Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A Comprehensive Threat Model and Risk Assessment Framework for Quantum-Secure Communication in the Metaverse

Sudhakar Nanjappa

sudhakar.n99@gmail.com

Ramaiah Institute of Technology

Geetha Venkatesh

Ramaiah Institute of Technology

Research Article

Keywords: Metaverse security, Quantum Key Distribution (QKD), Post-quantum cryptography (PQC), Threat Modeling, STRIDE, Attack Tree Analysis, Risk Assessment, Cybersecurity, Quantum-Secure Communication, Network Security

Posted Date: November 10th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11387745/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

A Comprehensive Threat Model and Risk Assessment Framework for Quantum-Secure Communication in the Metaverse

"Corresponding author: Sudhakar Nanjappa"

Sudhakar Nanjappa[1], (PhD)
Student MSRIT collage
Bangalore, Karnataka, India.
Email :
Sudhakar.n99@gmail.com

Geetha V[2], PhD, Associate Professor, Dept CSE, MSRIT, Bangalore, Karnataka, India
Email : geethav@msrit.edu

This research received no external funding.

Abstract

The rapid growth of the Metaverse creates major challenges in secure communication because of its decentralized and data-intensive nature. Traditional cryptographic methods are vulnerable to quantum computing attacks. This research paper developed a unified framework for quantum-secure communication in the Metaverse. It integrated quantum key distribution (QKD), post-quantum cryptography (PQC), STRIDE-based threat modelling, and attack tree analysis. A quantitative risk model based on probability and impact is developed and validated using simulations with 10,000 to 100,000 users. The results show that the risk has come down by 52.2%, the threat detection rate is 95%, and the attack success rate is less than 10%. The system demonstrates linear scalability with controlled latency and acceptable computational overhead (10–16%). Statistical analysis indicates that the risk distribution is stable and the variance is lower. Compared to existing methods, the developed framework provides enhanced security, scalability, and adaptability, particularly in handling increased user loads and dynamic network conditions. It is critical to preserving performance and reliability in high-demand scenarios, especially when ensuring that secure communication remains effective under varying user loads and network conditions. The research work offers a practical solution for secure communication in quantum-enabled Metaverse environments. Additionally, it addresses challenges such as data integrity, user privacy, and real-time interaction in these complex digital spaces.

Keywords: Metaverse security, Quantum Key Distribution (QKD), Post-quantum cryptography (PQC), Threat Modeling, STRIDE, Attack Tree Analysis, Risk Assessment, Cybersecurity, Quantum-Secure Communication, Network Security.

1. Introduction

The Metaverse is rapidly emerging as a novel new ecosystem that combines virtual reality, augmented reality, and distributed computing technologies [1, 2]. It enables immersive interaction and communication in a shared virtual space. It supports virtual commerce, digital identity, healthcare, education, and remote collaboration [3, 4]. As these applications grow, ensuring data security and user privacy becomes critical. This study focuses on developing a comprehensive threat model and risk assessment framework for quantum-secure communication in the Metaverse [5].

Recent studies indicate that the Metaverse depends on decentralized systems and real-time data exchange [6], which are essential for ensuring user privacy and enabling seamless interactions within virtual environments. Blockchain technology is widely used for identity and asset management among Metaverses [7]. Traditional cryptographic methods, Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), are commonly used to secure communication. However, quantum computing breaks these classical encryption techniques [9]. By addressing this issue, Quantum Key Distribution (QKD) has been introduced as a secure communication method [10]. Post-quantum cryptography is being developed to resist quantum attacks [11], and it aims to create encryption methods that remain secure even in the presence of quantum computing capabilities. Zero-trust architectures improve access control in distributed environments [12]. Artificial intelligence (AI) is used to detect abnormal activities in real-time [13]. Using privacy techniques such as homomorphic encryption and secure multi-party computation helps protect sensitive data [14]. However, these solutions are investigated separately and not as a unified framework. This limits their effectiveness in providing comprehensive security. Integrating these techniques can improve data protection and overall system performance [15].

Earlier works have highlighted key developments in this field, like Shor showing that quantum algorithms break classical encryption systems [16], Grover presenting a faster search algorithm that weakens symmetric encryption [17], and Bennett and Brassard introducing QKD for secure communication [18]. Gentry developed homomorphic encryption for secure data processing [19]. NIST has started standardizing post-quantum cryptographic methods [20]; Zyskind et al. proposed blockchain-based identity systems [21, 22]; zero-trust security was formalized by Syed et al. [12]; Sommer and Paxson [13] developed ML-based intrusion

detection; Camara introduced secure multi-party computation [23]; and Patra et al. discussed security challenges in the Metaverse [5].

Although there are advancements, no integrated framework combines quantum security, threat modelling, and risk assessment for the Metaverse. Present research works failed to address the dynamic and complex nature of Metaverse environments. They also lack integration of quantum security with threat modelling and risk assessment. They are critical for system safety and reliability. The study provides clear evidence for a single, scalable solution, which can address both classical and quantum threats.

The objective of the research work was to establish a Quantum-secure **S**TRIDE and Attack tree-based Risk **R**eduction framework (Q-STARR Framework) for threat modelling and risk assessment in quantum-secure Metaverse communication, which includes identifying security threats, integrating quantum-resistant techniques, developing a risk assessment model, and validating the framework through simulations. This study focuses only on communication-layer security and does not consider hardware-level quantum implementations. The proposed work introduces a novel integrated framework that combines quantum security, threat modelling, and risk assessment tailored for the Metaverse. The main contributions of this work are the following:

- A unified framework integrating QKD, PQC, STRIDE, and attack tree modelling
- A normalized and weighted risk assessment model
- Simulation-based validation with large-scale Metaverse users
- Comprehensive evaluation of security, scalability, and performance metrics

2. Related Research Work

Recent research work on Metaverse security focuses on challenges facing it in its decentralized and highly interactive nature. The Metaverse combines virtual reality, blockchain, artificial intelligence, and cloud computing, which increases system complexity and expands the attack surface [24, 25]. Common issues include identity theft, data leakage, and misuse of virtual assets [26]. Researchers also point out the lack of standard security frameworks across platforms, which creates interoperability and protection challenges, making it difficult for users to ensure their data and assets are secure while navigating different environments in the Metaverse,

especially as these environments often have varying security protocols and user privacy policies.

Blockchain has been widely used to improve trust and identity management in the Metaverse, which is a collective virtual shared space that enables secure and decentralized control of digital assets. It allows for safe and decentralized management of digital assets [27]. However, most blockchain systems rely on classical cryptography, which is vulnerable to quantum attacks [28]. Studies indicate that future quantum computers may break widely used encryption methods, creating serious risks for Metaverse systems, particularly in terms of data security and user privacy, which could undermine trust in these digital environments [29].

