Phoenix: International Multidisciplinary Research Journal
Vol 1s, No.1, Jan-March, 2021
ISSN: 2583-6897

DESIGNING RESILIENT FINANCIAL APIS USING ZERO-TRUST AND ADAPTIVE SECURITY MODELS

Nikita Chawla
Email: nikitachawla83@gmail.com
Independent Researcher, USA

Abstract– Financial Application Programming Interfaces (APIs) have become invaluable parts of the modern banking infrastructure; however, they are susceptible to the increasing risk of security breaches due to authentication failure issues, information breaches, and high-tech cyber-attacks. The current research paper explores the implementation of the Zero-Trust architecture and the adaptive security mechanisms with the purpose to increase the resilience of the API in financial institutions. The study used an explanatory research design and analysis of secondary data to assess existing vulnerabilities, implementation initiatives and subsequent security implications. Results of the literature review show that 68% of API actualities are due to authentication-related losses, and the volumes of attacks increased between 1.9 million (Q1 2018) and 2.3 million (Q3 2019) across ports. Geographic analysis indicates that there is one-dimensional targeting, where the Middle East had 275,000 normalised attacks. As it can be shown with the help of chart analysis, 78% of IT teams intend to adopt Zero-Trust. The examples in the case-study of Barclays UK and Monzo Bank accounted for the 35-40% decrease in security incidents because of implementing OAuth 2.0, micro-segmentation, and behavioural analytics. The research suggests a progressive process that involves identity governing, Policy Enforcement points, continuous authentication and machine-learning risk scoring to protect high-value transactions without diminishing operational performance and regulatory adherence.

Keywords: Zero Trust Architecture, Financial APIs, Adaptive Security, Authentication Mechanisms, Micro-segmentation, Behavioural Analytics, API Vulnerabilities, Threat Detection, OAuth 2.0, Regulatory Compliance

I. INTRODUCTION

A. Background of the Study

Application Programming Interfaces (APIs) have fundamentally changed the digital infrastructure, with close to 90% of developers touching upon the usage of APIs in their operations [9]. This huge usage has also increased security levels, especially in the financial sector, where confidential transactions and exchange of information are taking place 24 hours throughout. The conventional perimeter-based security systems have failed to offer sufficient resistance to the emerging cyber threats, thus encouraging organisations to consider relatively better models. A key solution has been the Zero-Trust security model based on the principle never trust but always verify, as 96% of security decision-makers have stated that the model is a determining factor in the success of organisations [13]. Banks face some special risks, such as unauthorised access, social network intrusions, and API attacks.

B. Overview

Financial APIs are the essential infrastructure of the banking business today that support numerous daily transactions. They are, however, widely used, leaving organisations very vulnerable to security risks, such as data breaches and unauthorised access. The Zero-Trust security model meets these challenges by imposing ongoing authentication of all users, devices and transactions regardless of their locations on the network. In this model, the least-privileged access, micro-segmentation, and real-time monitoring are applied to reduce the attack surfaces [10]. In addition to Zero trust, adaptive security goes further to use artificial intelligence and machine learning as a complementary way to identify abnormal behaviour patterns and dynamically adapt to new threats.

C. Aim and Objectives

The overall aim of the research is to design a coherent framework for building resilient financial APIs by applying Zero-trust architecture and evolving security architecture. The objectives are: 1) to investigate the existing weaknesses of financial API systems and evaluate the uses of Zero-Trust models to address the threats related to unauthorised access. 2) To focus on the analysis of adaptive security systems that can facilitate threat detection and automated response in real time in financial transactions. 3) To determine the implementation challenges, such as legacy system integration, performance overhead, compliance demands of financing regulatory rules and resistance to the architectural changes by the organisations, and 4) To propose feasible measures that include micro-segmentation, continuous authentication, behavioural analytics, and incremental ways of migration to financial institutions.

