<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<title>Bangalie Koroma - Portfolio</title>

<link rel="stylesheet" href="styles.css">

<!-- QR Code Library -->

<script src="https://cdnjs.cloudflare.com/ajax/libs/qrcodejs/1.0.0/qrcode.min.js"></script>

<!-- Animate.css for animations -->

<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/4.1.1/animate.min.css">

</head>

<body>

<!-- Background Logo -->

<div class="background-logo"></div>

<!-- Navigation -->

<nav>

<ul>

<li><a href="#home">Home</a></li>

<li><a href="#about">About</a></li>

<li><a href="#projects">Projects</a></li>

<li><a href="#resume">Resume</a></li>

<li><a href="#contact">Contact</a></li>

</ul>

</nav>

<!-- Main Content Container -->

<div class="main-container">

<!-- Home Section -->

<section id="home" class="section">

<h1 class="welcome-message animate\_\_animated animate\_\_fadeInDown">Hi, I'm Bangalie Koroma</h1>

<p class="welcome-subtext animate\_\_animated animate\_\_fadeInUp">Cyber Analyst & Intrusion Detection Specialist</p>

<p class="welcome-quote animate\_\_animated animate\_\_fadeIn">Protecting systems, detecting threats, and securing digital environments</p>

<img src="https://scontent-iad3-2.xx.fbcdn.net/v/t39.30808-6/470142439\_17986487591758820\_2559798136472926039\_n.jpg?\_nc\_cat=109&ccb=1-7&\_nc\_sid=127cfc&\_nc\_ohc=TJG0dadzFJYQ7kNvgH80VQv&\_nc\_oc=Adj7DVsq2VAZKMJWD34No8uuZzcEGWajXfC5DKMyhr7goGcu1NdCqYoSjPsK77Dk5kg&\_nc\_zt=23&\_nc\_ht=scontent-iad3-2.xx&\_nc\_gid=ADuU7BsxPpl6\_IOkJqZx9o-&oh=00\_AYFvEDXwYL-\_GQoq5n61MuZo3hhWLmp9U-UHa2\_4nmWZLA&oe=67D004A5" width="500px" alt="Bangalie Koroma" class="profile-image animate\_\_animated animate\_\_zoomIn">

<div id="qrcode" class="animate\_\_animated animate\_\_fadeIn"></div>

</section>

<!-- About Section -->

<section id="about" class="section">

<h2>About Me</h2>

<p>As a dedicated Cyber Analyst and soon-to-be graduate, I specialize in identifying vulnerabilities, mitigating risks, and fortifying digital systems against ever-evolving cyber threats. With hands-on experience in intrusion detection, threat analysis, and risk management, I am passionate about staying ahead of emerging security challenges. My goal is to apply my knowledge and skills to help organizations strengthen their cybersecurity posture, protect critical data, and build resilient digital infrastructures. I look forward to contributing to a team where I can make a meaningful impact in securing the digital world.</p>

<div class="content">

<h3>Skills</h3>

<ul>

<li>Intrusion Detection & Prevention (IDS/IPS, SIEM tools)</li>

<li>Vulnerability Assessment and Penetration Testing</li>

<li>Incident Response & Threat Hunting</li>

<li>Security Information and Event Management (SIEM)</li>

<li>Risk Assessment & Mitigation Strategies</li>

<li>Firewall Configuration & Management</li>

<li>Endpoint Security & Malware Analysis</li>

<li>Zero Trust Architecture Implementation</li>

<li>Security Policies & Compliance (NIST, ISO 27001, SOC 2, GDPR)</li>

<li>Cryptography & Data Protection</li>

<li>Python & Scripting for Automation (Bash, PowerShell)</li>

<li>Machine Learning in Cybersecurity</li>

</ul>

<h3>Soft Skills:</h3>

<ul>

<li>Critical Thinking & Problem-Solving</li>

<li>Analytical & Investigative Mindset</li>

<li>Effective Communication (Technical & Non-Technical Audiences)</li>

<li>Collaboration & Teamwork</li>

<li>Adaptability to Emerging Threats</li>

<li>Strong Ethical Judgment & Confidentiality Awareness</li>

</ul>

<h3>Education</h3>

<div class="education">

<p><h5><ul>

<li>Bowie State University, Bowie, MD</li>

<li>Bachelor of Science in Health Technology and Cybersecurity (Expected May 2025)</li>