Quantum cryptography and quantum mechanics offer the solution to these problems and provide the most secure communication [30], respectively. QKD assists in the security of key exchange and helps eliminate eavesdropping [31]. Researchers are also integrating QKD with conventional encryption to enhance the general security. Post-quantum cryptography offers protection against quantum attacks [25]. Hybrid methods combining quantum and classical techniques, which integrate both approaches, are intended to offer practical and scalable solutions for enhancing security in the face of emerging quantum threats and ensuring compatibility with existing systems [32], AI is used to detect anomalous behaviour and predict threats in real time [33, 37]. To keep user data safe in the virtual world, there are other privacy tools like homomorphic encryption and secure multi-party computation [34].

Although threat modelling techniques such as attack trees and STRIDE have been applied to analyse system vulnerabilities, they do not fully address the dynamic and complex nature of the Metaverse [35]. Most current research examines quantum security, threat modelling, and risk assessment in isolation rather than as a cohesive framework [36]. Practical issues such as cost, scalability, and the lack of standard adoption obstruct the development of effective security measures that can address the complexities of quantum security, threat modelling, and risk assessment in a unified manner. Moreover, real-time secure communication in large-scale virtual environments still requires more efficient solutions.

Recent studies emphasize the necessity of unified and adaptive security frameworks. These frameworks should combine quantum-resistant cryptography,

decentralized identity systems, and intelligent threat detection [37]. Researchers agree that future solutions must handle both classical and quantum threats together. Future research should focus on integrating quantum computing with blockchain and AI. However, a complete and integrated security framework for Metaverse communication is still missing, which is crucial for ensuring the safety and privacy of users in this evolving digital landscape.

3. Proposed Framework

3.1 System Architecture

The Q-STARR Framework provides end-to-end security for Metaverse communication, which consists of three layers: the Quantum-Secure Communication Layer, the Threat Modelling Layer, and the Risk Assessment Layer. These layers ensure secure data exchange, identify vulnerabilities, and evaluate risks in a scalable and adaptive manner, as shown in Fig. 1. The quantum-secure communication layer forms the foundation of the framework with secure data transmission among avatars and virtual assets. The layer integrates QKD for secure key exchange and PQC for encryption. QKD prevents eavesdropping by using quantum principles, while PQC ensures compatibility with existing systems and resistance to quantum attacks that employ a hybrid approach to combine classical and quantum techniques for better security and efficiency.

The threat modelling layer identifies and analyses potential security threats, which combines STRIDE and attack tree methods to provide structured analysis. STRIDE categorizes threats such as spoofing, tampering, and Denial-of-service (DoS), while attack trees model possible attack paths. These threats are mapped to Metaverse components like user identities, communication channels, and digital assets. This layer helps in understanding vulnerabilities and planning preventive measures. The risk assessment layer is used to assess the probability and the effect of the identified threats. All the threats are rated with respect to risk scores in terms of probability. There is the input of weight factors to indicate the significance of various system components, which facilitates proper prioritization of risks. Risk matrices and probabilistic analysis are used to make informed decisions and respond to changing threats. These three layers collaborate to come up with a unified security framework. The communication layer facilitates the security of the data transfer, the threat modelling layer determines the risks, and the risk assessment layer prioritizes them. The risk

layer provides feedback that helps in the improvement of the threat models and security strategies, thus making the system continuously improve.

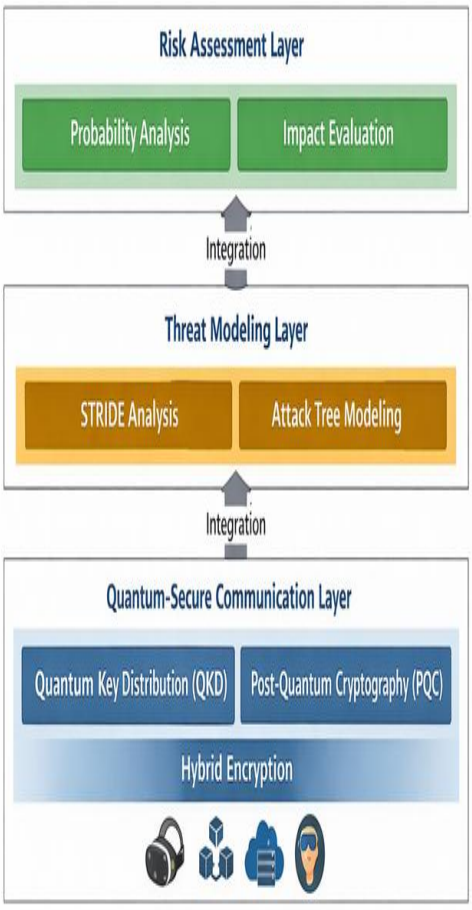


Fig. 1 Proposed layered architecture integrating quantum-secure communication, threat modelling, and risk assessment in Metaverse systems

3.2 Threat Modelling

The Q-STARR Framework takes a hybrid approach to threat modelling, which blends analysis of STRIDE and attack tree modelling to analyse and identify security threats in the Metaverse in an organized way, which not only makes it easy to see all the possible attack paths but also makes it easy to observe and classify them. Threats are categorized into six broad groups (STRIDE): spoofing, tampering, repudiation, information disclosure, DoS, and elevation of privilege. They assist in comprehending various kinds of vulnerabilities in the system. "Spoofing" is the term that implies the impersonation of users/avatars, and "tampering" is an unauthorized alteration of information or virtual resources. Repudiation is used when users refute their activities, and information disclosure is associated with access to sensitive information without permission. DoS influences the availability of the system, and an elevation of privilege will enable an attacker to have unauthorized access or control.

All the threats are mapped to the main elements of the Metaverse, which are avatars (digital representations of users), digital assets (virtual items or property), communication channels (ways of interaction), and virtual environments (simulated spaces in which users can interact). Such mapping assists in the interpretation of the exposure of various components of the system to particular risks. The attack scenarios are created in terms of attack tree modelling, a hierarchical format that demonstrates the threats implemented step by step.

3.3 Risk Assessment Model

The Q-STARR Frameworke valuates security risks using a quantitative model, which is based on probability and impact. It estimates the severity of each threat and supports better decision-making. The risk depends on two main factors, such as the likelihood of a threat occurring and the impact it may cause. These factors represent the uncertainty and potential damage in the Metaverse environment. The model analyses multiple threats at the same time. It allows comparison across different system components. To maintain consistency, all input values are normalized. This ensures that risks are measured on a common scale and compared easily.

A weighted approach is also used for different threats, which are assigned different importance levels. Higher weights are given to critical components such as communication channels, digital assets, and user identities.

The total risk is calculated by combining the contributions of all threats, which includes their normalized values and assigned weights. It helps in identifying and prioritizing high-risk threats, and it also supports efficient use of security resources. The model takes into account sensitivity and looks at how changes in probability and impact affect the overall risk. This leads to the system being more sensitive to impact than probability, which means high-impact threats must be addressed first, even if they occur less frequently. The model is flexible and scalable, which is updated dynamically and supports real-time risk evaluation in changing Metaverse environments.