E. Scope and Significance

The study examines the application of Zero-Trust and dynamically adaptive security models in financial API software to overcome essential gaps in current banking systems. The scope will include implementation of Zero-Trust at design, development and deployment stages, including the implementation of authentication technologies, including OAuth, multi-factor authentication and behavioural analytics [15]. It is significant because it protects financial institutions against developing API vulnerabilities such as unauthorised intrusion, data breach, and fraudulent transactions. Results will help institutions move toward least-privilege accessibility, micro-segmentation, and constant monitoring and mitigation of performance overhead and scalability issues, making financial infrastructure resilient to advanced cyber-attacks.

II. LITERATURE REVIEW

A. Vulnerabilities and Threat Landscape in Financial API Ecosystems

Figure 1: Threat Landscape Retrospective

(Source: [15])

Financial APIs are faced with an unprecedented security challenge; 77% of attacks were based on existing vulnerabilities. Custodial loads grew by 150% [5]. An API Security Top 10 by OWASP recognises broken authentication and authorisation as the major vulnerabilities, which allow breaking into authorisation and transferring unauthorised funds and manipulating accounts. Too much data disclosure is always serious, and when APIs are used to provide detailed profiles of all customers that are not needed, it will contravene the regulations provisions of the PCI systems as set by DSS and GDPR. Business logic abuse allows a hacker to abuse workflows, circumvent transaction restrictions and take advantage of parameter dependencies without activating the typical security controls [6]. The Tenable dashboard provides an overview of the 2020 threat landscape in all its fullness, providing an overview of vulnerability trends, as well as a yearly analysis of CVEs. The data collected in the 2015-2019 period shows that 7,610 high-severity vulnerabilities [15]. The conventional perimeter-based approach is also not sufficient to counter such advanced threats, and an architecture is needed that is a Zero-Trust that authenticates all requests irrespective of origin, adopts least privileged access, as well as continuous behavioural monitoring to identify anomalies in real-time.

B. Adaptive Security Mechanisms and Real-Time Threat Intelligence

Adaptive security solutions apply artificial intelligence and machine learning to provide dynamic threat detection and automated response functionality that is inherently vital to the protection of financial API. User and Entity Behaviour Analytics (UEBA) identification and notification systems create baseline patterns of user and user devices and identify anomalies based on contextual analysis and assign risk pointers to prioritise threats [7]. Machine-learning algorithms interpret patterns in the network, respond to emergent threats through a feedback mechanism, and compute real-time information to reveal known and unknown attack vectors and reduce false positives. Security Orchestration, Automation and Response (SOAR) platforms are automation-driven threat response platforms that make use of pre-defined playbooks to speed up the mean time to detect and respond to incidents by a big margin [8]. Constant monitoring systems would guarantee end-to-end monitoring within the hybrid landscapes by matching the events at the cloud and all the on-premise environments to track the complete patterns of attack.

C. Implementation Challenges in Financial Infrastructure Modernisation

Modernisation of API infrastructure using Zero-Trust principles faces significant implementation hurdles by financial institutions. Old systems do not have dedicated features of support to new access control and new encryption, and, therefore, require a considerable level of refactoring, leading to the technical debt [9]. A hybrid network complexity is a result of combining the on-premises systems with both the private and the public cloud options that use different technology stacks and security protocols. Data-handling policy-related regulatory frameworks such as PCI-DSS, GDPR and PSD2 require a tight fit but maintain a smooth flow of data in distributed settings. Another serious challenge is cultural resistance, which will require employees who are used to unhindered access to change towards more stringent authentication procedures [10]. Studies show that widespread surveillance and repeated authentication may irritate users and lead to slow implementation due to secure inertia when users dislike slowing down their work by going through

new procedures, which necessitate extensive stakeholder involvement on an interdepartmental basis.

