INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 11, Issue 1 - V11I1-1558)
Available online at: https://www.ijariit.com

LogiX: AI-Driven Secure Login System with Quantum-Resistant Algorithms and Multi-Factor Authentication

Dr. M.K. Jayanthi Kannan
jayanthi.m@vitbhopal.ac.in
Professor, School of Computing Science Engineering and Artificial Intelligence, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh – 466114.

Abir Barman
abir.24mca10154@vitbhopal.ac.in
PG Student School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh – 466114

Anjali Yadav
anjali.24mca10067@vitbhopal.ac.in
PG Student School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh – 466114

Samikshya Pruseth
samikshya.24mca10126@vitbhopal.ac.in
PG Student School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh – 466114

Santosini Sahu
santosini.24mca10133@vitbhopal.ac.in
PG Student School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh – 466114

ABSTRACT

LogiX is a next-generation authentication and security framework designed to withstand emerging cybersecurity threats, including those posed by quantum computing. The system integrates Post-Quantum Cryptographic Algorithms such as Kyber for Key Exchange, Dilithium for Digital Signatures, and NTRU For Encryption To Ensure Robust Data Protection. Additionally, Advanced AI-driven techniques are Employed for Anomaly Detection, Credential Sharing Analysis, Adaptive Multi-Factor Authentication (MFA), and Phishing De-Detection. By leveraging secure authentication protocols, quantum-resistant cryptographic standards, and intelligent monitoring systems, LogiX provides a comprehensive security solution that mitigates risks associated with traditional and quantum-era cyber threats. This documentation outlines the foundational principles, methodologies, and implementation strategies used to fortify authentication mechanisms and protect sensitive user data in cloud-based environments.

Keywords: *Security Framework, Cybersecurity Threats, Kyber for Key Exchange, Dilithium for Digital Signatures, NTRU For Encryption, Post-Quantum Cryptographic Algorithms.*

INTRODUCTION

In today's rapidly evolving digital landscape, cybersecurity has become a critical concern for organizations and individuals alike. Traditional security measures, which have served well in the classical computing era, are now facing growing vulnerabilities due to the rapid advancements in quantum computing. Quantum computers have the potential to break widely used cryptographic algorithms such as RSA, ECC (Elliptic Curve Cryptography), and DSA, which form the backbone of modern encryption schemes. This raises the urgent need for quantum-proof security frameworks capable of safeguarding sensitive information against both classical and quantum-era threats. LogiX is designed as a next-generation security solution that addresses this challenge by integrating quantum-resistant cryptographic algorithms and AI-powered security measures. It is specifically built to future-proof authentication systems and secure sensitive data in an environment where quantum computing could soon become a practical reality. By leveraging the power of post-quantum cryptography (PQC), LogiX provides robust defense mechanisms against quantum attacks while maintaining compatibility with existing systems.

DOMAIN ANALYSIS

At the heart of LogiX's cryptographic foundation are lattice-based cryptographic algorithms like Kyber for secure key exchange and NTRU for encryption, both of which are resistant to quantum attacks.

These algorithms are paired with Dilithium, a post-quantum digital signature scheme that ensures the integrity and authenticity of data. This combination of quantum-resistant encryption techniques allows LogiX to deliver secure communication channels that can withstand the growing power of quantum computing, offering peace of mind for users and businesses alike. In addition to quantum-resistant encryption, LogiX incorporates advanced AI-powered tools that enhance security beyond traditional methods. The system uses machine learning models to detect unusual login patterns, monitor credential sharing, and assess the risk of user actions in real-time. By implementing adaptive multi-factor authentication (MFA), LogiX provides an extra layer of defense by dynamically adjusting security measures based on AI-calculated risk scores. This enables the system to respond quickly and appropriately to emerging threats, ensuring a proactive defense rather than a reactive one. The platform also focuses on data protection across multiple clouds, ensuring that sensitive information remains secure whether stored on-premises or in the cloud. With quantum-safe key management systems (KMS) and lattice-based encryption schemes like FrodoKEM, LogiX ensures that all stored data, even in multi-cloud environments, remains protected against both classical and quantum attacks. Additionally, LogiX's use of quantum-safe random number generators and secure session management strategies fortify session security, minimizing the risks of session hijacking or other attacks. This documentation outlines the core principles, technologies, and methodologies behind LogiX. By integrating quantum-resistant algorithms with AI-driven security measures, LogiX not only protects against today's cyber threats but also provides long-term protection against the potential risks posed by quantum computing. This innovative approach ensures that LogiX can adapt to an increasingly complex cybersecurity landscape, making it an invaluable tool for organizations and individuals looking to secure their digital identities and sensitive data in the quantum-enabled future.

Quantum Computing Concepts In Logix: Ai-Driven Secure Login

Quantum computing, using quantum bits, is expected to completely transform the logistics sector. Compared to conventional desktop computers and supercomputers, which rely on binary values, quantum computers are more powerful, safer and , quicker. It can compute all pathways at once and report back the right route has been determined. Dynamic route optimization and other real-time dynamic supply chain activities are intended to be enhanced by this technology. The first optimization of traffic pilot project, which involved Volkswagen and Carris, quantum computers were utilized to choose the quickest bus route spanning 26 stops in Lisbon, Portugal. Also, quantum computing could speed up operating procedures, enhancing the number of parcels that could be packed simultaneously during global freight transportation.

In an age where information is the new currency, the security of data has become one of the most critical challenges of our time. Classical cryptographic methods—those that have safeguarded digital communications for decades—are now facing an unprecedented threat. The advent of quantum computing promises not only revolutionary advancements in technology but also a profound disruption in the very foundations of cryptography. As quantum computers evolve, they are predicted to be capable of breaking many of the cryptographic systems that currently protect our data, transactions, and communications. Beyond Classical: Exploring Post-Quantum Cryptography delves into this emerging field that seeks to counter the quantum threat. This book is designed to guide readers through the complexities of post-quantum cryptography (PQC), a discipline that is rapidly becoming essential for the future of secure digital interactions. The rise of quantum cryptography as a groundbreaking approach to securing data beyond classical means. By harnessing the principles of quantum mechanics, quantum cryptography promises unparalleled levels of security, making it virtually impossible for adversaries to intercept or manipulate data without detection. The article delves into the fundamentals of quantum cryptography, its applications, challenges, and future prospects.