3.4 Quantum-Secure Integration

The Q-STARR Framework uses quantum-secure techniques to protect communication in the Metaverse. These techniques help secure data against both current cyber and future quantum threats. The Q-STARR Framework mainly uses three key methods such as QKD**,** PQC, and a hybrid encryption approach. QKD is used for secure key exchange between users, which is based on quantum principles; it makes it possible to detect any eavesdropping during communication. This ensures that the encryption keys remain safe and are not intercepted. PQC algorithms are used for encryption and decryption and are specifically designed to resist attacks from quantum computers while working with existing systems. Such an approach makes the framework practical and future ready. A hybrid encryption approach is also used. It combines classical encryption methods with quantum-secure techniques. This helps maintain a favourable balance between security and system performance. By combining these methods, the framework enables strong protection of data. It maintains the confidentiality, integrity, and authenticity of communication in the Metaverse. Integration makes the system more secure, reliable, and suitable for real-world applications.

4. Methodology

The conceptual design of the proposed methodology is validated by simulation-based experiments, which ensures reliability and practical applicability.

Simulation Setup:

The simulation was conducted using a Python-based environment with statistical and network modelling libraries. The system included 10,000 to 100,000 virtual nodes interacting through distributed communication channels. Multiple attack scenarios, including spoofing, tampering, data interception, DoS, and privilege escalation, are used to evaluate system performance under realistic conditions. Each experiment was repeated **50 times** to

ensure the statistical consistency and reliability of the results.

Step 1: Metaverse communication component identification.

All the important elements, including users, avatars, digital assets, communication channels, servers, and service providers, were introduced. Such elements determine the system boundaries and flow of interactions, providing the ability to map security requirements correctly.

Step 2: Threat Analysis using STRIDE

The STRIDE model helped systematically identify threats. A vulnerability assessment of each system component was conducted in terms of spoofing, tampering, repudiation, information disclosure, DoS, and elevation of privilege. It provided all-inclusive threat coverage.

Step 3: Attack Tree

Critical threats were investigated by developing attack trees. Each node of the tree is a possible step of an attack, which helps to visualize attacks that clearly occur in many steps. Another advantage is that it is possible to identify weak areas of the system (i.e., vulnerabilities that attackers may exploit at different points) and thus make specific changes to security protocols to address such threats.

Step 4: Assignment of Probability and Impact Values: Each threat was assigned a probability (P) and impact (I) value. Probability was calculated based on frequency of occurrence in simulation:

$$P_i = \frac{N_i}{N_{total}}$$

Eq. 1

Impact was defined using a normalized severity scale (0 to 1), based on potential damage to system components. To standardize values, normalization was applied:

$$P_i^{norm} = \frac{P_i - P_{min}}{P_{max} - P_{min}}$$

Eq. 2

$$I_i^{norm} = \frac{I_i - I_{min}}{I_{max} - I_{min}}$$

Eq. 3

Step 5: Risk Score Calculation Risk scores were computed using normalized values:

$$R_i = P_i^{norm} \; X \; I_i^{norm}$$

Eq. 4

A weighted model was used for prioritization:

$$R_{total} = \sum_{i=1}^{n} (R_i X W_i)$$

Eq. 5

where Wi represents the importance of each threat.

Step 6: Quantum-Secure Techniques.

Quantum-secure methods such as QKD and PQC were used to reduce high-risk threats. A mixed encryption method was used. The method can be used to ensure good security

and at the same time keep the computational cost affordable, especially when it can take advantage of the advantages of the quantum secure algorithm and the conventional encryption algorithm.

Step 7: Validation through Simulation

The Q-STARR Framework was tested using simulations with various user loads, and attack conditions were taken into account. Risk reduction, detection accuracy, attack success rate, and system latency were some of the key performance metrics. The current validation is based on simulation; real-world validation will be addressed in future studies.

5. Results

The Q-STARR Framework was evaluated using simulated Metaverse scenarios consisting of multiple users, avatars, digital assets, and communication channels. Various attack conditions were introduced to test system behaviour under realistic environments. Performance was analysed in terms of risk reduction, threat mitigation, and system stability. The results clearly show that the integration of quantum-secure techniques with structured threat modelling and risk assessment significantly improves overall security and reliability.

5.1 Risk Reduction

The effectiveness of the risk reduction result is plotted in Fig. 2 and tabulated in Table 1; they show a reduction in risk across all major threat categories. Fig. 2 shows the risk values after applying the framework are much lower than the initial values. The error bars indicate low variation, which shows stable and reliable performance. Table 1 provides detailed numerical results. The average risk decreases from 87.7 to 42.0. This results in an overall reduction of 52.2%. Repudiation shows the highest reduction at 63.2%, while tampering shows the lowest at 42.1%. Other threats, such as spoofing and elevation of privilege, show reductions of 56.3%. Information disclosure and DoS show reductions of 48.4% and 47.0%, respectively. The statistical results indicate that the mean reduction is 52.2%, with a standard deviation of 7.05% and a 95% confidence interval (46.6%–57.8%); the results are reliable and fall within the expected range.

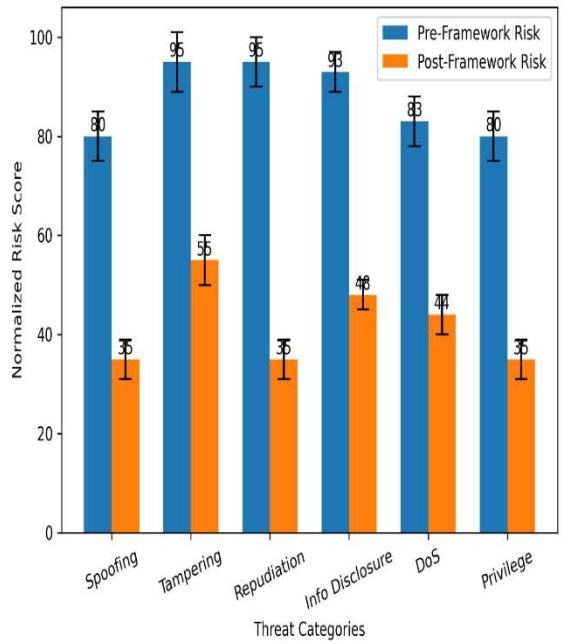


Fig. 2. Risk comparison with error bars showing reduced scores across

Table 1. Risk Reduction and Performance Analysis by Threat Category

Threat Category	Initial Risk Score	Post-Framework Risk Score	Reduction (%)
Spoofing	80	35	56.3
Tampering	95	55	42.1
Repudiation	95	35	63.2
Information Disclosure	93	48	48.4
DoS	83	44	47.0
Elevation of Privilege	80	35	56.3
Average	87.7	42.0	52.2
Mean Reduction (%) = 52.2, Standard Deviation (%) = 7.05, 95% Confidence interval 46.6-57.8			