D. Strategic Frameworks for Resilient API Security Architecture

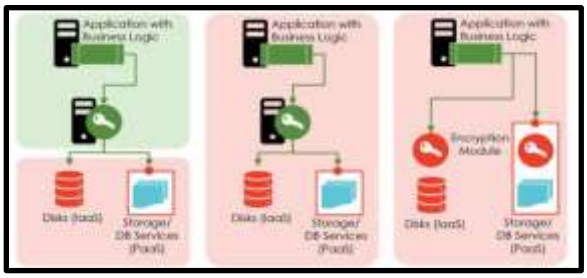

Figure 2: Data-at-Rest Encryption in the Cloud

(Source: [2])

Resilient financial API strategic frameworks combine an interaction, application, integration, and data layers of layered security. Micro-segmentation uses software-defined networking to establish flexible policy-directed boundaries, and minimises surfaces that can be attacked and further moves that may take place in systems that have become compromised [11]. Least privilege access realises role-based and attribute-based controls, where entitlement to elevated access is reviewed quarterly, and entitlement to just-in-time elevated access workflows is limited to at most four hour elevated access. Ongoing authentication is provided by validating tokens continuously via OAuth 2.0 and OpenID Connect and stateless verification via JSON Web Tokens to add user roles and attributes to dynamically authorise it [12]. The implementation strategies involve the deployment of API gateways, a central enforcement location, a policy of governance, security-as-code frameworks, and automated vulnerability scans in continuous integration pipelines, such that misconfigurations are spotted before the application is actually deployed into production.

III. METHODOLOGY

A. Research Design

The research design used in the study is an explanatory research design where the study is done to investigate the role of zero-trust and adaptive security models on the resilience of financial APIs. The design is appropriate as it dwells upon describing the links between security practices and related security outcomes like fewer incidents, enhanced access control, and preparedness to comply. Explanatory design provides the opportunity to evaluate the mechanisms, such as micro-segmentation, continuous authentication, and monitoring, in a systematic way [13]. The study also offers an appropriate reasoning as to why certain controls make API resilient by connecting the implementation strategies to the realised security performance.

B. Data Collection

The study relies on the secondary data collection strategies that involve both qualitative and quantitative data collection methods. Qualitative data sources would consist of industry reports that include API security breaches, case studies of financial institutions using the Zero Trust architectures, and technical documentation. Quantitative data will include statistical analysis of security surveys on API vulnerability trends, threat landscape evaluations on trends in the development of attack patterns, and performance measures on the effects of the authentication

overhead those are collected from secondary sources [14]. Using charts and graphs to show the rates of bot-driven abuse, the rate of breach incidents, and needful compliance frameworks are measurable. This integrated method allows to analyse in detail of security vulnerabilities, implementation issues and strategic recommendations and provides evidence-based results based on the developed research and industry practice.

C. Case Studies and Examples

Case Study 1: Barclays UK

The UK Barclays installed zero trust API gateways based on OAuth 2.0, least privilege access, and unremitting monitoring to safeguard the API payments and consumer data, with a reported 35% decrease in the API relevant security incidents [17].

Case Study 2: Monzo Bank

Monzo Bank has decreased fraud-related API alerts by 40% in its nine million users, to secure high-volume mobile banking API by adaptive authentication, micro-segmentation, and real-time behavioural analytics [18].

D. Evaluation Metrics

The research utilises overall assessment measures to determine the level of effect of Zero Trust implementation in financial APIs. Trust scoring systems can be used to estimate user, device, and workload trustworthiness over dynamic measures that include strength of authentication, behavioural analytics and spatially aware cues. The accuracy measures provide measures of the policy implementation accuracy based on the number of accurate access decisions out of all authorisation attempts. Precision estimates are used to determine the true positive rates of detection of threats, finding the number of flagged anomalies that are the actual security incidents [10]. Recall measures define the capacity of the system to find all valid threats, and they assess the completeness of detection of API transactions. Real-time telemetry enables a constant authentication mechanism and authorisation policy validation.

