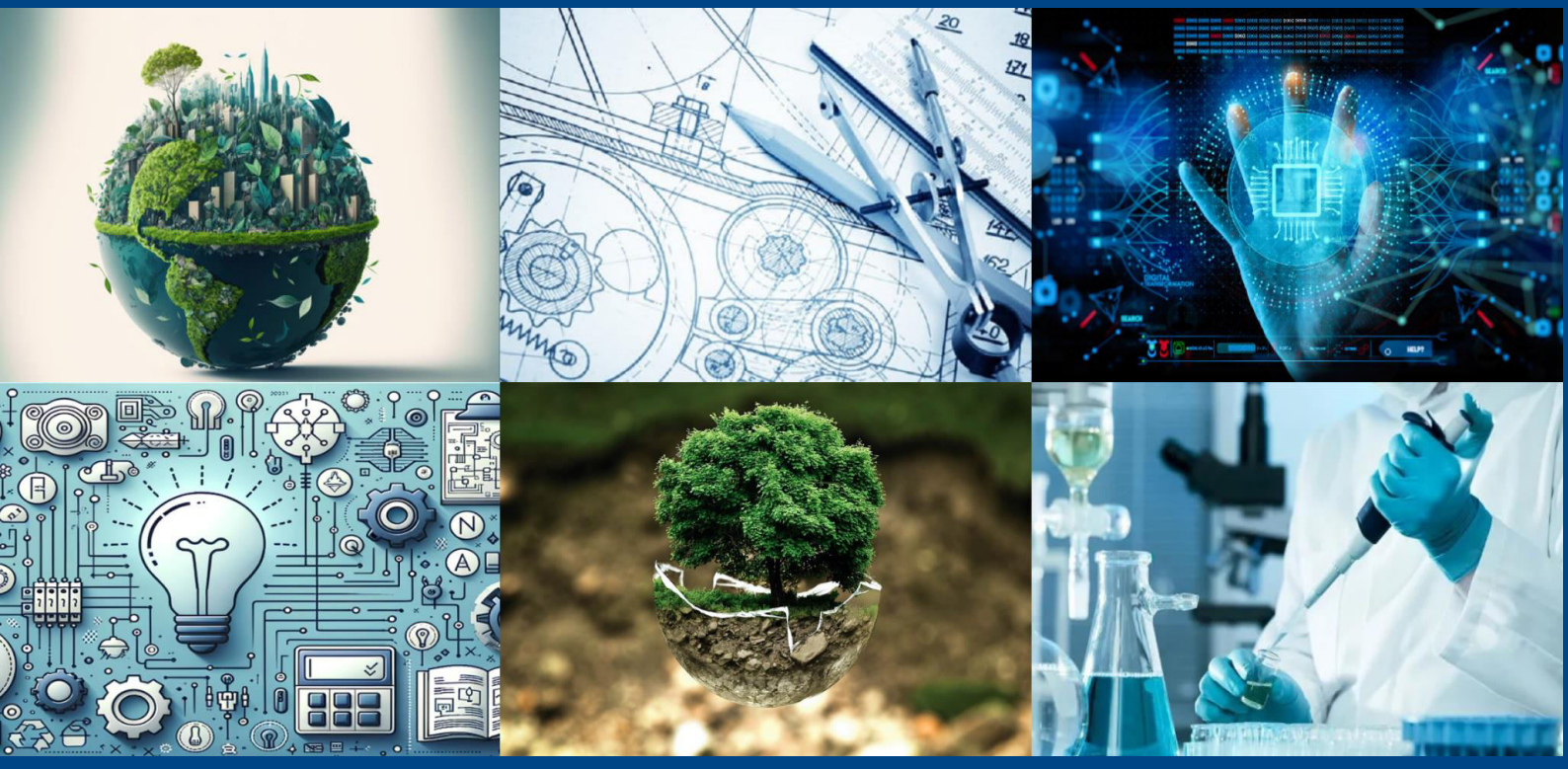
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 5, May 2025**

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805083

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Implementation of Zero Trust Model in Microfinance