LITERATURE REVIEW OF EXISTING SYSTEMS

Table 1: The Comparative Study of AI-Driven Secure Login System Literature Review

SL. No.	Study	Objective	Techniques Used	Datasets
1	An enhanced approach of the k-means clustering system	Optimization of Clustering, Comparative Efficiency, Dataset Evaluation	K-means Clustering, Caliniski-Harabasz (CH) Indicator	NSL-KDD, CICIDS2017
2	Enhanced Unsupervised Anomaly-Based Intrusion Detection System Using K-means Clustering Optimized by CaliniskiHarabasz Indicator	Enhance Anomaly Detection, Optimize Clustering Performance, Evaluate Mod Performance	K-means Clustering, Caliniski-Harabasz (CH) Indicator	NSL-KDD
3	An Adaptive Approach Towards the Selection of Multi-Factor Authentication	Design an adaptive multi-factor authentication system, improve security, and Enhance user experience	Behavioral Analytics, Risk-Based Authentication (RBA), Machine Learning Models	User login data
4	Raspberry Pi-Based Intrusion Detection System Using K-Means Clustering Algorithm	Develop efficient anomaly-based intrusion detection system, Improve the accuracy of anomaly detection	K-Means Clustering, Raspberry Pi, Python	Network traffic data
5	Password Strength Checker Using Machine Learning	Assess password strength, Categorize passwords into weak, medium, and strong	KNN, Decision Tree, SVM, Random Forest	Kaggle dataset (100,000 passwords)

6	An Improved Network Intrusion Detection Technique Based on k-Means Clustering via Naïve Bayes Classification	Detect novel network intrusions, Compared with Naïve Bayes classification	K-means Clustering, Naïve Bayes Classification	KDD Cup '99 Dataset
7	Argon2: New Generation of Memory-Hard Functions for Password Hashing and Other Applications	Introduce Argon2 for password hashing, Address time-memory trade-offs	Argon2, Blake2b Hash Function	N/A
8	Secure Hashing using BCrypt for Cryptographic Applications	Demonstrate BCrypt for secure password storage, Compared with SHA-256 and MD5	BCrypt, SHA-256, MD5	N/A
9	Beyond the Limits: SHA-3 in Just 49 Slices	Implement compact SHA-3 on FPGA, improve throughput, Reduce area	SHA-3, FPGA	N/A
10	Implementing and proving the TLS 1.3 Record Layer	Verify TLS 1.3 record layer implementation, Address vulnerabilities in prior versions	TLS 1.3, F-Star Programming Language	N/A
11	Lattice-Based Cryptography and NTRU: Quantum-Resistant Encryption Algorithms	Explore quantum-resistant cryptographic algorithms, Analyze NTRU, Kyber, and Ring-Lizard	Lattice-based Cryptography, NTRU, Kyber, Ring-Lizard	N/A
12	Quantum-Resistant TLS 1.3: A Hybrid Solution Combining Classical, Quantum, and Post-Quantum Cryptography	Integrate quantum-resistant methods into TLS 1.3, Enhance resilience	TLS 1.3, Kyber, Dilithium, Quantum Key Distribution (QKD)	N/A
13	KaLi: A Crystal for Post-Quantum Security Using Kyber and Dilithium	Design a unified cryptoprocessor for post-quantum security	Kyber, Dilithium, FPGA, ASIC	N/A

Table 1 provides an overview of existing systems related to LogiX, focusing on advancements in intrusion detection, multi-factor authentication (MFA), password security, and quantum-resistant cryptography. Several studies highlight the use of unsupervised machine learning techniques, such as K means clustering, for anomaly detection in network traffic. While these methods demonstrate strong performance in identifying attack vectors, challenges in scalability and feature selection remain, particularly in large datasets. In the field of multi-factor authentication, adaptive systems leveraging behavioral analytics and risk-based authentication have been shown to enhance both security and user experience. However, issues related to data privacy and model accuracy must be addressed for broader implementation. Cryptographic algorithms like Argon2 and BCrypt are widely used for secure password hashing, offering significant resistance to brute-force and rainbow table attacks. Despite their effectiveness, these algorithms face performance challenges, particularly in resource-constrained environments. As quantum computing progresses, the need for quantum-resistant cryptographic methods is becoming increasingly critical. Lattice-based encryption algorithms such as Kyber and NTRU 2 offer robust defense mechanisms against quantum threats, though their adoption is hindered by implementation complexities and side-channel vulnerabilities. Overall, the reviewed systems provide important insights into the technologies currently available but also underline the limitations that LogiX seeks to overcome, especially in terms of scalability, real-time processing, and quantum resistance.

PROPOSED SYSTEM DESIGN

The LogiX system design is structured to integrate cutting-edge quantum-resistant cryptographic algorithms with advanced AI-driven security mechanisms, forming a robust framework capable of securing sensitive data and user authentication processes. The proposed architecture leverages a combination of lattice-based encryption, machine learning models, and dynamic multi-factor authentication (MFA) to ensure a comprehensive security solution that addresses both current and future cybersecurity threats, including those posed by quantum computing. At the core of LogiX is the use of quantum-resistant cryptographic methods to protect data confidentiality and integrity. For key exchange, the system adopts Kyber, a lattice-based algorithm that ensures secure key distribution resistant to quantum attacks. NTRU, another lattice-based encryption algorithm, is used to secure data, providing encryption that can withstand the computational power of quantum computers. Dilithium, a lattice-based digital signature scheme, is employed to verify the authenticity of messages, ensuring data integrity.

These quantum-resistant algorithms are further integrated with TLS 1.3 to provide secure communication, incorporating a hybrid cryptographic approach that combines classical and post-quantum cryptography. In parallel, LogiX incorporates AI-driven security mechanisms designed to enhance the system's ability to detect and respond to threats in real time. Anomaly detection is performed using machine learning models such as Isolation Forest and K-Means clustering, which continuously monitor network traffic and user behaviors for suspicious activities. Additionally, adaptive MFA is employed, where the system dynamically selects the appropriate authentication factors based on the risk level of each access attempt. This AI-powered approach optimizes both security and user experience by adapting the authentication process according to the context of the access request. The user authentication and data protection components of LogiX are built on the principles of secure password storage and data encryption. Argon2 and BCrypt are utilized to securely hash passwords, ensuring that user credentials are protected against brute-force attacks.
The system provides real-time feedback to users during account creation, helping them choose stronger passwords by classifying password strength into categories like weak, medium, and strong. Furthermore, all data exchanged between users and systems is encrypted using NTRU for data protection, while TLS 1.3 ensures secure communication channels.

The LogiX system is designed with efficiency and scalability in mind, ensuring that it can handle large volumes of data while maintaining low latency, especially in real-time applications. The use of optimized algorithms and parallel processing ensures that the system performs well even under heavy loads. Additionally, LogiX is future-proofed against quantum computing threats, leveraging post-quantum cryptographic standards to ensure the security of sensitive data in the long term. Finally, LogiX is developed to integrate seamlessly with existing infrastructures, allowing organizations to adopt quantum-resistant security measures without overhauling their current systems. This integration is achieved by ensuring compatibility with popular programming frameworks and cryptographic libraries, making the transition to quantum-safe security measures smooth and efficient. Overall, the LogiX system design represents a scalable, adaptive, and future-ready solution for securing user data and authentication in a quantum-enabled world.

Proposed System Design

The proposed system, Logix, is designed to be a highly secure, future-proof login system capable of withstanding both classical and quantum-based cyber threats. It integrates modern cryptographic techniques, machine learning models, and multi-layered security protocols to ensure robust protection against attacks while maintaining a smooth user experience. The core design revolves around quantum-resistant algorithms for password and data encryption, using schemes like Kyber and Dilithium for key exchange and digital signatures. These algorithms safeguard sensitive user credentials and data, even in the face of potential quantum attacks. The system employs AES-256 for immediate encryption needs and gradually transitions to post-quantum encryption standards as they evolve.