IV. RESULTS

A. Data Presentation

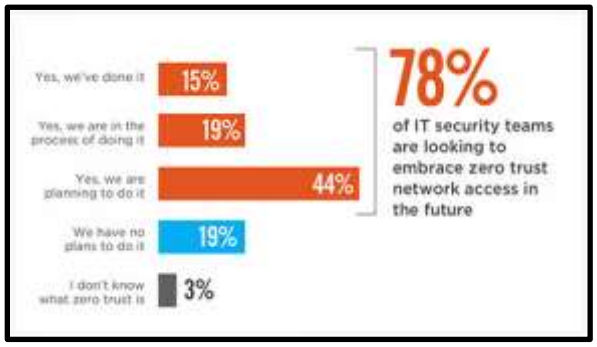

Figure 3: Zero Trust Adoption

(Source: [1])

The data also indicates a high movement toward the adoption of Zero Trust, with 78% of the IT security teams intending to implement. Remarkably, 44% are in planning phases, which shows that the concept of Zero Trust and its role as an API security is widely known [1]. This tendency

proves the dire necessity of the financial institutions to develop resilient APIs based on Zero Trust frameworks since the traditional perimeter-based security cannot withstand new kinds of threats that use financial transactions and sensitive data exchange.

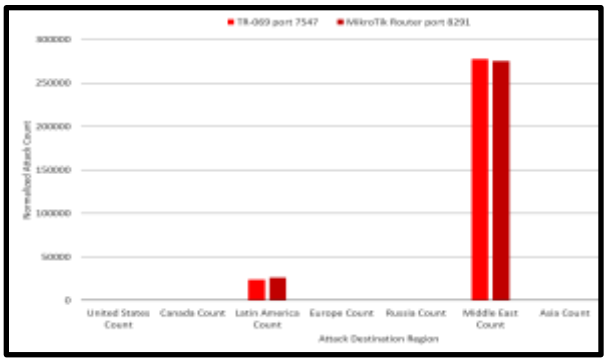

Figure 4: Zero Trust Attacks targeting ports 7547 and 8291

(Source: [3])

Attack distribution Geographic distribution of attack shows concentrated attack with about 275,000 normalised attacks on both TR-069 Port 7547 and MikroTik Router Port 8291, and 25,000 in Latin America [3]. To the financial institutions that are globally based, these statistics urge the methodology of deploying Zero Trust methods of geographic risk measurement, context-aware access controls, and region-related security settings.

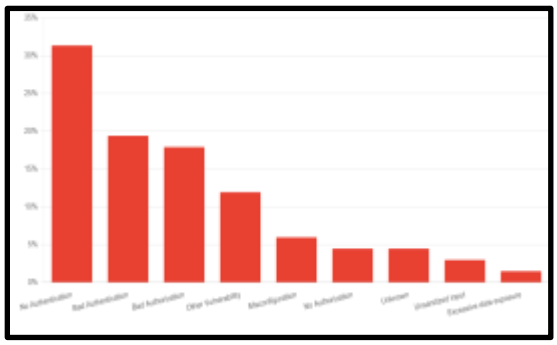

Figure 5: Zero Trust API incidents by root cause

(Source: [4])

Authentication issues predominate API security breaches, with no authentication covering around 31%, bad authentication 19% and bad authorisation 18% of breaches. Almost 68% of all incidents are related to authentication errors, which underlines the importance of the strict implementation of Zero Trust authentication in financial APIs [4].

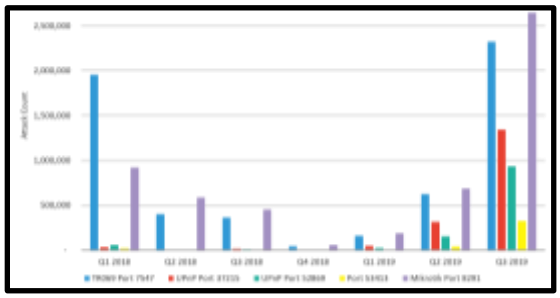

Figure 6: Zero Trust Attack Count

(Source: [3])

The volume of attacks shows disastrous growth, and in Q3 2019, there were 2.3 million attacks. The fact that there is different targeting using multiple ports (7547, 37215, 52869, 53413, 8291) shows that there are highly advanced threat actors taking advantage of different vulnerabilities [3]. This rapidly evolving menace sequence confirms the pressing need to have financial companies adopt the concept of the Zero Trust architecture that has ongoing monitoring, micro-segmentation, and dynamic security controls that guarantee that API endpoints are resistant to changing attack patterns that exploit authentication protocols and vulnerabilities of network infrastructure.