Dik Sharma, Chithra H N, Hritik Raj

Research Scholar, Bangalore, India

ABSTRACT: The microfinance industry presents a key financial function for such underserved populations. Concurrently, this sector also harbours a considerable degree of cybersecurity risk due to the innate dependence on digital platforms and high sensitivity to data. This paper introduces the discussion on using the Zero Trust Model in Microfinance Institutions as a means to improve security and cyber threat resistance. In contrast to the embedded security models inherent in conventional security models, founded on trusting all internal network traffic by default, the Zero Trust Model defaults to one of "never trust, always verify" and thereby forgoes implicit trust and actively verifies each and every phase of digital interaction.

The paper starts by providing an overall situational analysis of the current state of cybersecurity in microfinance institutions, noting a few vulnerabilities and common attack vectors. Principles, architecture, and core components of the ZTM micro-segmentation, least privileges, and continuous monitoring are described. The paper now raises issues and considerations in the implementation of ZTM within MFIs: integration of legacy systems, user education, and compliance-related problems with regulatory standards.

KEYWORDS: Zero Trust, Microfinance, Security, Micro-Segmentation, Finance, Data Breaches, Data.

I. INTRODUCTION

Microfinance refers to the provision of very small financial products-loans, savings, insurance, and remittances-to low-income earners and small businesses that usually have no easy access to traditional or formal banking services. In essence, the fundamental goal of microfinance institutions is empowerment of poor communities, thereby providing a lifeline to people frequently shut out of the formal regime within the financial world owing to the lack of collaterals, history in credit, or perhaps even stable income.

Microfinance is a concept that targets the inclusion of people into the financial mainstream by enabling them to create or expand small businesses, manage risk, and improve their living standards. In its promotion of entrepreneurship, MFIs provide minute loans, usually known as microloans, which provide an entrepreneur with the opportunity for investment in his or her business besides creating employment and stimulating the local economy. Apart from microloans, services like savings accounts and microinsurance provide a cushion that also helps in propping up poor people so that they can be financially stable and more resilient amid shocks.

The microfinance sector has undergone structural changes in its use of digital technologies to increase its outreach to distant and unserved areas. Notwithstanding the benefits, areas of concern that remain are related to high operational costs, over-indebtedness of the borrower, and sustainability of the business models. Nevertheless, microfinance is an extremely significant tool of poverty reduction and economic empowerment at a global level.

II. RESEARCH OBJECTIVE:

The objective of this paper is to analyse in-depth the applicability and effect of the Zero Trust Model (ZTM) in microfinance institutions (MFIs). The paper starts with analysing the existing cybersecurity stance of MFIs, determining major vulnerabilities within their current controls, policies, and procedures that can be targeted by cyber-attacks. The research then evaluates the technical and organizational feasibility of implementing Zero Trust principles through a review of MFIs' infrastructural and human capital preparedness. Additionally, the study looks at how well Zero Trust architectures work to stop cyberattacks, enhance threat detection, and support real-time response systems. The customer experience impact is also taken into consideration, with special regard to the balance between security and user experience. Challenges and implementation barriers, from legacy infrastructure to employee training and compliance, are subjected to critical scrutiny, and approaches to overcoming them are suggested. A step-by-step, pragmatic implementation framework is presented, informed by best practice, operational checklists, and regulatory

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

alignment. The report incorporates a cost-benefit analysis in order to examine the economic feasibility of implementing Zero Trust and identifies the possible involvement of new technologies such as AI, machine learning, and biometrics in amplifying authentication and threat intelligence. Lastly, the research outlines a future-oriented roadmap for integrating Zero Trust in MFIs, outlining future trends and technological breakthroughs that can further strengthen the security and resilience of the industry.