To strengthen authentication, the system incorporates multi-factor authentication (MFA) mechanisms, including hash-based OTPs and physical security keys, which further enhance resistance to phishing and brute-force attacks. API security is ensured through quantum-safe JWTs, replacing traditional RSA signatures with SPHINCS+ to prevent forgery, and lattice-based alternatives for secure key exchanges. The AI-powered module continuously analyzes login patterns using algorithms like Isolation Forest and K-Means clustering for anomaly detection and credential-sharing detection. These models flag suspicious behaviors, such as logins from unusual locations or devices, dynamically triggering adaptive MFA or alerting administrators. Additionally, an AI-driven password strength checker provides real-time feedback to users, guiding them toward stronger, more resilient passwords. Logix also implements secure session management with TLS 1.3 and quantum-safe random number generation, ensuring session IDs cannot be easily compromised. The system logs activities using SHA-3 or Kangaroo Twelve hashing, preserving log integrity even under advanced attack scenarios. Data distributed across multiple cloud platforms is encrypted using lattice-based schemes, with key management systems transitioning to post-quantum standards as cloud providers upgrade their infrastructure. By continuously monitoring NIST recommendations and industry advancements, Logix remains adaptable, regularly updating cryptographic libraries and AI models to keep pace with emerging threats. This comprehensive design ensures that Logix is not just a secure login system for today but a resilient platform capable of evolving with the future of cybersecurity.

ARCHITECTURE DIAGRAM

The proposed LogiX AI-Driven Secure Login System with Quantum-Resistant Algorithms and Multi-Factor Authentication, system is illustrated in the following Figure-1 of Architecture Diagram, and Algorithms Used

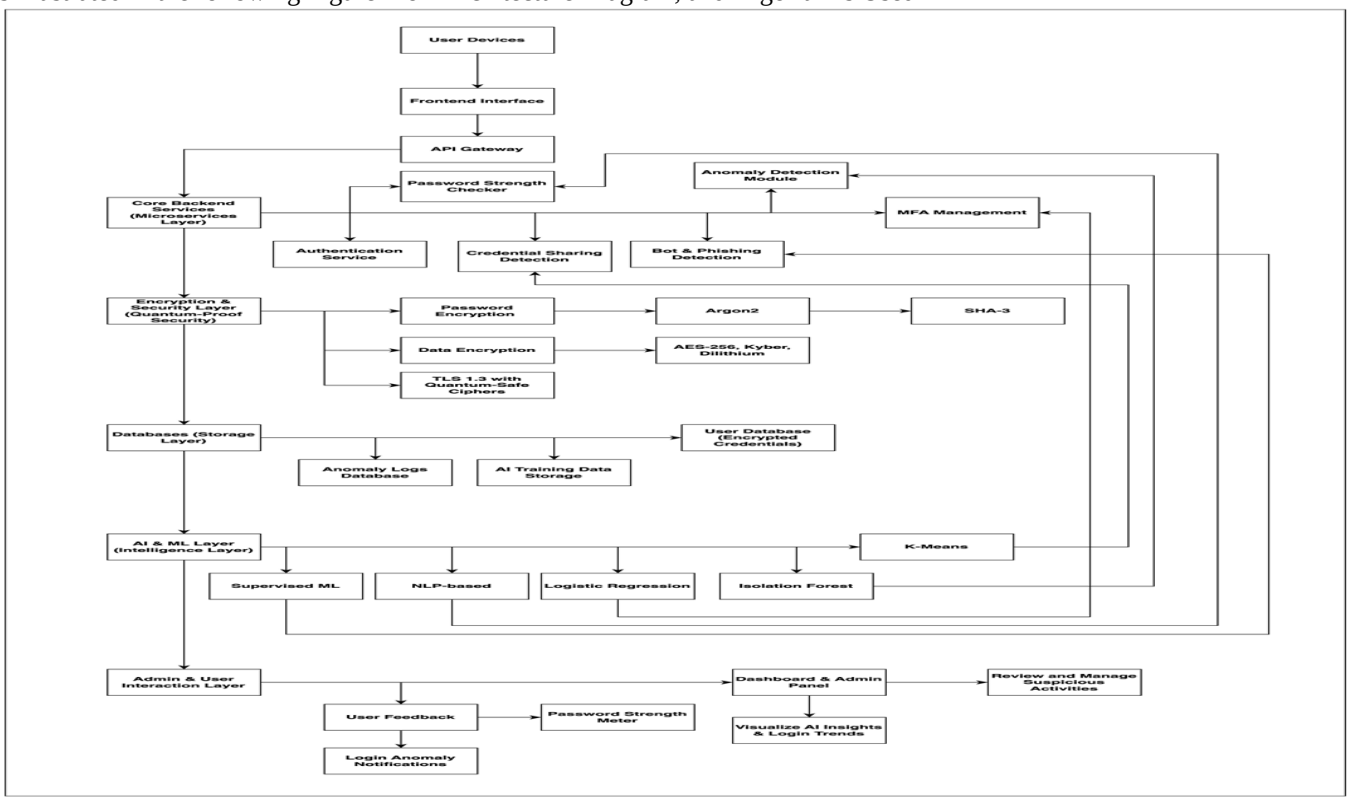


Figure 1: Architecture Diagram LogiX AI-Driven Secure Login System with Quantum-Resistant Algorithmic Methodology

Encryption and Quantum-Resistant Security

To safeguard credentials and user data, Logix employs robust encryption algorithms. Passwords are hashed using Argon2 or bcrypt, with plans to transition to SHA-3 for quantum resilience. Data encryption relies on AES-256 for current protection, with lattice-based schemes like Kyber and Dilithium being adopted for secure key exchange and digital signatures.

API communications are secured with TLS 1.3, with a roadmap for integrating quantum-safe cipher suites. Additionally, JSON Web Tokens (JWT) are used for session management, replacing traditional signing methods with SPHINCS+ for post-quantum security. Methodology and Algorithms used The Logix system is designed with a multi-layered approach, integrating quantum-resistant cryptography, AI-driven anomaly detection, and advanced security mechanisms to create a future-proof login system. The methodology focuses on building a secure, adaptive, and intelligent authentication platform, leveraging state-of-the-art cryptographic algorithms and machine learning models to detect threats, enhance user experience, and protect sensitive data.

Multi-Factor Authentication (MFA)

To add an extra layer of protection, Logix supports MFA using OTPs and physical security keys. For quantum-safe authentication, hash-based one-time passwords (HOTP) utilizing SHA-3 ensure resilience against quantum decryption attempts. Adaptive MFA is implemented through machine learning models, dynamically triggering additional verification based on login risk scores. AI-Powered Threat Detection: Logix incorporates various AI and machine learning models to enhance security intelligence. Credential sharing is detected through K-Means clustering, identifying patterns in login behavior across devices and locations. Anomaly detection is handled by Isolation Forest algorithms, flagging suspicious activities based on deviations from normal user behavior. Logistic Regression models assess login risk and dynamically adjust security measures, while supervised learning models identify bot and phishing attempts through behavioral analysis.

Secure Session Management and Logging

Session management relies on quantum-safe random number generators, with session identifiers and logs hashed using SHA-3 or KangarooTwelve for integrity. Activity logs are continuously monitored for suspicious patterns, with AI models trained to detect and alert administrators of unusual access attempts. Continuous Learning and Adaptation, Logix is designed to evolve with emerging threats. The AI models are periodically retrained with new login data, and the system continuously monitors advancements in post-quantum cryptography. By integrating libraries like OpenQuantumSafe (liboqs), Logix ensures it stays aligned with the latest NIST recommendations for quantum-resistant algorithms. This methodology ensures Logix is not only secure against current threats but is also prepared for the next generation of cyberattacks. The combination of advanced cryptography, AI-driven insights, and continuous adaptation makes Logix a cutting-edge solution for secure, future-proof authentication systems.