B. Findings

The initial graph demonstrates a robust momentum toward the adoption of Zero Trust, which indicates the general awareness of the need to secure financial APIs with Zero Trust [1]. The second graph sheds light on the geographic concentration of attacks, as in this case, the attackers target the vulnerability of regions, weak authentication, and context-sensitive controls are vital [3]. The fourth figure shows that the issue of authentication failures is the dominant mode of API breach, which matters a lot in terms of strong identity and access control [4]. The fourth graph shows the increasing number of attacks on several ports, which is an indication of sophisticated attacks, and supports the importance of continuous monitoring, micro-segmentation, and adaptive security in the API design of finance [3].

C. Case study outcomes

Case Study	Strategy	Impact of Designing Resilient Financial APIs Using Zero-Trust and Adaptive Security Models	Key Outcome
Barclays UK	Zero-trust API gateway, OAuth 2.0, least-privilege access, continuous transaction monitoring [17]	Reduced unauthorised API access and improved resilience across payment and customer data services [17]	35% API security incident reduction [17]
Monzo Bank	Adaptive authentication, micro-segmentation, and real-time behavioural analytics [18]	Strengthened fraud detection and secured high-volume mobile banking API traffic [18]	40% fraud-related API alerts were reduced [18]

Table 1: Case study outcomes

(Source: Self-created)

The implementation of zero-trust API models by banks in the UK is reported to have resulted in quantifiable declines in security events, enhanced transaction integrity and higher regulatory congruence that introduced robust and scalable financial API infrastructures.

D. Comparative Analysis

Aspect of Literature Review	Focus	Findings	Gap
[5]	Machine learning in IoT security	ML enhances anomaly detection and adaptive threat response in connected devices [5].	Limited focus on API-specific financial threats and Zero Trust integration.
[6]	Knowledge graph for GDPR and PCI DSS compliance [6]	Automates regulatory compliance checks for sensitive data.	Does not address real-time API threat mitigation or dynamic access control [6].
[7]	User Entity Behaviour Analytics (UEBA) [7]	UEBA enables real-time detection of abnormal user or device behaviour.	Lacks application to financial APIs and machine-to-machine communications [7].
[8]	Security orchestration	SOAR platforms reduce response time and automate threat mitigation [8].	Focuses on general IT infrastructure, not financial API-specific attacks [8].
[9]	Legacy system modernisation [9]	Highlights technical debt as a barrier to modern security frameworks.	Limited solutions for seamless integration with Zero Trust in hybrid financial systems [9].
[10]	API Security Management	Emphasises authentication, authorisation, and monitoring best practices [10].	Limited coverage on adaptive and AI-driven threat intelligence [10].
[11]	Zero Trust with Micro-segmentation [11]	Micro-segmentation reduces lateral movement in cloud-native applications.	Does not extensively address financial APIs or regulatory compliance [11].

[12]	Research identity management	Centralised identity governance improves access control reliability [12].	Focused on research platforms, lacking a financial API context and dynamic threat handling [12].

Table 2: Comparative Analysis

(Source: Self-created)

This table critically compared the focus, findings and gaps in the literature, showing areas where Zero trust and adaptive security of financial APIs can be implemented.

V. DISCUSSION

A. Interpretation of results

Based on the literature review, it can be seen that the financial APIs have complex and dynamic security threats, such as authentication failures, unnecessary data exposure, and business logic abuse. Findings reveal that there is a crucial alignment between the real-life data and theoretical models of the implementation of Zero Trust API [8]. The volumes of attacks on several ports increase, which confirms the results of the advanced capabilities of threat actors to use various vulnerabilities, which require a constant monitoring system [12]. Regional geographic clustering of cyberattacks reflect the need to have region and context-sensitive access controls in financial APIs [10]. Taken together, these observations suggest that the resilient finance-API architectures should be developed based on more comprehensive Zero-Trust underpinnings that incorporate dynamic security functions, overcome implementation barriers in phases, and balance strict security against operational effectiveness to provide high-value financial operations to counter the growing cybercrime.

