Self-Learning Assessment Report (MOOC)

Student Information
● Name: pranav shewale
● Roll No.: 47
● Branch / Semester: CYSE / SEM 5
● Email ID: pranav.17928@sakec.ac.in

Stage 1: Activity 1 – Article Writing

Chosen Topic: Future of Cyber Crime Investigation with Quantum Computing
Article Summary (300–400 words):
The article "Future of Cyber Crime Investigation with Quantum Computing" explores how the
revolutionary power of quantum computing is set to transform the landscape of cyber crime
investigation and digital forensics. With cyber threats growing more complex—ranging from
ransomware and identity theft to cryptocurrency-related crimes—traditional computing
systems
often struggle to analyze massive datasets or decrypt sophisticated encryption schemes.
Quantum
computing, based on the principles of quantum mechanics, introduces a new paradigm
capable of
addressing these challenges through unparalleled computational speed and precision.
The article begins by explaining the basic principles of quantum computing, such as
superposition and entanglement, which allow quantum bits (qubits) to perform multiple
calculations simultaneously. This fundamental difference gives quantum computers a
significant
advantage over classical systems, particularly in solving cryptographic and analytical
problems
that are currently considered infeasible.
It then highlights the key roles of quantum computing in cyber crime investigation, including
accelerated data analysis, faster decryption of encrypted evidence, enhanced machine
learning
capabilities, and the development of quantum cryptography methods such as Quantum Key
Distribution (QKD) for secure communications. Quantum-enhanced AI can process vast
forensic
data, detect anomalies, and predict cyber threats more effectively. Additionally, investigators
could use quantum algorithms to trace blockchain transactions or reconstruct corrupted
digitalevidence.
The article also addresses real-world implications and challenges such as high
implementation
costs, limited availability of quantum hardware, and ethical concerns surrounding the
potential
misuse of decryption power. Despite these obstacles, global research in quantum-safe
cryptography and quantum forensic tools is rapidly advancing.
In conclusion, the article emphasizes that quantum computing represents the next major
leap in
digital forensics and cybersecurity. As the technology matures, it will empower investigators

with tools capable of uncovering cybercrimes faster and more accurately than ever before. The
integration of quantum computing into cyber crime investigation promises a future where digital
security, privacy, and justice are stronger, smarter, and more resilient.