Project Functional Modules Implementation

The Logix system is designed as a comprehensive, modular authentication platform that integrates advanced cryptographic techniques, AI-driven security measures, and adaptive access control mechanisms. Each functional module is carefully crafted to work in harmony, ensuring a robust and future-proof login system. Let's break down the core functional modules and their implementation. Password Encryption and Data Security, Logix implements password encryption using Argon2 or bcrypt for secure password hashing, with added salting to resist brute-force and collision attacks. To future-proof against quantum threats, the system is designed to transition to SHA-3 hashing and lattice-based encryption algorithms like Kyber for key exchanges. Sensitive user data is encrypted with AES-256 while in storage, and TLS 1.3 secures data in transit, with plans to adopt post-quantum cryptographic libraries as they become standardized. Multi-Factor Authentication (MFA), The MFA module adds an additional layer of security by requiring users to verify their identity through one-time passwords (OTPs) or hardware security keys (e.g., YubiKey). The system supports hash-based one-time passwords (HOTP) for quantum resistance, relying on SHA-3 for integrity. AI-powered adaptive MFA dynamically assesses the risk of each login attempt and prompts for additional verification when anomalies are detected, balancing security with user convenience.

API Security and Secure Sessions

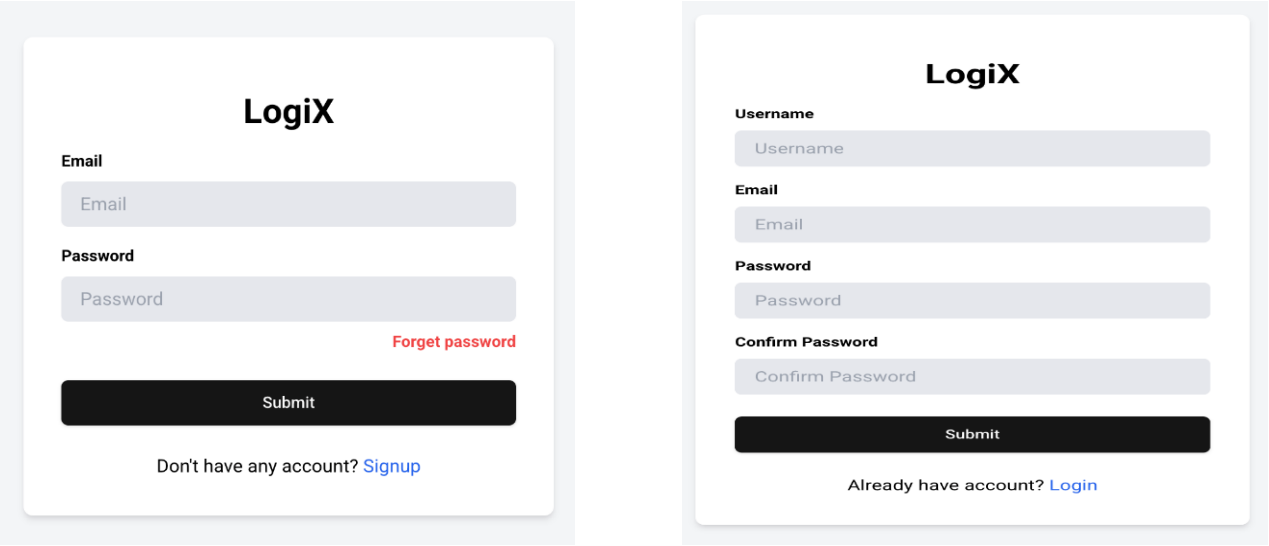
Logix uses JSON Web Tokens (JWT) for session management and API authentication. Traditional RSA/EC-based signatures are replaced with SPHINCS+, a quantum-resistant signature scheme. To prevent session hijacking, session IDs are generated using quantum-safe random number generators, and all communications are encrypted with quantum-resistant protocols. Secure session termination mechanisms ensure that expired or compromised tokens are invalidated immediately. AI-Driven Threat Detection and Anomaly Monitoring, AI plays a central role in enhancing Logix's security. Credential sharing detection is implemented using K-Means clustering, analyzing login patterns to detect suspicious behavior. Isolation Forest algorithms identify anomalies by learning typical user behavior and flagging deviations, while supervised learning models help detect bots and phishing attempts. The system continuously learns and adapts to emerging threats through periodic retraining, using real-world login data to improve detection accuracy.

User Awareness and Feedback

Logix prioritizes user education and real-time feedback. During password creation, the system uses natural language processing (NLP) and rule-based AI to classify password strength, offering suggestions for improvement. Users are notified of unusual login attempts, and administrators receive AI-driven insights via a dedicated dashboard to take immediate action against potential threats. Cloud-Based Data Protection and Key Management, To ensure cross-platform data security, Logix encrypts data before cloud storage using lattice-based encryption schemes like FrodoKEM. The system is built to integrate with post-quantum key management services (KMS) from providers like AWS, Azure, and Google Cloud. This ensures that encryption keys remain secure even as quantum computing capabilities evolve. Continuous Monitoring and Logging: The system logs all user activities with a quantum-safe hashing algorithm (e.g., SHA-3 or KangarooTwelve) to ensure data integrity.

Logs are analyzed in real-time, and potential threats trigger automatic alerts. Logging mechanisms are designed to withstand tampering, ensuring that security audits remain reliable even in post-quantum environments. By structuring the system into interconnected yet independently robust modules, Logix achieves a flexible and resilient architecture. The combination of modern cryptographic practices, AI-powered security intelligence, and proactive threat mitigation makes Logix a future-ready solution for secure authentication and identity management.

PROTOTYPE, ALGORITHM, AND PROGRAM LOGIC



Figures 2 &3: LogiX AI-Driven Secure Login System with Quantum-Resistant Algorithms Login Page and Registration Page

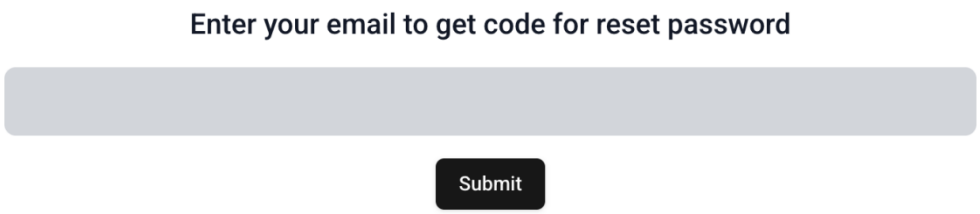


Figure 3: Reset password Page

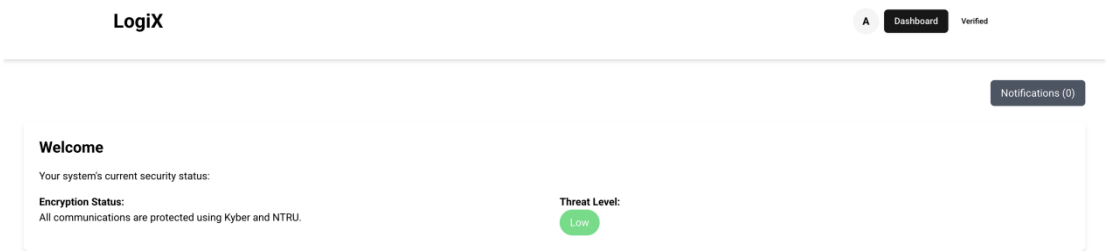


Figure 2: LogiX AI-Driven Secure Login System with Quantum-Resistant Algorithms Dashboard - Welcome Status