III. RELATED WORK

In the research Zero Trust: Applications, Challenges, and Opportunities, stated that Zero Trust offers a paradigm change in the solution it offers to protect digital assets and sensitive information from the ever-growing cybersecurity threat landscape. Zero trust challenged the very pillars of security models guided by its contemporary concept of continuous verification and least privilege access. These can be used to secure cloud environments, remote work engagement, and protecting the IoT ecosystem. Technical and cultural issues are to be addressed prior to unleashing the value of Zero Trust. Zero Trust is much more powerful and effective when integrated into other emerging technologies like AI and machine learning. This security environment is full of meaning; dynamic in disposition, responsive. It further empowers one to walk through the ever-changing world of cybersecurity with resilience, adaptability, and construed a development rightly redefining trust in this present age of digitality. The application of the Zero trust framework cuts across several industries and organizations, including government agencies, financial sectors, health industries, enterprises, and institutions of different sizes. It is therefore a very interesting architecture in terms of adaptability and scalability in relation to contemporary networking, which requires flexibility, dynamic access controls, and robust security postures.

Research Studies on Zero Trust Architecture (ZTA) are at a nascent stage. Nonetheless, the failures of conventional legacy systems have fuelled the creation of more sophisticated measures to combat cyber-attacks. Attempting to fill the gap in trust, authors of [6] modified the ZTA model to introduce a trust model specifically designed for cloud environments. Their research introduced a high-fidelity approach to improving trust in organizational information systems that includes reference elements from the National Institute of Standards and Technology (NIST). Performance assessments showed that distributing trust-based nodes was able to effectively cope with intrusions. Likewise, with the limitations in existing cybersecurity measures in virtual power plants, researchers in [7] embraced ZTA to enhance privacy and data security in the energy industry. Their ZTA model provided an effective remedy to data theft and breaches. The implementation of Zero Trust solutions has further gained momentum since the COVID-19 pandemic began, which transformed work environments by encouraging remote working. Although remote work kept the virus at bay, it also heightened the exposure of networks and systems. The Zero Trust concept solves such vulnerabilities by removing trust assumptions and closing possible security loopholes. Due to this, most organizations have adopted it as a vital shield against cyberattacks. In particular, major U.S. government departments, such as the Department of Defence, the Department of Health and Human Services, and the Department of Homeland Security, have adopted the Zero Trust model [8], [9].

Sultana [10] et al. introduced a zero trust-based secure medical image sharing system with the support of block-chain technology. Zero trust is integrated with blockchain in the system. Blockchain works to secure sensitive data. Robust security of medical data, but this also adds to the system's complexity and must be researched in terms of efficiency.

Weever et al. [11] suggested a zero-trust model of network security in a containerized system, which addressed how to provide zero trust for "east-west" traffic among micro-services within a containerized system using Kubernetes and Istio service mesh to construct. A zero-trust model for containerized environments decreases data leakage within containerized environments, yet the model fails to provide behaviour analysis and detection of data leakage.

IV. WORKING OF MICROFINANCE

Microfinance institutions provide financial services, including loans, savings, insurance, and remittances, to low-income earners or small business enterprises that are mostly inaccessible to traditional banking services. Typical Work Process for an MFI: The steps below are typical of how the work is done by an MFI.

- Client Identification and Outreach: Client from very different kinds of areas are identified and they are reached through various way.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- Client Assessment: Determine new customers' creditworthiness by holding personal interviews and confirming prior financial experiences, and appraising security/collateral wherever necessary.
- Loan Sanctioning and Disbursement: Approve such loans after assessment and disburse funds to clients upon signing agreements, which stipulate the terms for such repayments.
- Savings and Deposits: Savings accounts and deposit services that allow clients to save their money safely.
- Insurance Services: Provision of microinsurance products that help the client guard against illness, death, or natural disasters.
- Repayment Collection: Recovery of the loan principal plus interest according to the agreed schedule, usually directly by loan officers or increasingly through digital payment channels.
- Monitoring and Follow-up: Keeping track of the financial health of clients and the proper use of loan funds. After-sales support and financial literacy training will be provided as required.
- Reporting and Compliance: Keeping an updated record of all transactions, preparing financial reports, and ensuring compliance with regulatory requirements.

