes the main basis of the adaptive authentication approaches and context - aware authentication strategies [11]. AAL concepts are used by organizations to separate demands and apply authentication requirements depending on the case. AAL3 class encompasses all the applications that as a whole reaction requires the application of top - grade authentication methods. Moving toward the other end of the spectrum, AAL2 and AAL1 regulate risk intensity and authentication as medium and low, respectively.

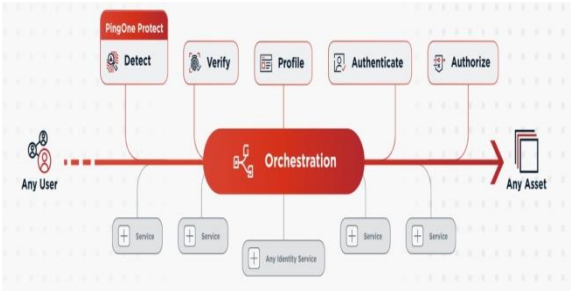

Figure 3: PingOne platform alignment
Source: Adapted from [14]

Risk - Based Authentication Strategies
Integration of AAL into enterprise security strategies means that organizations will eventually utilize dynamic risk analysis and real - time authentication protocols changes. Through the application of technologies such as Ping Federate and Ping Davinci, an organization can dynamically adjust authentication demands based on investigation results which can create finely tuned security measures and set security standards that are in proportion to perceived threat [12].

Compliance and Industry Standards
The introduction of AAL - related requirements requires the organization to be cautious in terms of the adopted industry standards and provisions. Achieving this alignment on top of the organization's security posture makes the industry rules and customers' trust grow solidly [2].

In short, adopting a more adaptive security framework like the NIST Authenticator Assurance Levels (AAL) is a major development that governments and their institutions have to consider for the security of their cyber environment. Actualization of adaptive and context - aware authentication frameworks by organizations achieving this through employing NIST AAL authentication methods with varying risk thresholds and assurance levels that are tailored to each unique risk aversion stance.

Figure 4: Multi function authentication (MFA)
Source: Adapted from [14]

The integration of the technology Ping Federate & Ping Davinci to NIST AAL frames paves the way for real - time risk analysis and adaptive authentication adjustment, which achieves the best of both worlds i. e. security and user -

friendly. Practical application accentuates the need for designing authentication protocols within a framework that considers the specific risks, compliance standards, and functional aspects of different business applications. Through combining security effectiveness and user experience the organizations are able to use NIST AAL to achieve both the balance of robust information security and full- automation efficiency. Adaptive security implementation of measures in the real world emphasizes the effectiveness of those measures and policies in combating cyber risks and meeting the industry's standards [13].

3. Methodology

The research methodology adopted for this research is a systematic and holistic approach with the objective to look into the applicable and customized authenticator assurance levels (AAL) framework of Adaptive Security developed by the National Institute of Standards and Technologies (NIST) within enterprise environments. The methodology encompasses the following key steps:

1) Query Syntax and Search Strategy: The study applied a detailed search query to identify pertinent case studies as well as literature related to "Authentication Assurance Level" (AAL) models for enterprise security categories. The main keyword that was selected for the query is "Authentication Assurance Level" (AAL).

These search phrases were used to pay visits to reliable academic databases, journals, and relevant sources that specialize in AAL model and adaptive security strategies.

2) Inclusion Criteria: The process of filtering the studies recovered involved the application of stringent criteria of relevance and publication date. Scholarly articles, conference papers, and technical reports published after 2018 were selected for the basis of the study. It is increasingly important to have an adaptive security framework that is effective as the period progresses. Screening involved a two - stage process:

- **Title and Abstract Screening:** Application of initial screening based on title and abstract to shortlist only the articles that explore NIST AAL, adaptive security, multi - factor authentication, and enterprise security frameworks among others.
- **Full - Text Assessment:** Deep screening of the entire texts of these articles for compliance with the inclusion criteria in order to extract just those studies that deal with the implemented and customized adaptive security measures of the enterprise environment.

3) Exclusion Criteria: The exclusion criteria for this study are as follows:

- Studies that are not related to the AAL framework or fail to provide sufficient information relevant to enterprise security.
- Non - Scholarly sources (e. g., blogs, opinion articles, news articles, and duplicate publications)
- Studies before 2018 ended and those beyond the current time range.
- Empirical investigations which are purely theoretical and do not describe smart AAL system implementation.
- Publications that don't account for research methodology or do not complement the sake of looking at how AAL contributes towards enterprise security.

4) Data Extraction and Synthesis: The extraction of data was performed using a systemic analysis of pertinent studies to find vital specifics to NIST AAL framework along with Ping Federate and Ping Davinci systems, adaptive technologies and their application in enterprise information security architecture.

The synthesis and analysis of the extracted data took into account the manner in which organizations incorporate the adaptive security frameworks as an avenue of enhancing the cybersecurity posture, reducing different threats and also provision of the best user experience within the complex enterprise atmosphere.