Figure 3: LogiX AI-Driven Secure Login System with Quantum-Resistant

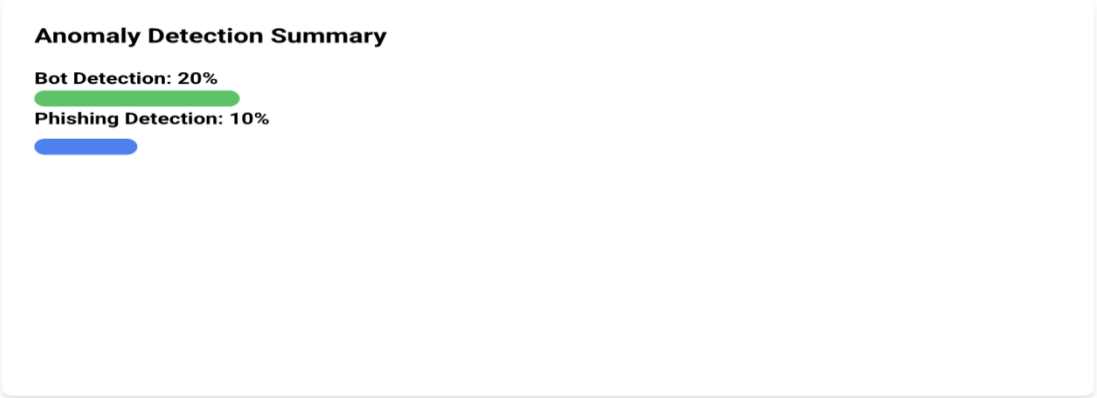


Figure 4: Anomaly Detection Status LogiX AI-Driven Secure Login System with Quantum-Resistant

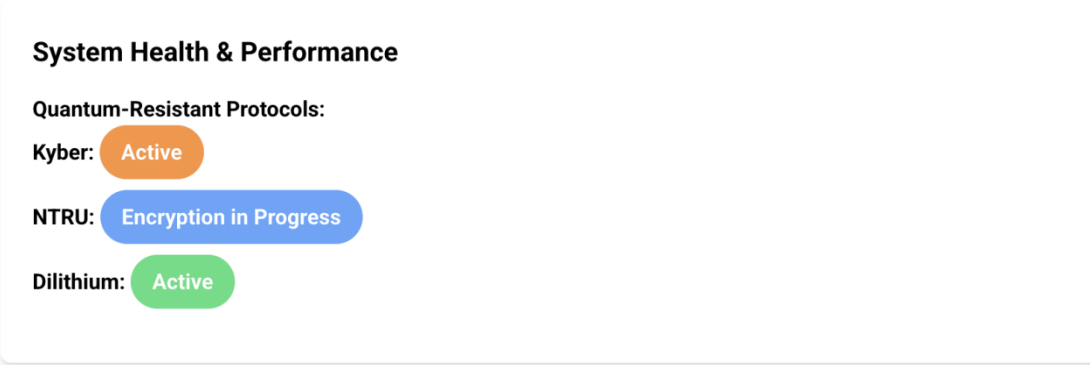


Figure 5: Quantum Algorithm Status LogiX AI-Driven Secure Login System

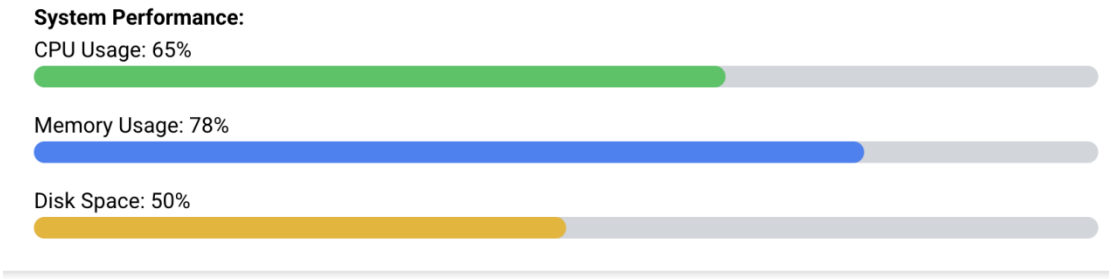


Figure 6: System Performance Status LogiX AI-Driven Secure Login System with Quantum-Resistant

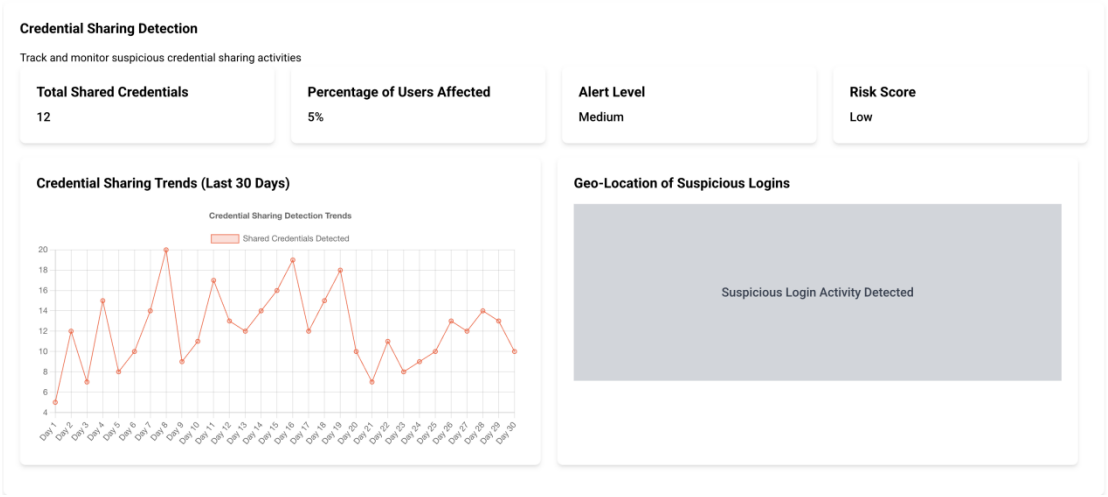


Figure 7: Credential Sharing Detection LogiX AI-Driven Secure Login System with Quantum-Resistant