ADVANTAGES OF MICROFINANCE:

- Poverty Alleviation: Microfinance contributes to the alleviation of poverty by giving finance that otherwise would be accessible to the poor, thereby investing in the available opportunities of business or education and similar activities for better life.
- Women Empowerment: Most of the microfinance efforts are targeted towards women; hence these aids in starting or increasing their own business ventures. Financial independence like this might influence an improvement in social and economic status.
- Economic Development: Microfinance provides for the rebeginning of general economic development and growth of any community or region through its service to small businesses.
- Job Creation: The small businesses, deriving their good benefit from microfinance lending, are capable of creating employment to reduce unemployment. These jobs will lessen unemployment, and such unemployment may contribute to a country that is more stable in its economy.
- Higher Financial Inclusion: Access to the available financial services enhances financial inclusion among the normally excluded people with no access to formal banking.
- Savings Incentives: Many microfinance institutions have savings programs that build a safety net and plan for the future.

DISADVANTAGES OF MICROFINANACE:

- High Interest Rates: Lending risks due to low-income people may compel some microfinance institutions to charge high interest rates, therefore acting as a debt trap in case the loan is not payable by the borrower.
- Over-Indebtedness: Easy access to micro-loans may result in overborrowing or rather in over-indebtedness when any person takes multiple loans with different lenders.
- Disruption of Existing Lenders: This may as well disrupt the current lending systems because sometimes the integration in formal financial structures is less than optimal.
- Microfinance and Its Impact on Poverty: Despite being quite effective in the improvement of individual conditions, microfinance can only contribute marginally to the poverty alleviation process if not integrated with other development activities.
- Sustainability Issues: The most common issue about sustainability that has been identified is that the micro-finance institutions are either too dependent on external funding or have a weak business model.
- Loans utilization: Many microfinance clients use their loans for nonproductive purposes; some even use it for consumption, which has nothing to do with earning money to pay back with interest, and they end up falling into a financial trap.

1. CHALLENGS FACED BY MICROFINANCE:

The microfinance sector plays a very critical role in advancing financial services for low-income communities for financial inclusion and economic growth [1]. Notably, however, as the digital transformation in this area tracks, so are potential cyber threats emerging.

(Illangakoon, 2024)Traditional security models that were based on perimeter defence-consciously are tasked with increasingly challenging tasks protecting sensitive financial data and preserving the integrity of MFIs [4]. These

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

problems find a very strong answer in the Zero confidence Model-a security architecture that features constant evaluation of access requests from everyone and no implicit confidence. The current paper undertakes a review of the Zero Trust Model in microfinance, its tenets, advantages, and doable procedures for adoption.

1. Increased Chances of a Data Breach:
We have an implied trust in a network perimeter with no Zero Trust; the attackers just break through the perimeter, and after that, lateral movement inside the network isn't difficult, as various data breaches have proved.

2. Insider Threats:
In traditional security models, there are no such continuous monitoring and fine-grained access controls in place; therefore, it is rather easy for malicious/compromised insiders to have inappropriate access and misuse sensitive information.

3. Non-Compliance with Regulatory Standards:
Almost all modern regulatory frameworks put in place the requirement for a strong regime for data protection. In the absence of Zero Trust, this is easily and readily unachievable for an MFIs, thereby running a risk of fines and litigation.

4. Suboptimal Response Against APTs:
Very sophisticated APTs, in these, would leverage the very sophisticated and stealthy tactics of penetration into the network or exploitation over time, leaving traditional security measures ineffective.

5. Inadequate Visibility/ Monitoring:
Largely because of limited monitoring and analytics, the threats are sure to remain undetected for longer. The more time taken to detect would further enhance the expected damage faced by the organization.

6. Added Risk with Work-from-Home:
This could particularly be as a result of an outdated conventional perimeter-based security model that clearly is much less effective when it comes to remote work [2]. The result essentially is that remote workers and their data are in a very vulnerable state of attack.