</ul></h5></p>

</div>

</div>

</section>

<!-- Projects Section -->

<section id="projects" class="section">

<h2>My Projects</h2>

<div class="project-grid">

<div class="project">

<h3>Project 1</h3>

<h3>Protection of Sensitive Data with Zero Trust Model and Machine Learning</h3>

<h4>Abstract</h4>

<p>The increasing sophistication of cyberattacks and insider threats has highlighted the limitations of traditional security approaches in protecting sensitive data. This research explores the integration of the Zero Trust Model and Machine Learning (ML) to fortify data protection mechanisms. Zero Trust enforces strict access controls and assumes breach scenarios, while ML provides advanced analytics and automation to detect and mitigate threats. This paper examines the principles, applications, challenges, and future potential of combining these technologies, offering insights into their transformative role in cybersecurity.</p>

<h4>Introduction</h4>

<p>Organizations today face an escalating threat landscape where sensitive data is at constant risk of breaches. Conventional "castle-and-moat" security models, which trust users and devices within the network perimeter, are inadequate in the face of modern attack methods, including phishing, ransomware, and insider threats (Smith & Jones, 2021). The Zero Trust Model, a paradigm that eliminates implicit trust, provides a robust framework for securing sensitive data. By integrating Machine Learning (ML), Zero Trust can dynamically adapt to emerging threats and ensure continuous protection (Brown et al., 2022).</p>

<p>This paper investigates the principles of Zero Trust, the applications of ML in enhancing its effectiveness, and the challenges in implementing these technologies. It also discusses potential future developments and best practices.</p>

<h4>The Zero Trust Model</h4>

<p>The Zero Trust Model operates on the principle of "never trust, always verify," ensuring that no user or device, whether inside or outside the network, is granted access without explicit verification (Krause, 2020). Key tenets of Zero Trust include:</p>

<p>Verify Explicitly: Authenticate and authorize every access request using factors such as identity, device, and location.</p>

<p>Least Privilege Access: Restrict access rights to the minimum necessary for users and devices to perform their roles.</p>

<p>Assume Breach: Continuously monitor and analyze network activity to identify potential breaches.</p>

<p>The model significantly reduces the attack surface and enhances compliance with data protection regulations like the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) (Davis, 2021).</p>

<h3>Role of Machine Learning in Zero Trust</h3>

<p>Machine Learning augments the Zero Trust Model by enabling data-driven decisions, automating responses, and improving threat detection. ML algorithms analyze vast datasets to uncover anomalies and predict risks, enhancing the model's efficacy (Chen & Patel, 2022).</p>

<h4>Applications of ML in Zero Trust</h4>

<p>Behavioral Analytics: ML models learn patterns of user and device behavior to detect anomalies, such as unusual login locations or times, which may indicate compromised accounts (Singh et al., 2021).</p>

<p>Dynamic Access Control: Access permissions are dynamically adjusted based on context, such as device trustworthiness, location, and activity, reducing the risk of unauthorized access (Brown et al., 2022).</p>

<p>Threat Detection: ML identifies threats like phishing or malware by recognizing patterns in network traffic and application usage, often flagging attacks before they execute (Krause, 2020).</p>

<p>Automated Incident Response: Using predictive models, ML can isolate compromised devices or revoke access rights automatically, minimizing damage and response time (Davis, 2021).</p>

<p>Data Classification and Encryption: ML helps classify sensitive data (e.g., personal identifiable information) and apply appropriate encryption or access policies (Smith & Jones, 2021).</p>

<h4>Challenges in Implementation</h4>

<p>Despite its advantages, integrating ML with Zero Trust poses challenges:</p>

<P>Complexity: Implementing Zero Trust with ML requires reengineering existing infrastructure and integrating multiple technologies (Chen & Patel, 2022).</P>