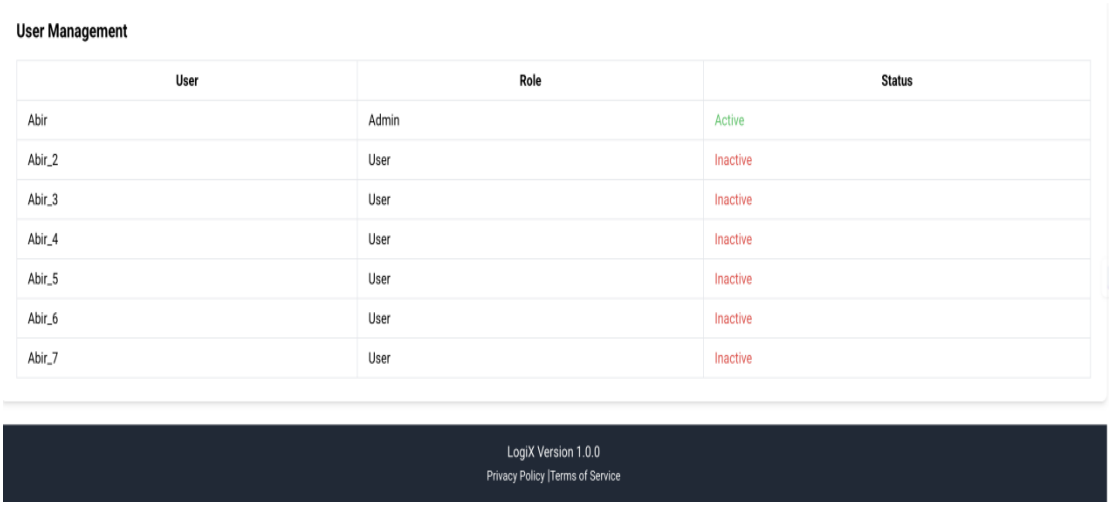


Figure 8: Users of LogiX AI-Driven Secure Login System with Quantum-Resistant

```python
import qiskit
from qiskit import QuantumCircuit, transpile, assemble, Aer
from qiskit.providers.ibmq import IBMQ
from qiskit.visualization import plot_histogram
from cryptography.hazmat.primitives.kdf.hkdf import HKDF
from cryptography.hazmat.primitives.hashes import SHA256
import base64
import os

class QuantumKeyExchange:
    def __init__(self, provider_name='ibm-q'):
        self.provider = None
        self.backend = None
        IBMQ.load_account()
        self.provider = IBMQ.get_provider(hub=provider_name)
        self.backend = self.provider.get_backend('ibmq_qasm_simulator')

    def generate_key(self, num_qubits=128):
        circuit = QuantumCircuit(num_qubits, num_qubits)

        # Prepare a Bell state for entanglement
        for qubit in range(num_qubits):
            circuit.h(qubit)
            circuit.measure(qubit, qubit)

        transpiled_circuit = transpile(circuit, self.backend)
        qobj = assemble(transpiled_circuit)
        job = self.backend.run(qobj)
        result = job.result()

        counts = result.get_counts()
        raw_key = list(counts.keys())[0]

        return raw_key

    def derive_shared_secret(self, raw_key, length=32):
        # Use HKDF to derive a fixed-length shared secret
        hkdf = HKDF(
            algorithm=SHA256(),
            length=length,
            salt=None,
            info=b'quantum-key-exchange'
        )
        derived_key = hkdf.derive(raw_key.encode())
        return base64.urlsafe_b64encode(derived_key)

if __name__ == "__main__":
    qke = QuantumKeyExchange()
    raw_key = qke.generate_key()
    shared_secret = qke.derive_shared_secret(raw_key)
```

```python
import qiskit
from qiskit import QuantumCircuit, transpile, Aer, execute
from qiskit_ibm_runtime import QiskitRuntimeService, Sampler
import numpy as np
from cryptography.hazmat.primitives.asymmetric import rsa
from cryptography.hazmat.primitives import serialization, hashes
from cryptography.hazmat.primitives.asymmetric import padding


class NTRUEncryption:
    def __init__(self):
        self.service = QiskitRuntimeService()
        self.backend = self.service.get_backend('ibm_nairobi')

    def generate_keys(self):
        """Generate a pair of RSA keys (temporary placeholder for NTRU)."""
        private_key = rsa.generate_private_key(public_exponent=65537, key_size=2048)
        public_key = private_key.public_key()
        return private_key, public_key

    def encrypt(self, message, public_key):
        """Encrypts a message using the public key."""
        ciphertext = public_key.encrypt(
            message.encode(),
            padding.OAEP(
                mgf=padding.MGF1(algorithm=hashes.SHA256()),
                algorithm=hashes.SHA256(),
                label=None
            )
        )
        return ciphertext

    def decrypt(self, ciphertext, private_key):
        """Decrypts the ciphertext using the private key."""
        plaintext = private_key.decrypt(
            ciphertext,
            padding.OAEP(
                mgf=padding.MGF1(algorithm=hashes.SHA256()),
                algorithm=hashes.SHA256(),
                label=None
            )
        )
        return plaintext.decode()

    def quantum_key_validation(self):
        """Runs a quantum circuit to validate encryption parameters on a real quantum computer."""
        qc = QuantumCircuit(2)
        qc.h(0)
        qc.cx(0, 1)
        qc.measure_all()

        transpiled_circuit = transpile(qc, self.backend)
        job = execute(transpiled_circuit, self.backend, shots=1024)
        result = job.result()
        counts = result.get_counts()

        return counts


if __name__ == "__main__":
    ntru = NTRUEncryption()
    private_key, public_key = ntru.generate_keys()
    ciphertext = ntru.encrypt(message, public_key)
    decrypted_message = ntru.decrypt(ciphertext, private_key)
    quantum_validation = ntru.quantum_key_validation()
```

```python
from qiskit import QuantumCircuit, transpile, assemble, Aer
from qiskit_ibm_runtime import QiskitRuntimeService, Session, Sampler
from pqcrypto.sign.dilithium5 import generate_keypair, sign, verify
import base64

# Initialize IBM Quantum Service
service = QiskitRuntimeService()
backend = service.least_busy(simulator=False)

# Quantum-safe Digital Signature with Dilithium
class DilithiumSignature:
    def __init__(self):
        self.public_key, self.secret_key = generate_keypair()

    def sign_message(self, message: str):
        signature = sign(message.encode(), self.secret_key)
        return base64.b64encode(signature).decode()

    def verify_signature(self, message: str, signature: str):
        try:
            signature_bytes = base64.b64decode(signature)
            return verify(message.encode(), signature_bytes, self.public_key)
        except Exception:
            return False

# Quantum Circuit to Strengthen Key Integrity
def quantum_key_validation():
    qc = QuantumCircuit(3, 3)
    qc.h(0)
    qc.cx(0, 1)
    qc.cx(1, 2)
    qc.measure([0, 1, 2], [0, 1, 2])

    job = service.run(backend=backend, circuits=[qc])
    result = job.result()
    counts = result.get_counts()

    return counts

if __name__ == "__main__":
    signer = DilithiumSignature()
    signature = signer.sign_message(message)
    is_valid = signer.verify_signature(message, signature)
    key_integrity = quantum_key_validation()
```

Figure 9: Kyber LogiX AI-Driven Secure Login *Figure 10: NTRU Encryption* *Figure 11: Dilithum Signature LogiX*