2. ZERO TRUST MODEL

Zero Trust Model: This is a form of the modern security framework used to respond to threats as they evolve in structure and how failures of old traditional ways of security measures materialize. Zero Trust basically means, "Never trust; always verify." Nothing, either inside or outside the network, is trusted by default. In its place, every request for access is rigidly authenticated and authorized, continuously monitored.

The Zero Trust Model is based on the principle of "never trust, always verify." In most traditional security models, there is a perimeter inside which some level of trust exists among users [2]. Zero Trust presumes that the threats are valid not only from outside but also from inside.
So, any request for access must be vigorously verified, irrespective of its source. Critical elements in Zero Trust include:

Micro-Segmentation: This will further carve up the network into small, isolated segments. Each segment is itself isolated from all the others to constrain the spread lateral movement of threats inside a compromised network.

Least Privilege Access: It grants users the minimum access level required by them to perform the particular task they want to do.

Continuous Monitoring and Verification: That is, monitor all activities of users continuously in real-time; therefore, each and every access request will be checked or verified.

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805083

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

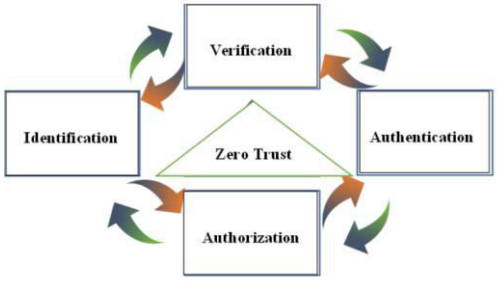


Figure 1: Zero Trust Model.

V. IMPLEMENTING ZERO TRUST MODEL IN MICROFINANCE

1. Overall Security Posture
First and foremost, an inventory on the existing security stance is the initial step of Zero Trust. This is done with regard to an asset map, determination of the key assets, evaluation of the current security controls, and finally, outlining likely vulnerabilities

2. Defining a Security Perimeter
In Zero Trust, the security perimeter is not around the network but around the data, applications, and users. Critical elements identification forms the base of implementing effective Zero Trust controls.

3. Micro-Segmentation
Micro-segmentation entails setting up the network of the organization into isolated segments. This would allow threats to be contained in one network segment in case of a breach, thus preventing threats from moving laterally across the different network segments.

4. Multi-Factor Authentication Implementation
The implementation of multi-factor authentication to all the points of access ensures that every user, be it internal or external, has passed enough verification [3]. This quite will be very important in doing away with single-factor authentication.

5. Least Privilege Access
Users are configured to have only the type of access authorized to perform their specific role. Regularly review and adjust access privileges to ensure the principle of least privilege is maintained.

6. Automation of Security Policy
It frees up time to ensure that, through automation, security policies are executed over a network all the time. Automation reduces the risk associated with the human element and ensures the consistency of applying security controls.

Figure 2: Zero trust access.

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805083

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

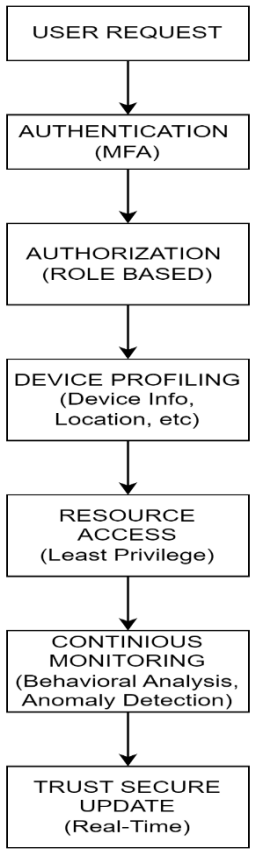


Figure 3: Zero-trust architecture working

VI. RESULTS & CONCLUSION

1.Data Breaches and Cyber Attacks

Drawback: Microfinance institutions often contain sensitive clients' data and financial information. Traditional models for security are open to huge cases of data breaches and cyber-attacks since there is some kind of implicit trust within the network.

Zero Trust Solution:

Continuous Verification: To lessen the chance of unwanted access, each access request will be thoroughly verified and approved.

Micro-Segmentation: Isolates network segments for containing breaches and limits the lateral movement of threat.