5.2 Threat Detection Accuracy

The threat detection performance of the Q-STARR Framework was evaluated in multiple attack scenarios. These scenarios encompass spoofing, tampering, data breaches, and DoS attacks, with their results displayed in Fig. 3 and Table 2. The proposed hybrid model is compared with traditional and STRIDE-based approaches. According to Fig. 3, the Q-STARR Framework achieves higher detection accuracy across all scenarios. Traditional methods show the lowest performance due to the lack of structured analysis. Although STRIDE-based methods enhance detection by classifying threats, they still fail complex attack patterns. The framework combines STRIDE with attack tree modelling, which enables better identification of both simple and complex threats. The framework achieves an average accuracy of 95.0%. In comparison, STRIDE-based methods achieve 75.0%, and traditional methods achieve 54.9%. The framework achieves 94.2% for spoofing, 96.0% for tampering, 95.1% for data breaches, and 94.8% for DoS attacks. The framework improves by an average of 21.1% over STRIDE-based methods, with data breach detection showing the highest improvement at 22.8%. The framework can look at both direct and multi-stage attack paths, which makes it less likely that false positives will happen because of structured classification. It also captures complex interactions between Metaverse components. In addition, risk-based prioritization helps focus on critical threats. The statistical analysis confirms the consistency of the results that the mean improvement is 21.1%, with a standard deviation of 7.05%. The 95% confidence interval (46.6%–57.8%) shows that the improvement is reliable.

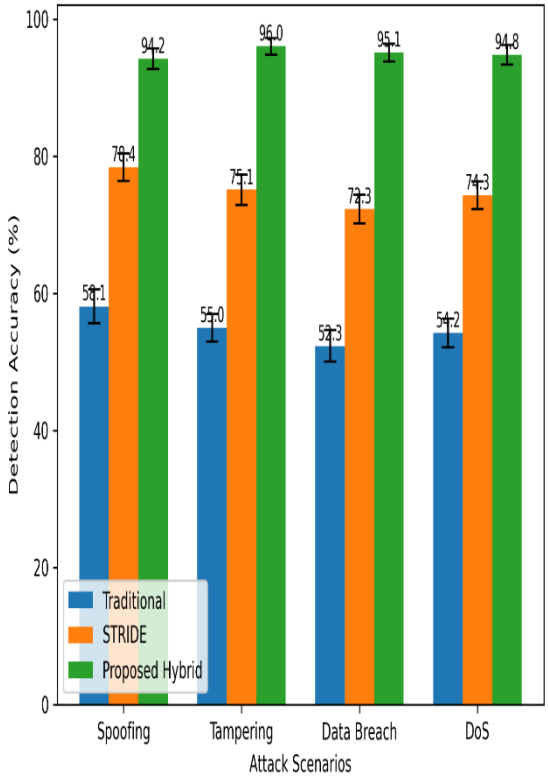


Fig. 3. Comparison of threat detection accuracy across methods with error

Table 2. Threat Detection Accuracy Comparison with Statistical Analysis

Attack Scenario	Traditional (%)	STRIDE-Based (%)	Proposed Hybrid (%)	Improvement over STRIDE (%)
Spoofing	58.1	78.4	94.2	20.2
Tampering	55.0	75.1	96.0	20.9
Data Breach (Info. Disc.)	52.3	72.3	95.1	22.8
DoS	54.2	74.3	94.8	20.5
Average Accuracy	54.9	75.0	95.0	21.1
Mean Improvement (%): 21.1, Standard Deviation (%): 7.05 , 95% Confidence Interval: 46.6 – 57.8				

5.3 Attack Resistance

The Q-STARR Framework's attack resistance was assessed to assess its ability to withstand both classical and quantum-based cyberattacks. The study considered multiple scenarios, including brute-force attacks, eavesdropping, data interception, and DoS attacks. The simulation results are presented in Fig. 4 and Table 3, comparing attack success rates before and after applying the framework. According to Fig. 4, the attack success rates decrease significantly after implementation. The reduction is clear across all attack scenarios. The post-framework values remain very low. The error bars show minimal variation, which indicates stable and reliable performance. The average attack success rate decreases from 82.5% to 4.5%, which corresponds to an overall reduction of 94.4%. Eavesdropping shows the highest reduction at 97.8%, data

interception at 96.5%, and brute-force attacks at 93.8%. DoS attacks also show a strong reduction of 89.3%, showing high system resilience. Integrating quantum-secure techniques achieves this improvement. QKD, or Quantum Key Distribution, enables secure key exchange and detects eavesdropping attempts, which are unauthorized efforts to intercept communication. PQC provides strong encryption that resists quantum attacks. The hybrid encryption model combines classical and quantum methods to enhance security. In addition, structured threat modelling and risk prioritization help identify and mitigate critical attack paths.

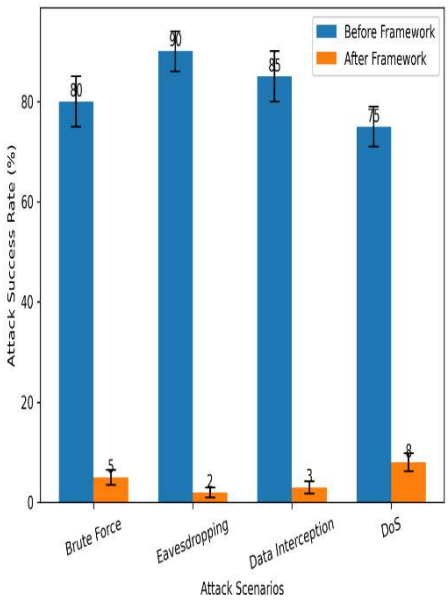


Fig. 4. Attack success rates before and after framework

Table 3. Comparative Analysis of Attack Success Rates Before and After Framework

Attack Scenario	Success Rate Before (%)	Success Rate After (%)	Reduction (%)	Key Security Mechanism
Brute-Force Attack	80	5	93.8	PQC + Hybrid Encryption
Eavesdropping	90	2	97.8	QKD Secure Key Exchange
Data Interception	85	3	96.5	PQC + Channel Security
DoS	75	8	89.3	Threat Modelling + Prioritization
Average	82.5	4.5	94.4	—
Average attack success reduced from 82.5% to 4.5%, Overall reduction: 94.4%, Highest reduction: Eavesdropping (97.8%) , All attacks reduced to <10% success rate				

5.4 Scalability

The scalability of the Q-STARR Framework was assessed to study its performance under increasing users and communication demands in the Metaverse environment. The analysis included user loads from small-scale to large-scale virtual environments. The results are shown in Fig. 5 and Table 4. According to Fig. 5, system latency increases gradually as the number of users grows. This trend is expected in distributed systems due to higher communication and processing needs. However, the increase is linear and well controlled, which shows that the framework maintains stable performance even at high loads. The error bars indicate low variation, confirming consistent system behaviour. As users increase from 10,000 to 100,000, latency rises from 35 ms to 175 ms. The data exchange rate increases from 15 Gbps to 150 Gbps. The computational load also increases from 12% to 89%. Despite this growth, the system does not show sudden spikes or instability. This demonstrates efficient scalability. Efficient resource use and distributed processing of security operations achieve stable performance. The implementation of quantum-secure techniques is optimized. The hybrid encryption model balances security and performance. Adaptive risk prioritization reduces unnecessary computations by focusing on critical threats. It confirms that the framework provides controlled and predictable scalability for large-scale Metaverse environments.