<p>False Positives: ML models can mistakenly identify legitimate actions as threats, disrupting workflows and increasing administrative overhead (Singh et al., 2021).</P>

<p>Resource Intensity: Training and deploying ML algorithms require significant computational resources and expertise (Davis, 2021).</P>

<p>Evolving Threats: Adversaries continuously adapt, creating new attack vectors that may bypass ML defenses (Brown et al., 2022).</P>

<h4>Case Study: Zero Trust and ML in Action</h4>

<p>A multinational financial institution faced challenges in preventing unauthorized access to customer data. By implementing a Zero Trust framework augmented with ML-driven behavioral analytics, the organization achieved:</p>

<p>Anomaly Detection: Identified suspicious login attempts from untrusted devices.</p>

<p>Dynamic Policies: Automatically adjusted access controls based on user location and device status.</p>

<p>Improved Incident Response: Reduced response time to potential breaches by 60%.</p>

<p>This approach enhanced data protection and compliance with financial regulations (Smith & Jones, 2021).</p>

<h4>Future Directions</h4>

<p>The integration of advanced ML techniques, such as reinforcement learning and federated learning, holds promise for improving the Zero Trust Model. These methods can:</p>

<p>Enhance Adaptability: ML models can continuously update themselves based on new threats, improving predictive accuracy.</p>

<p>Preserve Privacy: Federated learning enables training ML models across distributed datasets without sharing sensitive data.</p>

<p>Proactive Threat Prevention: Advanced algorithms can simulate attack scenarios to identify vulnerabilities before exploitation.</p>

<h4>Conclusion</h4>

<p>The convergence of the Zero Trust Model and Machine Learning represents a transformative approach to protecting sensitive data. While challenges such as complexity and resource requirements persist, the benefits of enhanced threat detection, automated responses, and dynamic access control are undeniable. Organizations adopting these technologies can significantly improve their cybersecurity posture and resilience against evolving threats. Future research should focus on overcoming implementation barriers and exploring new ML techniques to further strengthen Zero Trust frameworks.</p>

<h4>References</h4>

<p>Brown, T., Chen, Y., & Patel, S. (2022). Advancing cybersecurity: The role of machine learning in Zero Trust frameworks. Journal of Cyber Defense, 35(2), 123–135.</p>

<p>Chen, Y., & Patel, S. (2022). Dynamic access control in Zero Trust architectures using machine learning. Cybersecurity Advances, 10(4), 89–101.</p>

<p>Davis, M. (2021). Zero Trust implementation challenges and solutions. Information Security Review, 28(1), 45–58.</p>

<p>Krause, R. (2020). Zero Trust: A paradigm shift in enterprise security. Enterprise Cybersecurity Journal, 12(3), 34–50.</p>

<p>Singh, A., Smith, J., & Jones, L. (2021). Machine learning for anomaly detection in network security. International Journal of Cyber Analytics, 7(2), 56–70.</p>

<p>Smith, J., & Jones, L. (2021). Protecting sensitive data with Zero Trust frameworks. Data Security Journal, 14(4), 98–115.</p>

</div>

</section>

<!-- Resume Section -->

<section id="resume" class="section">

<h2>Resume</h2>

<p>Download my resume to learn more about my experience and certifications.</p>

<!-- Resume Section -->

<section id="resume" class="section">

<h2>Resume</h2>

<p>

<h2>BANGALIE KOROMA</h2>

<br><hr>

<h4>7773 Riverdale RD New Carrollton MD 20784 | (240)-883-1099 | bangaliekoroma.bk@gmail.com | <a href="https://github.com/bkoroma">github.com</a> | <a href="https://www.linkedin.com/in/bangalie-koroma-4a762b335/">linkedin.com</a></h4>

<hr>

<h5>Dedicated and results-driven Cybersecurity Engineer with a strong background in health technology and IT security. I am currently pursuing a Bachelor of Science in Health Technology and Cybersecurity at Bowie State University, with hands-on experience in vulnerability assessment, risk mitigation, and IT management. Passionate about developing secure architectures, mitigating cyber risks, and strengthening defenses against emerging threats.</h5>