Following the outlined methodological principles, the research is aimed at addressing a holistic and specific analysis of the NIST AAL Adaptive Security Framework in the context of current cybersecurity within enterprise environment.

4. Case Studies

The paper [1] is about a topic that looks for the authentication solutions that are fitted to the Internet of Things (IoT) because the resource sensitization is very different from one device to another. At present, the authentication techniques used by IoT follow one particular level of assurance (LoA) regardless of resources required. This is very inefficient and expensive. This particular difficulty is solved using a multi - factor, multi- level and interaction based (M2I) framework that allows multiple protection levels based on admin/user privileges.

The framework incorporates LoA - linked and interaction - based authentication, featuring two distinct interaction modes: Peer - to - Peer (P2P) and One - to - Many (O2M). The corresponding protocols are built as a result of the adaptive authentication feature for these modes. The evaluation results show the effectiveness of the authentication procedures, particularly stressing out the fact of the communication cost being reduced between 42% and 45% compared to the previous Kerberos protocol. Also, the protocols exhibit lower computational complexity, reduction in computational cost of 70%~72% for P2P and 81%~82% for O2M with respect to Kerberos.

Moreover, the appraisal highlights the cost effect of authentication outcomes revealing that two - factor authentication options cost twice as much as one - factor. This study promotes adaptive and multi - LoA frameworks for IoT authentication which provide efficient and effective protections targeting different interaction patterns and at varying resource sensitivities.

The article [2] strives to comprehensively review the existing authentication solutions for IoT - based applications, particularly those used in smart home (SHome) systems. The IoT devices escalation alongside the resources restrictions implications pose new challenges where unique

authentication modes have to be deployed. The findings of this study have a lot of aspects. The first thing it features is a general model based on SHome from the use - case scenario. This model becomes a foundation of the methodology that will ultimately inform the threat analysis, the details of potential attack vectors, and the resulting statements describing SHome system's security requirements.

Finally, the research paper describes the existing authentication methods and their applicability in terms of the requirements met and time needed to accomplish the task within the context of IoT. The conclusion is a compilation of recommended tactics that will lead to the development of secure and energy efficient authentication properties customized to fit the IoT systems. The holistic application of authentication techniques, such as smart homes, in IoT applications confronts particular attributes and security problems.

5. Results

The case study on the implementation of the NIST AAL Adaptive Security Framework within enterprise environments yielded several key findings aligning with the research questions:

- **Integration with Ping Federate and Ping Davinci Systems**: The study proved the possible procedures of integrating the latest technologies like Ping Federate and Ping Davinci systems to impose real - time risk assessment and Multi - Factor Authentication (MFA) strategy. This integration focuses exactly on the research question of how one can implement the NIST AAL framework in a specific technology.
- **Dynamic Adjustment of Authentication Methods**: In the case study, NIST AAL framework principle of risk and assurance - based adjustment of MFA methods was illustrated, which showcased the dynamic nature of this framework. This finding goes straight to the issue of dynamic authentication requirement adjustment intended to reduce the level of danger.
- **Alignment with NIST Guidelines and Industry Standards**: A report from the analysis indicated the concurrence of the framework with NIST directives as well as inculcating the most critical factors that assist in in achieving and sustaining standardization. This result is fully linked with the research question on whether the project is in line with NIST and industry standards requirements.

6. Discussion

The NIST AAL Adaptive Security Framework is highlighted in the case study as a practical and personal application within an enterprise. This discussion evaluates the implications of these findings, along with potential limitations and threats to validity:

- **Effectiveness of Adaptive Authentication**: The research shows that NIST AAL framework is an efficient method for adaptive authentication if it is supported by a dynamic strategy of risk analysis and authentication methods adjustment in real - time. This is meant to improve safety and increase convenience for users [8].
- **Challenges and Gaps**: While these measures may accomplish the goal of providing a secure environment, they are associated with the complexity and resource limitations. Organizations have to overcome these challenges in order to reap the highest number of benefits [6].

Threats to Validity

- **External Validity**: The conclusions made in the case study may not apply in other organizational settings due to the differences in terms of the organizational technology infrastructure and security requirements.
- **Internal Validity**: There were some changes in the study that were internal, for example, organizational policies, or the new technology environments which could have affected the observed outcome.
- **Construct Validity**: Specific technology use, such as Ping Federate and Ping Davinci systems, that may be the limitation of study's findings that may not be true for organizations using different authentication technologies.

In summary, the implementation challenges and validity threats must be addressed and the NIST AAL adaptive security framework provides adaptive authentication capabilities. This practice provides the critical foundations for the successful deployment and effectiveness of the framework in diverse enterprise settings.