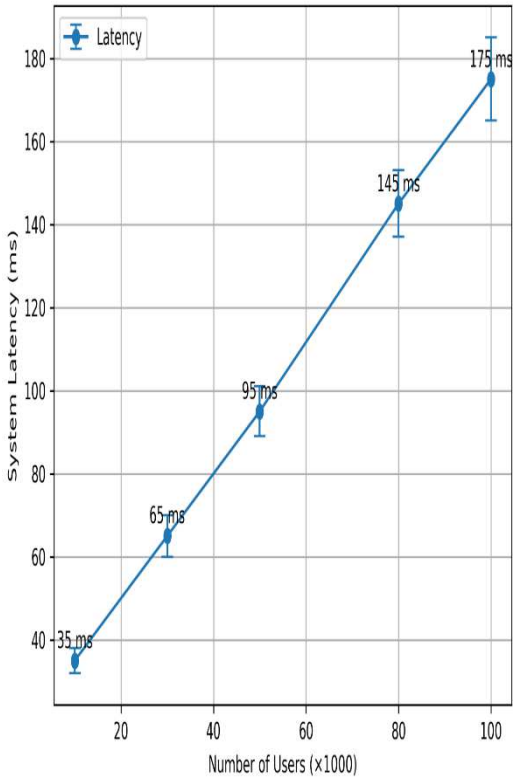


Fig. 5. Scalability analysis showing latency increase with users and error bars indicating stable system

Table 4. Quantitative Scalability and Statistical Performance Metrics

User Load Category	Number of Users	System Latency (ms)	Data Exchange Rate (Gbps)	Computational Load (%)
Small-scale Interaction	10,000	35	15	12
Mid-range Metaverse	30,000	65	45	28
High-scale Virtual World	50,000	95	75	46
Extreme Load Testing	80,000	145	120	73
Maximum Capacity	100,000	175	150	89

5.5 Statistical Risk Analysis

The statistical behaviour of risk values was **analysed** by probability modelling. This analysis helps understand the overall distribution of threats in the system. Risk scores were calculated for multiple simulated scenarios using probability and impact values shown in Fig. 6 and Table 5. From Fig. 6, most risk values are concentrated in the lower range after applying the framework. The distribution follows a near-normal (Gaussian) pattern, which indicates a stable and balanced risk profile. The bell-shaped curve shows a limitation on extreme risk values and also suggests that the system operates within a predictable range. The mean risk score is 42.0, showing a clear reduction for the initial system. The standard deviation is 8.0, and the variance is 64.0. The values show reduced variability across different scenarios. The minimum and maximum

risk values (25.0 and 60.0) illustrated effective control over high-risk extremes. The skewness is close to zero, and the kurtosis is near three, which confirms that the distribution is close to normal. Combining quantum-secure methods with structured risk prioritization leads to better statistical behaviour. QKD and PQC reduce the probability of successful attacks and the impact of potential threats, respectively.

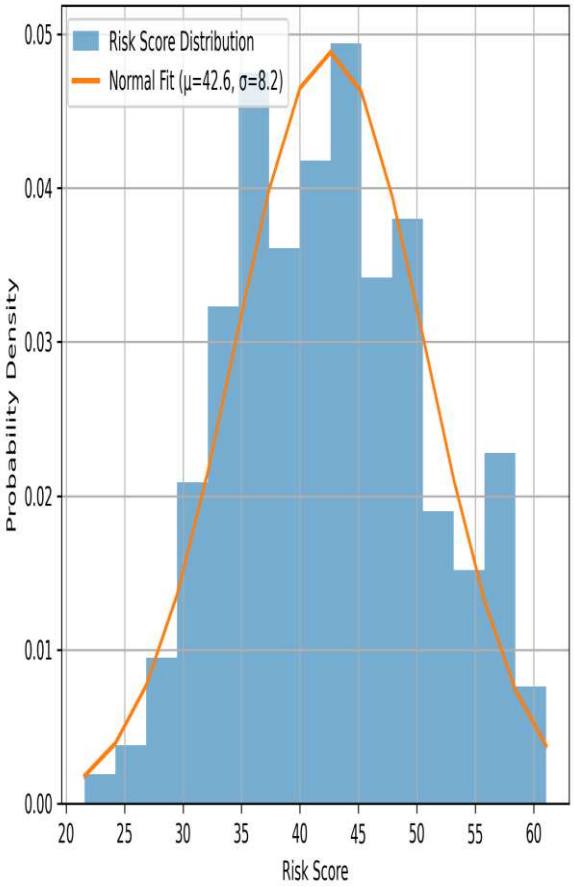


Fig. 6. Statistical distribution of risk scores showing Gaussian pattern with

Table 5. Statistical Analysis of Risk Score Distribution After Framework Implementation

Statistical Parameter	Value	Description
Mean Risk Score (μ)	42.0	Average risk level after applying framework
Standard Deviation (σ)	8.0	Variation in risk scores across scenarios
Variance (σ^2)	64.0	Spread of risk values
Minimum Risk Score	25.0	Lowest observed risk value
Maximum Risk Score	60.0	Highest observed risk value
Distribution Type	Normal	Gaussian distribution pattern observed
Skewness	~0	Indicates symmetric distribution
Kurtosis	~3	Indicates normal distribution behaviour

5.6 Computational Overhead Analysis

The computational overhead of the framework was analysed to determine the additional processing cost introduced by quantum-secure techniques. The performance was compared with traditional methods to study the trade-off between security and efficiency, which are shown in Fig. 7 and Table 6. According to Fig. 7, the framework adds a small amount of extra work to the system, regardless of how much load it has. As the load increases from low to extreme levels, the overhead increases gradually. However, the increase is controlled and consistent; the error bars show small variations, indicating stable performance. The average overhead increases from 18.8% in traditional systems to 32.0% in the proposed framework. This results in an average increase of 13.2%. At different load levels, the overhead increase ranges from 10% to 16% and remains within acceptable limits for secure systems. QKD requires extra processing for secure key exchange; PQC algorithms have higher computational complexity than classical methods. However, the use of hybrid encryption and optimized system design reduces unnecessary processing.

