



Chapter 6

The Role of AI in Zero Trust Architectures


Tushar

 <http://orcid.org/0000-0001-7190-7687>
*United College of Engineering and
Research, Prayagraj, India*


Nandita Pradhan

 <http://orcid.org/0009-0006-8819-1009>
*United College of Engineering and
Research, Prayagraj, India*


Venktesh Mishra

 <http://orcid.org/0000-0003-4476-4064>
*United College of Engineering and
Research, Prayagraj, India*


Ajay Sharma

 <http://orcid.org/0000-0002-9112-6228>
*United College of Engineering and
Research, Prayagraj, India*


Pooja Jaiswal

 <http://orcid.org/0009-0007-2507-1525>
*University of Allahabad, Prayagraj,
India*


Ajit Kumar Yadav

 <http://orcid.org/0009-0003-5607-6100>
*United College of Engineering and
Research, Prayagraj, India*


Shyam Sundar

 <http://orcid.org/0009-0007-2507-1525>
B.C.S. Prayagraj, India


Satya Prakash Singh

 <http://orcid.org/0009-0003-2406-2054>
*United College of Engineering and
Research, Prayagraj, India*


Shatrughan Mishra

 <http://orcid.org/0009-0005-7366-4275>
*United College of Engineering and
Research, Prayagraj, India*


Manish Kumar

 <http://orcid.org/0009-0007-0735-0256>
P.K. University, Shivpuri, India

Sweta Singh

 <http://orcid.org/0000-0002-7006-817X>
United University, Prayagraj, India

Shivani Mishra

 <http://orcid.org/0009-0006-0110-7039>
*United College of Engineering and
Research, Prayagraj, India*

DOI: 10.4018/979-8-3693-8397-1.ch006

Chitranjan Dwivedi

 <http://orcid.org/0009-0009-5940-7837>

*United College of Engineering and
Research, Prayagraj, India*

Bhupesh Chandra Kushwaha

*United College of Engineering and
Research, Prayagraj, India*

ABSTRACT

The rapid growth of cybersecurity risks has led organizations to build stricter frameworks, with Zero Trust Architecture (ZTA) emerging as a significant paradigm. Based on “never trust, always verify,” zero trust involves ongoing user and device identification verification, even inside the network perimeter. ZTA has a solid foundation, but cyberattacks are becoming more sophisticated, requiring more flexible solutions. AI improves ZTA by enabling real-time threat detection, behavioral analytics, and automated security event responses. A complete review of AI-powered tools and methodologies such natural language processing, anomaly detection, and predictive analytics is presented in this chapter to improve ZTA. It discusses AI implementation challenges, how AI interacts with ZTA components to improve security, and future research objectives.

1. INTRODUCTION

The zero trust architecture (ZTA) philosophy is based on the protection of resources. In such a scenario, for the sake of resource validation and authorization checks, ZTA has a goal to abolish assumed or inherited trust (attacker can only compromise a single point and then gain access) by imposing correct authentication, restricted authorizing and therefore constantly verifying stance (or trust inference) at each moment when an user or service decides to obtain a resource. In a bid to balance the advantages and disadvantages of ZTA in curbing cyber risks, we in this chapter introduce one of the potential solutions to the challenge, its opportunities, processes of implementation and constraints. Employees operated within the perimeter of security of the company. Under the ancient cybersecurity defence paradigm, technologies that would protect such a border would identify and prevent threats. However, as we all know, employees are human beings and they easily put themselves in the path of these hacks when they are not under each other protection and when they are accessing company information on their devices, said Fier. This shows how internal system services have their flaws in terms of authentication and verification, which renders the inner resources of the companies accessible to a potential black hat.

The zero trust model (ZTM) was first introduced to address some of these issues. The use case of MSRBAC is to protect resources in a fine-grained and authorized

30 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/the-role-of-ai-in-zero-trust-architectures/413290

Related Content

A Dynamically Optimized Fluctuation Smoothing Rule for Scheduling Jobs in a Wafer Fabrication Factory

Toly Chen (2011). *International Journal of Intelligent Information Technologies* (pp. 47-64).

www.irma-international.org/article/dynamically-optimized-fluctuation-smoothing-rule/60657

Applying Advisory Agents on the Semantic Web for E-Learning

Ralf Bruns, Jürgen Dunkeland Sascha Ossowski (2006). *International Journal of Intelligent Information Technologies* (pp. 40-55).

www.irma-international.org/article/applying-advisory-agents-semantic-web/2404

Social Coordination with Architecture for Ubiquitous Agents-CONSORTS

Koichi Jurumatani (2008). *Intelligent Information Technologies: Concepts, Methodologies, Tools, and Applications* (pp. 1743-1749).

www.irma-international.org/chapter/social-coordination-architecture-ubiquitous-agents/24367

Modelling of Safe Driving Assistance System for Automotive and Prediction of Accident Rates

Debraj Bhattacharjee, Prabha Bholaaand Pranab K. Dan (2019). *International Journal of Ambient Computing and Intelligence* (pp. 61-77).

www.irma-international.org/article/modelling-of-safe-driving-assistance-system-for-automotive-and-prediction-of-accident-rates/216470

Assessing the Critical Failure Factors of AI Chatbots for Research Using ISM Approach: A Case of Philippine State University Researchers

Catherine Camiguing Gabia, Dwight Gabia, Samuel C. Villa Jr., Blesie M. Villa, Nelson F. Nolon, Irene Mamitesand Melanie M. Himang (2026). *International Journal of Intelligent Information Technologies* (pp. 1-27).

www.irma-international.org/article/assessing-the-critical-failure-factors-of-ai-chatbots-for-research-using-ism-approach/402395