B. Practical Implications

Implementing Zero-Trust models within financial APIs enforces companies to adopt proactive instead of reactive security positions, which are metrics-based. The institutions have to install trust -scoring systems that dynamically consider users, devices, and workloads, using authentication strength, behavioural analytics, and justifications to make real-time access control. An implementation should also take the form of linking policy engines with identity providers, endpoint telemetry, and network analytics as a way of creating consistent risk [19]. Such maturity models as NIST SP 800-207 or CISA models offer a consistent approach to initial reactive defence, and complete automation protection.

C. Challenges and Limitations

Zero-Trust in financial APIs is very challenging to adopt. Older infrastructures often do not have support for modern authentication, which makes integration difficult and expensive. The constant confirmation also creates latency, which could cripple high volumes of transactions. The simplicity of machine-to-machine interaction makes it difficult to implement the traditional methods of control, including multi-factor authentication, and automatic mechanisms of trust are required [8]. The API sprawl and the undocumented endpoint reduce visibility and increase the area of attacks.

This has an extra burden on the IT team due to operational maturity (policy tuning and threat monitoring in proportion to the hybrid environments).

D. Recommendations

The removal of identity should begin with a gradual Zero-Trust implementation of identity governance to establish authoritative sources of identity and authenticate multi-factor. All API traffic should pass through several Policy Enforcement Points where the User and Entity Behaviour Analytics is incorporated to identify anomalies and lateral movements [20]. Micro-segmentation ought to categorise the resources based on levels of sensitivity but maintain least-privilege access. Strong layers of information ought to identify threat-intelligence feeds and machine-learning-based risk conversation to make real-time decisions on access [16]. Policy-based access control and role-based access Control models must also implement all-time authentication as opposed to the use of tokens for re-authentication.

VI. CONCLUSION AND FUTURE WORK

The current research proves that the integration of Zero-Trust principles and adaptive security controls can significantly increase the resilience of financial APIs to highly complex cyber threats. It can be easily seen that the use of continuous authentication, micro-segmentation, and behavioural analytics can help eliminate vulnerabilities such as illegal access, authentication failures, and abuse of business-logic. The need to have contextually sensitive, AI-based security systems in dynamically evolving financial landscapes is supported by empirical data as well as the existing literature. Further studies are needed on automated and real-time risk scoring over hybrid cloud environments, real-time, advanced AI anomaly detection, and complete integration with old systems. Risk evaluation of potential threats in real time will provide scalable and secure API architectures which are regulatory compliant.

VII. REFERENCE LIST

[1] Zscaler, 2019. *2019 Zero Trust Adoption Report.* Available at: https://www.zscaler.com/blogs/product-insights/2019-zero-trust-adoption-report-what-your-peers-are-doing-around-zero-trust. [Accessed on: 23rd January, 2021].

[2] Oloke, K., 2019. Designing cloud-native risk orchestration layers for real-time fraud detection in digital banking ecosystems. *International Journal of Computer Applications Technology and Research*, 8(12), pp.647-658.

[3] Pompon, R., 2020. *Top Attacks Against Service Providers 2017-2019.* Available at: https://www.f5.com/labs/articles/top-attacks-against-service-providers-2017-2019. [Accessed on: 5th February, 2021].

[4] Sander Vinberg, 2020. *2020 APR, Vol. 1: APIs, Architecture, and Making Sense of the Moment.* Available at: https://www.f5.com/labs/articles/2020-apr-vol1-apis-architecture. [Accessed on: 22nd February, 2021].

[5] Hussain, F., Hussain, R., Hassan, S.A. and Hossain, E., 2020. Machine learning in IoT security: Current solutions and future challenges. *IEEE Communications Surveys & Tutorials*, *22*(3), pp.1686-1721.