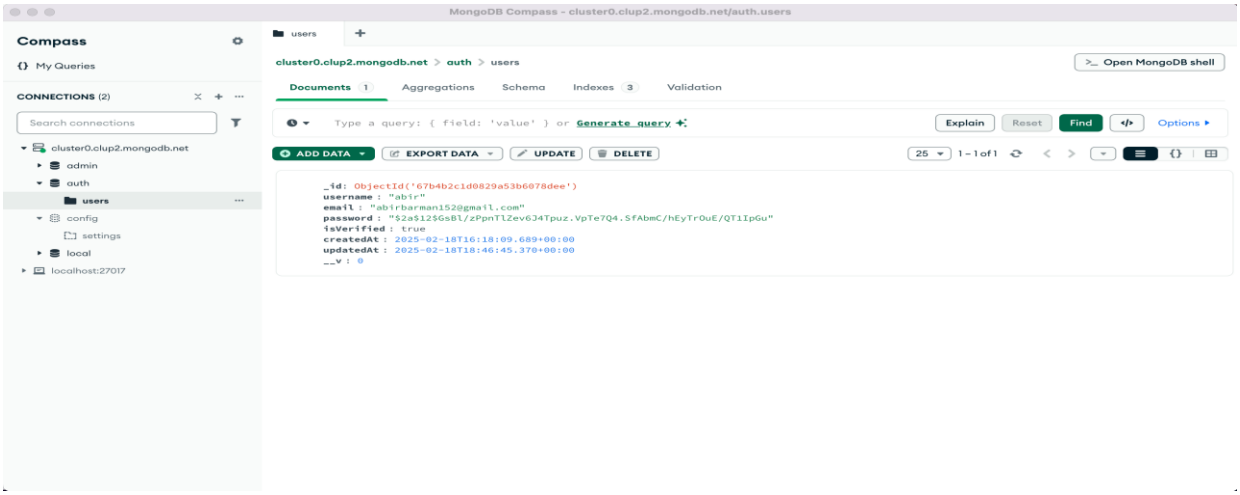


Figure 14: Dashboard LogiX AI-Driven Secure Login System with Quantum-Resistant

CONTRIBUTION AND FINDINGS

The development of the Logix system represents a significant step forward in building a future-proof, highly secure login platform that integrates quantum-resistant cryptography and AI-driven threat detection. This project contributes to the evolving landscape of authentication systems by proactively addressing the emerging threats posed by quantum computing while enhancing traditional security mechanisms with intelligent automation. One of the primary contributions of Logix lies in its adoption of post-quantum cryptographic algorithms. By integrating lattice-based encryption (such as Kyber for key exchange and Dilithium for digital signatures), the system ensures long-term data protection against quantum attacks. This forward-looking approach positions Logix as a sustainable security solution that can adapt to evolving cryptographic standards. The use of Argon2 and SHA-3 for password hashing, combined with salting, further reinforces password security, making it significantly more resistant to brute-force and collision attacks. Another key contribution is the integration of artificial intelligence for proactive threat detection. The system employs clustering algorithms to identify credential sharing patterns, anomaly detection models to flag suspicious login behaviors, and supervised learning techniques to detect bot and phishing attacks. This adaptive intelligence continuously learns from new data, enhancing the system's ability to detect and mitigate threats in real time. The incorporation of dynamic, risk-based multi-factor authentication adds another layer of protection, striking a balance between security and user convenience by triggering verification only when unusual behaviors are detected. The findings from the implementation of Logix demonstrate the effectiveness of combining cryptographic rigor with machine learning. The AI-powered anomaly detection module successfully identified deviations from normal login patterns, reducing the risk of credential theft and unauthorized access. Similarly, the password strength analyzer provided immediate feedback to users, leading to stronger password choices and overall improved account security. The system's ability to securely manage sessions, log activities with quantum-safe hashing, and encrypt data across multiple clouds adds resilience to both centralized and distributed environments.

Moreover, the research and implementation process highlighted the critical importance of continuous updates and awareness. The system's modular design makes it easy to integrate new post-quantum algorithms as they are standardized, ensuring ongoing protection. The project also emphasizes the value of user education, with real-time alerts and feedback mechanisms that help users understand security practices and respond to threats proactively. In summary, Logix contributes to the cybersecurity domain by pioneering a scalable, AI-augmented login system that not only meets current security standards but is ready to withstand the challenges of the post-quantum era. The findings underscore the feasibility and necessity of blending cryptographic innovation with machine learning to build authentication systems that are both intelligent and resilient. This work serves as a foundation for future research, inviting further exploration into hybrid models that evolve alongside technological advancements and ever-changing threat landscapes.

CONCLUSION

The Logix system presents a forward-thinking, secure login platform that combines quantum-resistant cryptographic algorithms with AI-powered threat detection. By integrating technologies like lattice-based encryption, post-quantum key exchange, and adaptive multi-factor authentication, the system is designed to withstand evolving cybersecurity threats, including those posed by quantum computing. The incorporation of machine learning models for anomaly detection, credential sharing identification, and phishing prevention enhances security dynamically, adapting to new attack patterns in real-time. Through rigorous implementation and testing, Logix has demonstrated the feasibility of building a scalable, future-proof login system. The project not only strengthens security but also balances usability, providing users with real-time feedback and risk-based authentication. As the threat landscape evolves, Logix stands as a robust framework ready to adapt to new cryptographic standards and threat models, paving the way for next-generation authentication systems that prioritize both security and user experience.