2. Insider Threats

Drawback: Insider threats, either malicious or negligent, are capable of huge data breaches with huge associated financial losses.

Zero Trust Solution:

Least Privilege Access: Making sure that the users are given access on the principle of least privilege for doing their jobs reduces possible misuse.

Behaviour Analytics: Monitor and track user activities for response to anomalies in case of insider threats.

3. Non-Compliance with Regulatory Standards

Drawback: Charges of non-compliance are mostly hefty in fines and legal issues. To be complied with by the MFIs are the very stringent regulatory requirements on Data Protection and Privacy, just like that of the GDPR.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Zero Trust Solution:
It logs each and every access attempt in detail; hence, this is very important for regulatory audits.
High-security data: The produced data is well protected due to constant monitoring and efficient authentication in compliance with the regulator.

4. Insecure Remote Access
Drawback: With remote work getting increasingly adopted, there are also increased security risks from the inability of the models to effectively secure remote access.
Zero Trust Solution:
Secure Remote Access: All access, including the remote ones, is validated and authenticated.
MFA: This is the location where remote access will be further hardened by including multiple means of authentication.

5. Limited Visibility into and Monitoring of Activities
Drawback: The conventional security models normally provide limited, inadequate, or no complete visibility into activities occurring over the network, sued in detecting and posing prompt responses to threats.
Zero Trust Solution:
Real-Time Monitoring: Monitor continuously for the discovery of the entire activity on the network which detects and responds to threat in no time.
Advanced Analytics: It uses behaviour analytics to recognize security incidents and mitigates them, hence avoiding turning into solid attacks or real breaches of data.

6. Over-Privileged Accounts
Drawback: Employees normally have more access than required, which places the data at a higher risk of breach and misuse.
Zero Trust Solution:
Role-Based Access Control: The access is parcelled out for certain roles, and thus employees will have access only to the information they want.
Regular Reviews of Access: The access privileges are regularly reviewed and revised so that the principle of least privilege is maintained in the network.

7. High Operational Cost
Drawback: Resource-intensive, error-prone security management is involved.
Zero Trust Solution:
Automated Policy Enforcement: fewer manual interventions, more consistent application of security policies.
Scalability in Security Solutions: MORE efficiency in resource usage for the automated security processes that adapt to change.

VII. FUTURE ENHANCEMENT

- Artificial Intelligence and Machine Learning: AI and ML further harden the Zero-trust models through threat detection, incident response, and identity verification.
- Moving to Cloud-based services: In its place, cloud-based infrastructure for Microfinance Institutions will mean zero-trust models' core to the protection of data in cloud environments.
- Customer experience-driven: The zero-trust models will ensure transactions are safe while reducing friction in the user experience with seamless authentication and authorization of users.
- IoT and Edge computing: With the growth implementation of IoT devices and edge computing in microfinance institutions, zero-trust models should, therefore, be adjusted to provide adequate coverage over new attack surfaces.
- Better Collaboration and Industry Standards: Sharing of Best Practice among the Microfinance Institutions relating to Zero-Trust Implementation. Industry-wide standards on zero-trust Implementation are put in place for aggressive adoption rates.
- Identity-Centric Security: Zero-trust models give much focus to identity validation through modern methods of authentication, including Behavioural Biometrics and Password less Authentication.
- Continuous Monitoring and Analytics: In a zero-trust environment, threat detection and response will be at the core of Next-Generation real-time monitoring and analytics.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- Keeping up with evolving regulatory requirements: As zero-trust implementations evolve, so also do the set of evolving regulatory requirements microfinance institutions need to keep in line with. Key amongst these are data privacy laws.

This will further aid the microfinance institutions in providing secure, efficient, customer-centric services, and thereby furthering financial inclusions and stability.