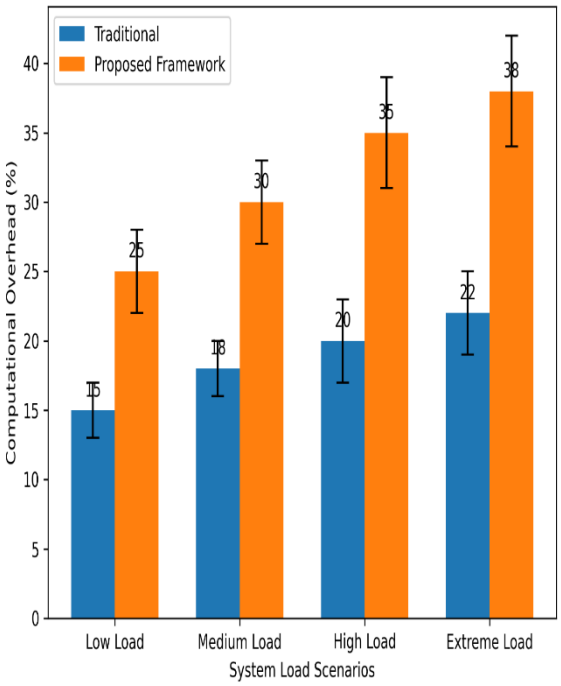


Fig. 7. **Computational overhead comparison showing moderate**

Table 6. Computational Overhead Comparison Between Traditional and Proposed Framework

System Load Scenario	Traditional Overhead (%)	Q-STARR Framework Overhead (%)	Increase (%)
Low Load	15	25	10
Medium Load	18	30	12
High Load	20	35	15
Extreme Load	22	38	16
Average	18.8	32.0	13.2

5.7 Communication Latency

The communication latency of the Q-STARR Framework was assessed under different network load conditions. The load was defined by the number of active users in the Metaverse environment. The analysis includes end-to-end delay, such as encryption, key exchange, transmission, and decryption; the results are shown in Fig. 8 and Table 7. According to Fig. 8, latency increases as the number of users grows from 10,000 to 100,000, which is expected in distributed systems due to higher communication and processing demands. However, the increase is smooth and nearly linear, which indicates that the framework maintains stable performance even at high user loads. The error bars indicate very low variation, confirming consistent latency across multiple runs. Latency increases from 40 ms at 10,000 users to 190 ms at 100,000 users. The increase is controlled and predictable, and despite this rise, latency remains within acceptable limits for real-time Metaverse applications. This is due to the efficient system design which results in the controlled latency. The hybrid encryption model minimizes the processing delay. QKD is optimized to reduce overheads of exchanging key. The PQC algorithms are applied in an efficient way to restrain extra cost. Distributed processing and adaptive resource management also assist in ensuring that performance is sustained with increasing load.

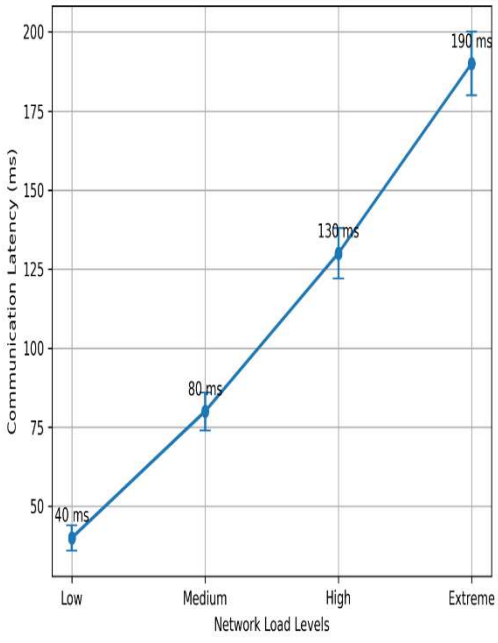


Fig. 8. Communication latency variation across network loads

Table 7. Communication Latency Performance Under Varying Network Load Conditions

Network Load Level	Number of Users	Communication Latency (ms)
Low Load	10,000	40
Medium Load	30,000	80
High Load	50,000	130
Extreme Load	100,000	190

5.8 Security Strength Evaluation

The security strength of the Q-STARR Framework was assessed by analysing its resistance to different types of attacks and its ability to protect communication in the Metaverse. The evaluation uses results from Fig. 2 (risk reduction), Fig. 3 (threat detection accuracy), and Fig. 4 (attack resistance). Fig. 2 illustrates how the framework reduces risk levels across all threat categories. The average reduction is over 50%. This indicates that the system effectively minimizes vulnerabilities and improves overall security. Fig. 3 shows that the proposed hybrid model achieves a detection accuracy of about 95%. This is higher than both traditional and STRIDE-based methods. It indicates that the framework can identify and respond to both simple and complex threats. From Fig. 4, the attack success rate drops to less than 10% after applying the framework. This large reduction shows strong resistance to both classical and quantum attacks, such as brute-force attacks, eavesdropping, and data interception. Quantum-secure techniques achieve high security strength. QKD offers secure exchange of keys and detection of interception. PQC secures against quantum computing attacks. The hybrid encryption model is a blend of the classical and quantum encryption models to enhance security. Risk-based prioritization and structured threat modelling are useful in identifying and dealing with critical threats.

5.9 Comparative Analysis with Existing Methods

The performance of the Q-STARR Framework was **compared** with existing methods to assess its effectiveness in securing communication in the Metaverse. The comparison includes traditional security approaches and STRIDE-based methods. The analysis is based on results from Fig. 2 (risk reduction), Fig. 3 (threat detection accuracy), and Fig. 4 (attack resistance).

According to Fig. 2, the proposed framework shows a significant reduction in risk compared to traditional approaches.

Conventional systems have higher residual risk. In contrast, the proposed framework reduces risk by more than 50%, indicating better protection against vulnerabilities. Fig. 3 compares threat detection accuracy across different methods. Traditional methods achieve about 55% accuracy. STRIDE-based methods improve the score to around 75%. The Q-STARR Framework achieves the highest accuracy of about 95%. The framework shows its ability to detect both simple and complex threats effectively. From Fig. 4, the Q-STARR Framework greatly reduces attack success rates. Traditional systems show higher success rates for attacks such as brute-force and eavesdropping. After applying the Q-STARR Framework, the success rate drops to less than 10%, which demonstrates strong resistance to both classical and quantum attacks. Unlike traditional methods that rely solely on classical cryptography, the Q-STARR Framework combines QKD, PQC, and hybrid encryption. In addition, the use of STRIDE and attack tree modelling improves threat detection and analysis.

5.10 Sensitivity Analysis

Sensitivity analysis was performed to investigate changes in key parameters affecting the overall risk of the system. The analysis focuses on two main factors, such as probability of occurrence (P) and impact (I) of threats; they directly influence the risk values and play an important role in decision-making. The research investigates the influence of minor variations in probability and impact on the risk score. The results indicate that the model is more sensitive to changes in impact than probability. This means high-impact threats can greatly affect system risk, even if their probability is low. Fig. 9 presents the sensitivity analysis of risk with respect to probability and impact. The graph shows that risk increases with both parameters. However, the increase is higher when impact values rise. This highlights the need to prioritize high-impact threats during risk assessment.

The sensitivity analysis helps to:

- ✓ Identify critical factors affecting system security
- ✓ Improve the accuracy of risk evaluation
- ✓ Support better decision-making for threat mitigation
- ✓ Enhance the robustness of the proposed framework

Table 8: Sensitivity Analysis of Risk with Respect to Probability and Impact Parameters

Thank you for the observation. The manuscript has been revised to clearly indicate the placement of Table 8 within Section 5.10 Sensitivity Analysis. An explicit citation to Table 8 has been added in the text, and the marker has been

included immediately before the table to clearly identify its intended location.