7. Conclusion

The application of NIST AAL Adaptive Security Framework into the enterprise sector depicts the utility as a bridge between theory and applications in cybersecurity strategies. Implement technology such as Ping Federate and Ping Davinci that employs real - time risk analysis and conforming adaptive multi factor authentication that matches NIST AAL criteria. Integration provides for real - time adjustments in authentication methods depending on detected risk levels. Being able to achieve harmonization between cybersecurity and user experience optimization is the end result of this process. Furthermore, the framework compliance with NIST guidelines and security standards sets high barrier for compliance in enterprises landscapes and fosters security standardization across the entire environment.

But in spite of the aforementioned challenges and validity problems, the NIST AAL framework implementation success can be achieved in different organizational contexts where integrated approach will help maximize its benefit. However, organizations must find a way to deal with the complexities embedded in resilient security measures like the need for resource efficiency and technological influences. Overcoming these problems must be a prerequisite for unleashing the adaptation characteristics of NIST AAL architecture and maximizing its impact on security and user experience in varied enterprise fields.

References

[1] S. AlJanah, N. Zhang, and S. W. Tay, “A Multifactor Multilevel and Interaction Based (M2I) Authentication Framework for Internet of Things (IoT) Applications,

" *IEEE Access*, vol.10, pp.47965–47996, 2022, doi: https: //doi. org/10.1109/access.2022.3170844.

[2] S. AlJanah, N. Zhang, and S. W. Tay, "A Survey on Smart Home Authentication: Toward Secure, Multi - Level and Interaction - Based Identification, " *IEEE Access*, vol.9, pp.130914–130927, 2021, doi: https: //doi. org/10.1109/access.2021.3114152.

[3] U. Saritac, X. Liu, and R. Wang, "Assessment of Cybersecurity Framework in Critical Infrastructures, " *IEEE Xplore*, Feb.01, 2022. https: //ieeexplore. ieee. org/abstract/document/9753250/

[4] G. B. White and N. Sjelin, "The NIST Cybersecurity Framework," *Research Anthology on Business Aspects of Cybersecurity*, 2022. https: //www.igi - global. com/chapter/the - nist - cybersecurity - framework/288672 (accessed Nov.03, 2021).

[5] A. Henricks and H. Kettani, "On Data Protection Using Multi - Factor Authentication, " *Proceedings of the 2019 International Conference on Information System and System Management*, Oct.2019, doi: https: //doi. org/10.1145/3394788.3394789.

[6] D. Maclean, "The NIST Risk Management Framework: Problems and recommendations, " *Cyber Security: A Peer - Reviewed Journal*, vol.1, no.3, pp.207–217, Jan.2017, Available: https: //www.ingentaconnect. com/content/hsp/jcs/2017/00000001/00000003/art00003

[7] T. Hardjono, "Federated Authorization over Access to Personal Data for Decentralized Identity Management, " *IEEE Communications Standards Magazine*, vol.3, no.4, pp.32–38, Dec.2019, doi: https: //doi. org/10.1109/mcomstd.001.1900019

[8] J. H. Addae, X. Sun, D. Towey, and M. Radenkovic, "Exploring user behavioral data for adaptive cybersecurity, " *User Modeling and User - Adapted Interaction*, vol.29, no.3, pp.701–750, May 2019, doi: https: //doi. org/10.1007/s11257 - 019 - 09236 - 5.

[9] J. Zhang, L. Yang, W. Cao, and Q. Wang, "Formal Analysis of 5G EAP - TLS Authentication Protocol Using Proverif, " *IEEE Access*, vol.8, pp.23674–23688, 2020, doi: https: //doi. org/10.1109/access.2020.2969474.

[10] M. A. Rashid and H. H. Pajooh, "A Security Framework for IoT Authentication and Authorization Based on Blockchain Technology, " *IEEE Xplore*, Aug.01, 2019. https: //ieeexplore. ieee. org/abstract/document/8887316/ (accessed Jan.27, 2023).

[11] A. Bumiller, Stéphanie Challita, Benôıt Combemale, Olivier Barais, N. Aillery, and Gaël Le Lan, "On Understanding Context Modelling for Adaptive Authentication Systems, " *ACM Transactions on Autonomous and Adaptive Systems*, vol.18, no.1, pp.1–35, Mar.2023, doi: https: //doi. org/10.1145/3582696.

[12] H. Omotunde and M. Ahmed, "A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond, " *Mesopotamian Journal of CyberSecurity*, vol.2023, pp.115–133, Aug.2023, doi: https: //doi. org/10.58496/MJCSC/2023/016.

[13] D. Preuveneers, S. Joos, and W. Joosen, "AuthGuide: Analyzing Security, Privacy and Usability Trade - Offs in Multi - factor Authentication, " *Trust, Privacy and Security in Digital Business*, pp.155–170, 2021, doi: https: //doi. org/10.1007/978 - 3 - 030 - 86586 - 3_11.

[14] "PingOne Protect, " www.pingidentity. com. https: //www.pingidentity. com/en/platform/capabilities/threat - protection/pingone - protect. html (accessed Feb.21, 2024).