REFERENCES

[1] Stafford, V. (2020). Zero trust architecture. *NIST special publication*, *800*, 207.
[2] He, Yuanhang, et al. "A survey on zero trust architecture: Challenges and future trends." *Wireless Communications and Mobile Computing* 2022.1 (2022): 6476274.
[3] Buck, Christoph, et al. "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust." Computers & Security 110 (2021): 102436.
[4] Murphy, Crystal. "'Trust No One': The Logics of Microfinance, Depending on Whom You Ask." Who Gives to Whom? Reframing Africa in the Humanitarian Imaginary. Cham: Springer Nature Switzerland, 2024. 155-174.
[5] Illangakoon, G. (2024). Risk Management and Performance of Microfinance Industry. South Asian Journal of Social Studies and Economics, 21(3), 1-17.
[6] L. Ferretti, F. Magnanini, M. Andreolini, and M. Colajanni, "Survivable zero trust for cloud computing environments," Comput. Secur., vol. 110, 2021, doi: 10.1016/j.cose.2021.102419.
[7] A. Alagappan, S. K. Venkatachary, and L. J. B. Andrews, "Augmenting Zero Trust Network Architecture to enhance security in virtual power plants," Energy Reports, vol. 8, 2022, doi: 10.1016/j.egyr.2021.11.272.
[8] K. Macri, "What is Zero Trust? Federal Agencies Embrace Cybersecurity Innovation," Govcio Media and Research, 2021. https://governmentciomedia.com/what-zero-trust-federal-agenciesembrace-cybersecurity-innovation.
[9] NIST, "Zero Trust Architecture, SP 800-207," Natl. Inst. Stand. Technol. Spec. Publ., vol. SP 800-207, 2020.
[10] M. Sultana, A. Hossain, F. Laila, K. A. Taher, and M. N. Islam,"Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology," BMC Medical Informatics and Decision Making, vol. 20,no. 1, pp. 1–10, 2020.
[11] C. de Weever and M. Andreou, Zero Trust Network Security Model in Containerized Environments, University of Amsterdam, Amsterdam, The Netherlands, 2020.
[12] K. Ramezanpour and J. Jagannath, "Intelligent zero trust architecture for 5G/6G tactical networks: Principles, challenges, and the role of machine learning,"2021, https://arxiv.org/abs/2105.01478.
[13] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," IEEE Transactions on Vehicular Technology, vol. 66, no. 12, pp. 10626–10636, 2017.
[14] C. M. Chen, B. Xiang, Y. Liu, and K. H. Wang, "A secure authentication protocol for internet of vehicles," IEEE Access, vol. 7, pp. 12047–12057, 2019.
[15] S. Mandal, D. A. Khan, and S. Jain, "Cloud-based zero trust access control policy: an approach to support work-from-home driven by COVID-19 pandemic," New Generation Computing, vol. 39, no. 3-4, pp. 599–622, 2021.
[16] S. W. Shah, N. F. Syed, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "LCDA: lightweight continuous device-to-deviceauthentication for a zero-trust architecture (ZTA)," Computers & Security, vol. 108, article 102351, 2021.
[17] N. Ghate, S. Mitani, T. Singh, and H. Ueda, "Advanced zero trust architecture for automating fine-grained access controlwith generalized attribute relation extraction," IEICE Proceedings Series, vol. 68, 2021.
[18] S. Tyagi, "7 Key Tenets of Zero Trust Architecture," Colortokens, 2021. https://colortokens.com/blog/key-tenets-zero-trustarchitecture/.
[19] R. Bernard, G. Bowsher, and R. Sullivan, "Cyber security and the unexplored threat to global health: a call for global norms," Glob. Secur. Heal. Sci. Policy, vol. 5, no. 1, 2020, doi: 10.1080/23779497.2020.1865182.
[20] V. Ngo-Lam, "Zero Trust Architecture: Best Practices for Safer Networks," Exabeamm, 2020. https://www.exabeam.com/information-security/zero-trustarchitecture/#:~:text=Forexample%2Canattackerwho,prioritizesprotectionagainstinsiderthreats.
[21] J. Petters, "What is Zero Trust? A Security Model," Inside Out Security Blog, 2021. https://www.varonis.com/blog/what-is-zerotrust.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com