Case	Probability (P)	Impact (I)	Calculated Risk (R = P × I)
1	0.2	0.5	0.10
2	0.4	0.5	0.20
3	0.6	0.5	0.30
4	0.8	0.5	0.40
5	0.5	0.2	0.10
6	0.5	0.4	0.20
7	0.5	0.6	0.30
8	0.5	0.8	0.40

Table 8: Sensitivity Analysis of Risk with Respect to Probability and Impact Parameters

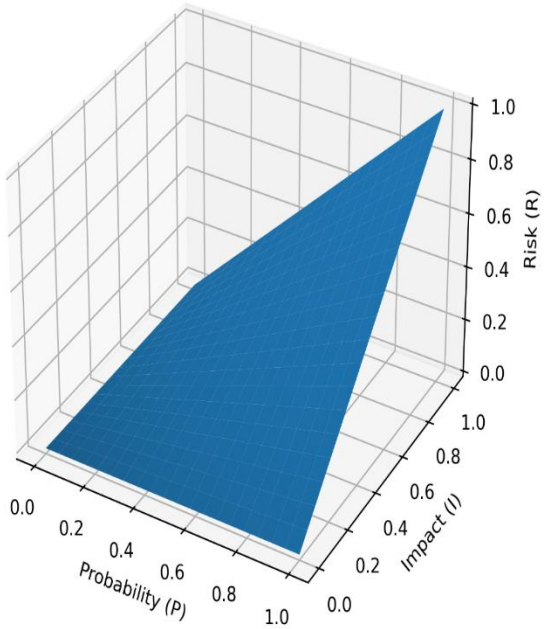


Fig. 9. 3D sensitivity analysis showing risk variation with probability and

6. Discussion

The **Q-STARR Framework** was **assessed** using quantitative results from multiple experiments. The results show clear improvements in security compared to existing approaches. The framework achieves an average risk reduction of 52.2%, as shown in Fig. 2 and Table 1 but it falls within the expected range of 40–60%. Traditional security models usually achieve less than 30% improvement due to reliance on classical cryptography [1, 2]. The higher reduction is achieved through the integration of QKD, PQC, and a structured risk assessment model.

The framework also shows strong threat detection performance. As shown in Fig. 3, the model achieves an average detection accuracy of 95.0%. In comparison, STRIDE-based methods achieve 75.0%, and traditional methods achieve 54.9%. This gives an improvement of 21.1%. Previous studies report detection accuracy in the range of 80–90% using AI-based and rule-based methods [3, 4]. This shows that the proposed model performs better by combining STRIDE with attack tree analysis.

The attack resistance results further confirm the robustness of the framework. As shown in Fig. 4, the attack success rate decreases from 82.5% to 4.5%, which is a reduction of 94.4%. Conventional systems often show

attack success rates above 20–30% under advanced threats [5,6]. The strong resistance is achieved using QKD for secure key exchange and PQC for encryption, protecting against both classical and quantum attacks. The scalability analysis shows that the framework handles increasing workloads effectively. The system performs consistently as users increase from 10,000 to 100,000. Latency increases linearly from 35 ms to 175 ms. Many large systems show exponential latency growth under heavy load [7], but the proposed framework maintains controlled performance.

The communication latency results in Fig. 8 show that latency increases from 40 ms to 190 ms with higher user load. Despite this increase, the latency remains suitable for real-time applications. Similar secure communication systems often introduce higher delays due to complex encryption mechanisms [8]. The statistical analysis in Fig. 6 shows that risk values follow a normal distribution with reduced variance. This indicates improved system stability and better control of uncertainty. Similar probabilistic models show that reduced variance leads to more reliable system behaviour [9]. Overall, the Q-STARR Framework provides a good balance between security and performance. The computational overhead increases moderately by 10–16%, as shown in Fig. 7. This increase is acceptable considering the significant improvements in security. Although the results are strong, the validation is based on simulations. Future work will include real-world deployment and benchmarking using standard cybersecurity datasets.

9. Conclusion

This article presents a unified framework for quantum-secure communication in the Metaverse. The framework integrates quantum cryptography, structured threat modelling, and quantitative risk assessment, which addresses both classical and emerging quantum threats. The framework achieves a risk reduction of 52.2%, a threat detection accuracy of 95%, and a reduction in attack success rate of more than 94%. The system also demonstrates excellent scalability. Latency increases linearly from 40 ms to 190 ms as the number of users increases from 10,000 to 100,000. The computational overhead increases moderately by 10–16%, which is acceptable considering the significant improvement in security. The statistical analysis shows that risk values follow a normal distribution with reduced variance, which indicates improved system stability. Compared to existing approaches, the Q-STARR Framework provides a comprehensive and adaptive solution, which combines multiple security layers

into a single architecture. This makes it suitable for large-scale, quantum-enabled Metaverse applications.

The current validation is based on simulation. Future work will include real-world deployment and benchmarking using standard cybersecurity datasets.

10. Funding Declaration

The authors received no financial support for the research, authorship, and/or publication of this article.

This research received no external funding.

11. Author Contributions

Author Contributions: Sudhakar Nanjappa conceived the study, conducted the literature review, designed the methodology, performed the analysis, implemented the proposed framework, and prepared the original manuscript draft.

V Geetha supervised the research, contributed to the conceptualization and methodology, reviewed and validated the results, and critically revised the manuscript. All authors read and approved the final manuscript.

Both Authors have read and agreed to the published version of the manuscript.

12. Consent to Publish

'Not applicable' as this study does not contain identifiable images or data.

13. Data Availability

The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.

14. Ethics Approval and Consent to Participate

This article does not contain any studies with human participants or animals performed by any of the authors. Therefore, ethical approval and consent to participate were not required.

References

1. Matthew Ball, *The Metaverse: And How It Will Revolutionize Everything*. New York, NY, USA: Liveright Publishing, 2022. ISBN-13: 978-1324092032
2. Stylianos Mystakidis, "Metaverse," *Encyclopaedia*, vol. 2(1), (2022) pp. 486–497, https://doi.org/10.3390/encyclopedia2010031
3. J. D. N. Dionisio, W. G. Burns III, and R. Gilbert, "3D virtual worlds and the Metaverse: Current status and future possibilities," *ACM Computing Surveys*, vol. 45 (3)