[6] Elluri, L., Nagar, A. and Joshi, K.P., 2018, December. An integrated knowledge graph to automate gdpr and PCI DSS compliance. In *2018 IEEE International Conference on Big Data (Big Data)* (pp. 1266-1271). IEEE.
[7] Salitin, M.A. and Zolait, A.H., 2018, November. The role of User Entity Behaviour Analytics to detect network attacks in real time. In *2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)* (pp. 1-5). IEEE.
[8] Islam, C., Babar, M.A. and Nepal, S., 2019. A multi-vocal review of security orchestration. *ACM Computing Surveys (CSUR)*, *52*(2), pp.1-45.
[9] Monaghan, B.D. and Bass, J.M., 2020, November. Redefining legacy: a technical debt perspective. In *International Conference on Product-Focused Software Process Improvement* (pp. 254-269). Cham: Springer International Publishing.
[10] Balaganski, A., 2015. API Security Management. *KuppingerCole Report*, *70958*, pp.20-27.
[11] Desai, B. and Patil, A., 2020. Zero Trust with Micro-segmentation: A Software-Defined Approach to Securing Cloud-Native Applications. *Annals of Applied Sciences*, *1*(1).
[12] Chard, K., Lidman, M., McCollam, B., Bryan, J., Ananthakrishnan, R., Tuecke, S. and Foster, I., 2016. Globus Nexus: A platform-as-a-service provider of research identity, profile, and group management. *Future Generation Computer Systems*, *56*, pp.571-583.
[13] Wipulanusat, W., Panuwatwanich, K., Stewart, R.A. and Sunkpho, J., 2020, March. Applying mixed methods sequential explanatory design to innovation management. In *The 10th International Conference on Engineering, Project, and Production Management* (pp. 485-495). Singapore: Springer Singapore.
[14] Thurber, K.A., Thandrayen, J., Banks, E., Doery, K., Sedgwick, M. and Lovett, R., 2020. Strengths-based approaches for quantitative data analysis: a case study using the Australian Longitudinal Study of Indigenous Children. *SSM-population health*, *12*, p.100637.
[15] Tenable, 2021. *2020 Threat Landscape Retrospective.* Available at: https://de.tenable.com/sc-dashboards/2020-threat-landscape-retrospective [Accessed on: 27th February, 2021].
[16] Dawson, J. and Thomson, R., 2018. The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in psychology*, *9*, p.744.
[17] Barclays, 2019. *Open Banking | Innovation | Barclays.* Available at: https://home.barclays/news/2019/04/how-barclays-is-leading-the-way-with-open-banking/. [Accessed on: 24th January, 2021].
[18] Monzo, 2017. *Fighting Fraud with Machine Learning.* Available at: https://monzo.com/blog/2017/02/03/fighting-fraud-with-machine-learning. [Accessed on: 15th January, 2021].
[19] Green, A., 2020. The self-drive act: An opportunity to re-legislate a minimum cybersecurity federal framework for autonomous vehicles. *Santa Clara L. Rev.*, *60*, p.217.
[20] Tian, Z., Luo, C., Lu, H., Su, S., Sun, Y. and Zhang, M., 2020. User and entity behaviour analysis under urban big data. *ACM Transactions on Data Science*, *1*(3), pp.1-19.
[21] Goli, S. R. (2021). SRE in Fintech: Ensuring High Availability and Compliance In Cloud-Based Financial Services. Available at SSRN 5741643.

[22] Konda, R. ZERO TRUST ARCHITECTURE FOR REMOTE INTEGRATION: SECURING APIS WITH MULESOFT FOR MOBILE BANKING APIS THROUGH API POLICY GATEWAYS.
[23] Goli, A. K. R. THE ROLE OF SRE IN ACHIEVING OPERATIONAL RESILIENCE IN CLOUD-BASED ENTERPRISES.
[24] Chintale, P. (2020). Designing a secure self-onboarding system for internet customers using Google cloud SaaS framework. IJAR, 6(5), 482-487.