<hr>

<h5><br>EDUCATION</h5>

<h5><ul>

<li>Bowie State University, Bowie, MD</li>

<li>Bachelor of Science in Health Technology and Cybersecurity (Expected May 2025)</li>

<li>GPA: 3.4</li>

</ul></h5>

<hr>

<h2><br>CERTIFICATIONS</h2>

<ul>

<li>CompTIA Security+ (Completed)</li>

<li>CompTIA CYSA+ (Completed)</li>

</ul>

<hr>

<h2><br>Relevant Coursework:</h2>

<ul>

<li>Client Operating Systems</li>

<li>Network Protocols (TCP/IP)</li>

<li>Server Administration II</li>

<li>Internet Technology</li>

<li>UNIX System Administration</li>

<li>Advanced Secure Coding with Java</li>

<li>Cryptography & Applications</li>

<li>Intrusion Detection & Prevention</li>

<li>Software & Operating System Security</li>

<li>Python</li>

</ul>

<hr>

<h2>EXPERIENCE</h2>

<h4>Yescare LLC</h4>

<h5>Medication Technician & Medical Records Technician | 5+ Years</h5>

<h5>Prince George’s County Dept. of Corrections, Upper Marlboro, MD</h5>

<ul>

<li>Managed and secured medical records while ensuring compliance with HIPAA regulations.</li>

<li>Administered medications while maintaining strict confidentiality and accuracy.</li>

<li>Assisted in data entry and management of health records within secure systems.</li>

</ul>

<h2>Family Services Foundation</h2>

<h5>Client Direct Services Provider | 5+ Years</h5>

<h5>New Carrollton, MD</h5>

<ul>

<li>Provided direct client support while maintaining secure documentation and case files.</li>

<li>Ensured compliance with data privacy regulations in handling sensitive client information.</li>

<li>Worked collaboratively with healthcare professionals to improve data security in client services.</li>

</ul>

<hr>

<h2>TECHNICAL SKILLS</h2>

<ul>

<li>Security & Risk Management: Vulnerability Assessment, Risk Mitigation, Intrusion Detection</li>

<li>Operating Systems: Windows, Linux/UNIX</li>

<li>Programming & Scripting: Python, Java (Secure Coding)</li>

<li>Networking & Protocols: TCP/IP, Firewalls, VPNs</li>

<li>Cybersecurity Tools: SIEM, IDS/IPS, OWASP ZAP</li>

<li>Data Protection: Encryption, Access Control, Incident Response</li>

</ul>

<hr>

<h2>ADDITIONAL INFORMATION</h2>

<ul>

<li>Availability: Open to internships, part-time, or full-time opportunities in Cybersecurity & IT Security.</li>

<li>Languages: English</li>

<li>Professional Interests: Cyber Threat Intelligence, Incident Response, Cyber Analyst</li>

</ul>

</p>

<a href="resume.pdf" download class="download-btn">Download Resume</a>

</section>

<!-- Contact Section -->

<section id="contact" class="section">

<h2>Contact Me</h2>

<form id="contactForm">

<input type="text" placeholder="Name" required>

<input type="email" placeholder="Email" required>

<textarea placeholder="Message" required></textarea>

<button type="submit">Send</button>

</form>

</section>

</div>

<!-- Chatbot Widget -->

<div class="chatbot">

<div class="chat-icon" aria-label="Open Chatbot">💬</div>

<div class="chat-window">

<div class="chat-header">

<h3>Chat with Me</h3>

<button class="close-btn">×</button>

</div>

<div class="chat-messages"></div>

<div class="chat-input-container">

<input type="text" placeholder="Ask me something..." id="chatInput" aria-label="Ask a question">

<button id="voiceButton" aria-label="Start Voice Recognition">🎤</button>

</div>

</div>

</div>

<!-- Weather Widget -->

<div class="weather-widget" aria-labelledby="weather-widget">

<input type="text" id="cityInput" placeholder="Enter city name" aria-label="City name input">

<button id="weatherButton" aria-label="Get weather">Get Weather</button>

<div id="weatherResult" aria-live="polite"></div>

</div>

<script src="script.js"></script>

</body>

</html>