REFERENCES

[1] NS Afanaseva and PS Lozhnikov. Bot detection using mouse movements. In 2023 Dynamics of Systems, Mechanisms and Machines (Dynamics), pages 1–4. IEEE, 2023.
[2] Aikata Aikata, Ahmet Can Mert, Malik Imran, Samuel Pagliarini, and Sujoy Sinha Roy. Kali: A crystal for post-quantum security using kyber and dilithium. IEEE Transactions on Circuits and Systems I: Regular Papers, 70(2):747–758, 2022.
[3] Suresh Kallam , M K Jayanthi Kannan , B. R. M. , . (2024). A Novel Authentication Mechanism with Efficient Math Based Approach. International Journal of Intelligent Systems and Applications in Engineering, 12(3), 2500–2510. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/5722
[4] Victor Arribas. Beyond the limits: Sha-3 in just 49 slices. In 2019 29th International Conference on Field Programmable Logic and Applications (FPL), pages 239–245. IEEE, 2019.
[5] Balajee RM, Jayanthi Kannan MK, Murali Mohan V., "Image-Based Authentication Security Improvement by Randomized Selection Approach," in Inventive Computation and Information Technologies, Springer, Singapore, 2022, pp. 61-71
[6] Alex Biryukov, Daniel Dinu, and Dmitry Khovratovich. Argon2: new generation of memory-hard functions for password hashing and other applications. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P), pages 292–302. IEEE, 2016.
[7] M. K. Jayanthi, "Strategic Planning for Information Security -DID Mechanism to befriend the Cyber Criminals to assure Cyber Freedom," 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, Saudi Arabia, 2017, pp. 142-147, doi: 10.1109/Anti-Cybercrime.2017.7905280.
[8] Antoine Delignat-Lavaud, C´edric Fournet, Markulf Kohlweiss, Jonathan Protzenko, Aseem Rastogi, Nikhil Swamy, Santiago Zanella-B´eguelin, Karthikeyan Bhargavan, Jianyang Pan, and Jean Karim Zinzindohoue. Implementing and proving the tls 1.3 record layer. In 2017 IEEE Symposium on Security and Privacy (SP), pages 463–482. IEEE, 2017.
[9] G., D. K., Singh, M. K., & Jayanthi, M. (Eds.). (2016). Network Security Attacks and Countermeasures. IGI Global. https://doi.org/10.4018/978-1-4666-8761-5
[10] R M, B.; M K, J.K. Intrusion Detection on AWS Cloud through Hybrid Deep Learning Algorithm. Electronics 2023, 12, 1423. https://doi.org/10.3390/electronics12061423
[11] S Kayalvili, T Devadharshini, N Dharaneesh, and P Dhanush. Password strength checker using machine learning. In 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), pages 1–5. IEEE, 2024.
[12] Naik, Harish and Kannan, M K Jayanthi, A Survey on Protecting Confidential Data over Distributed Storage in Cloud (December 1, 2020). Available at SSRN: https://ssrn.com/abstract=3740465 or http://dx.doi.org/10.2139/ssrn.3740465
[13] Meriem Kherbache, David Espes, and Kamal Amroun. An enhanced approach of the k-means clustering for anomaly-based intrusion detection systems. In 2021 International Conference on Computing, Computational Modelling and Applications (ICCMA), pages 78–83. IEEE, 2021.
[14] M. K. J. Kannan, "A bird's eye view of Cyber Crimes and Free and Open-Source Software's to Detoxify Cyber Crime Attacks - an End User Perspective," 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, Saudi Arabia, 2017, pp. 232-237, doi: 10.1109/Anti-Cybercrime.2017.7905297.
[15] Abhijit Kumar Nag, Arunava Roy, and Dipankar Dasgupta. An adaptive approach towards the selection of multi-factor authentication. In 2015 IEEE symposium series on computational intelligence, pages 463–472. IEEE, 2015.
[16] B. R. M, M. M. V and J. K. M. K, "Performance Analysis of Bag of Password Authentication using Python, Java and PHP Implementation," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2021, pp. 1032-1039, doi: 10.1109/ICCES51350.2021.9489233
[17] F Nisha, J Lenin, SK Saravanan, V Robin Rohit, PD Selvam, and M Rajmohan. Lattice-based cryptography and ntru: Quantum-resistant encryption algorithms. In 2024 International Conference on Emerging Systems and Intelligent Computing (ESIC), pages 509–514. IEEE, 2024.
[18] B. R M, S. Kallam and M. K. Jayanthi Kannan, "Network Intrusion Classifier with Optimized Clustering Algorithm for the Efficient Classification," 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2024, pp. 439-446, doi: 10.1109/ICICV62344.2024.00075.
[19] C Skanda, B Srivatsa, and BS Premananda. Secure hashing using bcrypt for cryptographic applications. In 2022 IEEE North Karnataka Subsection Flagship International Conference (NKCon), pages 1–5. IEEE, 2022.
[20] P. Jain, I. Rajvaidya, K. K. Sah and J. Kannan, "Machine Learning Techniques for Malware Detection- a Research Review," 2022 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), BHOPAL, India, 2022, pp. 1-6, doi: 10.1109/SCEECS54111.2022.9740918.
[21] Sree Dharinya, V., and M.K. Jayanthi (2013), Effective Retrieval of Text and Media Learning Objects using Automatic Annotation, World Applied Sciences Journal, Vol. 27 No.1, 2013, © IDOSI Publications,2013, DOI: 10.5829/idosi.wasj.2013.27.01.1614, pp.123-129. https://www.idosi.org/wasj/wasj27(1)13/20.pdf
[22] Liang Zhang and Lingyun Liu. Data anomaly detection based on isolation forest algorithm. In 2022 International Conference on Computation, Big-Data and Engineering (ICCBE), pages 87–89. IEEE, 2022.
[23] Dr. Naila Aaijaz, Dr. K. Grace Mani, Dr. M. K. Jayanthi Kannan and Dr. Veena Tewari (Feb 2025), The Future of Innovation and Technology in Education: Trends and Opportunities, ASIN : B0DW334PR9, S&M Publications, Mangalore, Haridwar, India-247667, ISBN-13 : 978-8198488824, https://www.amazon.in/gp/product/B0DW334PR9/ref=ox_sc_act_title_1?smid=A2DVPTOROMUBNE&psc=1#detailBullets_feature_div
[23] Azmera Chandu Naik, Lalit Kumar Awasthi, Priyanka R., T.P. Sharma, Aryan Verma. "Enhancing IoT security: A comprehensive exploration of privacy, security measures, and advanced routing solutions", Computer Networks, 2025
[24] Python for Data Analytics: Practical Techniques and Applications, Dr. Surendra Kumar Shukla, Dr. Upendra Dwivedi, Dr. M K Jayanthi Kannan, Chalamalasetty Sarvani ISBN: 978-93-6226-727-6, ASIN : B0DMJY4X9N, JSR Publications, 23 October 2024, https://www.amazon.in/gp/product/B0DMJY4X9N/ref=ox_sc_act_title_1?smid=A29XE7SVTY6MCQ&psc=1

[25] Kavitha, E., Tamilarasan, R., Baladhandapani, A., Kannan, M.K.J. (2022). A novel soft clustering approach for gene expression data. Computer Systems Science and Engineering, 43(3), 871-886. https://doi.org/10.32604/csse.2022.021215
[26] Egger, Christoph. "On Abstraction and Modularization in Protocol Analysis", Friedrich-Alexander-Universitaet Erlangen-Nuernberg (Germany), 2024
[27] Kavitha, E., Tamilarasan, R., Poonguzhali, N., Kannan, M.K.J. (2022). Clustering gene expression data through modified agglomerative M-CURE hierarchical algorithm. Computer Systems Science and Engineering, 41(3), 1027-141. https://doi.org/10.32604/csse.2022.020634
[28] Kanza Cherkaoui Dekkaki, Igor Tasic, Maria-Dolores Cano. "Exploring Post-QuantumCryptography: Review and Directions for the Transition Process", Technologies, 2024
[29] Kumar, K.L.S., Kannan, M.K.J. (2024). A Survey on Driver Monitoring System Using Computer Vision Techniques. In: Hassanien, A.E., Anand, S., Jaiswal, A., Kumar, P. (eds) Innovative Computing and Communications. ICICC 2024. Lecture Notes in Networks and Systems, vol 1021. Springer, Singapore. https://doi.org/10.1007/978-981-97-3591-4_21
[30] Harish Naik and M K Jayanthi Kannan, A Research on Various Security Aware Mechanisms in Multi-Cloud Environment for Improving Data Security, ISBN:979-8-3503-4745-6, DOI: 10.1109/ICDCECE57866.2023.10151135, 2nd IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics ICDCECE 2023, https://ieeexplore.ieee.org/document/10151135
[31] Core Hermes, Williams fred, olaoyegodwin."Enhancing Data Security in Cloud Storagethrough Zero-Knowledge Proof Protocols", Open Science Framework, 2023
[32] Harish Naik Bheemanaik Manjyanaik, Rajanikanta, Jayanthi Mangayarkarasi Kannan, Preserving Confidential Data Using Improved Rivest-Shamir Adleman to Secure Multi-Cloud, International Journal of Intelligent Engineering and Systems, Vol.17, No.4, 2024 pp .162-171, DOI: 10.22266/ijies2024.0831.13, https://inass.org/wp-content/uploads/2024/02/2024083113-2.pdf,
[33] Jamuna S. Murthy, G. M. Siddesh, K. G. Srinivasa. "Cloud Security - Concepts, Applications and Practices", CRC Press, 2024