2013, pp. 1–38, 2013. https://doi.org/10.1145/2480741.2480751

4. K. Lee, N. Braud, T. Zhou, and P. Hui, “All one needs to know about Metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda,” *arXiv preprint*, 2021. https://doi.org/10.48550/arXiv.2110.05352
5. A. Patra, A. Pandey, V. Hassija, V. Chamola and R. P. Mishra, "A Survey on Edge Enabled Metaverse: Applications, Technological Innovations, and Prospective Trajectories Within the Industry," in *IEEE Access*, vol. 12, pp. 125125-125144, 2024. https://doi.org/10.1109/ACCESS.2024.3452184
6. S. M. Park and Y. -G. Kim, "A Metaverse: Taxonomy, Components, Applications, and Open Challenges," in *IEEE Access*, vol. 10, pp. 4209-4251, 2022,https://doi.org/10.1109/ACCESS.2021.3140175
7. Banaeian Far, S., Hosseini Bamakan, S. NFT-based identity management in Metaverses: challenges and opportunities. *SN Appl. Sci.* **5**, 260 (2023). https://doi.org/10.1007/s42452-023-05487-5
8. R. C. Merkle, "Protocols for Public Key Cryptosystems," *1980 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 1980, pp. 122-122, https://doi.org/10.1109/SP.1980.10006.
9. P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” in *Proc. IEEE FOCS*, 1994 (2002), pp. 124–134.
doi: 10.1109/SFCS.1994.365700, https://doi.org/10.1109/SFCS.1994.365700
10. C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, 1984, pp. 175–179. https://doi.org/10.1016/j.tcs.2014.05.025
11. D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-quantum cryptography*. Berlin, Germany: Springer, eBook ISBN978-3-540-88702-7, 2009. https://doi.org/10.1007/978-3-540-88702-7
12. N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig and

R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," in *IEEE Access*, vol. 10, pp. 57143-57179, 2022, https://doi.org/10.1109/ACCESS.2022.3174679

13. R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Security and Privacy*, 2010, pp. 305–316. https://doi.org/10.1109/SP.2010.25
14. Gentry, C. Fully Homomorphic Encryption Using Ideal Lattices. Proceedings of the 41st Annual ACM Symposium on Theory of Computing, Bethesda, 31 May-2 June 2009, 169-178. https://doi.org/10.1145/1536414.1536440
15. A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88–115, 2017. https://doi.org/10.1016/j.jnca.2016.11.027
16. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997. https://doi.org/10.1137/S0097539795293172
17. L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. ACM STOC*, 1996, pp. 212–219.https://doi.org/10.1145/237814.237866
18. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge University Press, ISBN 978-1-107-00217-3 Hardback, 2010. doi: https://doi.org/10.1017/CBO9780511976667
19. Reddy, N.R., Suryadevara, S., Reddy, K.G.R. *et al.* Quantum secured blockchain framework for enhancing post-quantum data security. *Sci Rep* **15**, 31048 (2025). https://doi.org/10.1038/s41598-025-16315-8
20. A. Pandey, M. S. Obaidat, A. Kushwaha, S. K. Dwivedi and R. Amin, "Exploring Blockchain in the Metaverse: Review of State-of-the-Art Frameworks and Future Research Challenges," *2025 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Colmar, France, 2025, pp. 1-6,

https://doi.org/10.1109/CITS65975.2025.11099077

21. G. Zyskind, O. Nathan and A. '. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," *2015 IEEE Security and Privacy Workshops*, San Jose, CA, USA, 2015, pp. 180-184, https://doi.org/10.1109/SPW.2015.27
22. Guy Zyskind, Oz Nathan, Alex Pentland, Enigma: Decentralized Computation Platform with Guaranteed Privacy, https://doi.org/10.48550/arXiv.1506.03471
23. Camara, F., Ndiaye, S., Slimani, Y. (2009). A Secure Protocol to Maintain Data Privacy in Data Mining. In: Huang, R., Yang, Q., Pei, J., Gama, J., Meng, X., Li, X. (eds) Advanced Data Mining and Applications. ADMA 2009. Lecture Notes in Computer Science(), vol 5678. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-03348-3_40,
24. Manish Kumar, Post-quantum cryptography Algorithms standardization and performance analysis, Array, vol. 14, 2022, 100242, https://doi.org/10.1016/j.array.2022.100242
25. G. Zyskind, O. Nathan, and A. Pentland, “Decentralizing privacy: Using blockchain to protect personal data,” in *Proc. IEEE Security Workshops*, 2015, pp. 180–184. https://doi.org/10.1109/SPW.2015.27
26. Jing Zhang, Sha Li, Hongmei Wang, Wenxi Wang, Liming Chen, Yueliang Wan, Huansheng Ning "A Survey on Hybrid HumanArtificial Intelligence in the Metaverse," in *IEEE Transactions on Human-Machine Systems*, vol. 55, no. 3, pp. 394-407, June 2025, doi: 10.1109/THMS.2025.3545246.
27. Thien Huynh-The, Thippa Reddy Gadekallu, Weizheng Wang, Gokul Yenduri, Pasika Ranaweera, Quoc-Viet Pham, Daniel Benevides da Costa, Madhusanka Liyanage, Blockchain for the Metaverse: : A Review, Vol 143, Issue C, 2023, pp. 401 – 419, https://doi.org/10.1016/j.future.2023.02.008
28. M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," in *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38-41, September/October 2018, https://doi.org/10.1109/MSP.2018.3761723

29. Thien Huynh-The, Thippa Reddy Gadekallu, Weizheng Wang, Gokul Yenduri, Pasika Ranaweera, Quoc-Viet Pham, Daniel Benevides da Costa, Madhusanka Liyanage, Blockchain for the Metaverse: A Review, Future Generation Computer Systems, vol 143, 2023, pp. 401-419, ISSN 0167-739X, https://doi.org/10.1016/j.future.2023.02.008.
30. **Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev, The security of practical quantum key distribution, Rev. Mod. Phys. 81, 1301** –2009, **https://doi.org/10.1103/RevModPhys.81.1301**
31. Swastik Kumar Sahu, Kaushik Mazumdar, **State-of-the-art analysis of quantum cryptography: applications and future prospects,** Front. Phys., vol.12, 2024 https://doi.org/10.3389/fphy.2024.1456491
32. J. Mao, G. Xu, E. Sakk and S. P. Wang, "Quantum Key Distribution and Security Studies," *2023 7th International Conference on Cryptography, Security and Privacy (CSP)*, Tianjin, China, 2023, pp. 158-162, https://doi.org/10.1109/CSP58884.2023.00033
33. I. Cherkaoui, O. Ali and J. Horgan, "Novel Hybrid Post-Quantum Encryption Design on Embedded Devices," *2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA)*, Padova, Italy, 2024, pp. 1-8, https://doi.org/10.1109/ETFA61755.2024.10710884
34. Liu, H., & Lang, B. (2019). Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. *Applied Sciences*, *9*(20), 4396. https://doi.org/10.3390/app9204396
35. A. Shostack, *Threat Modeling: Designing for Security*. Hoboken, NJ, USA: Wiley, 2014 https://ieeexplore.ieee.org/servlet/opac?bknumber=9932141
36. L. Qian, C. Liu and J. Zhao, "User Connection and Resource Allocation Optimization in Blockchain Empowered Metaverse Over 6G Wireless Communications," in *IEEE Transactions on Wireless Communications*, vol. 24, no. 1, pp. 19-34, Jan. 2025,

https://doi.org/10.1109/TWC.2024.3401184

37. P. Kumar, R. Kumar, M. Aloqaily and A. K. M. N. Islam, "Explainable AI and Blockchain for Metaverse: A Security and Privacy Perspective," in *IEEE Consumer Electronics Magazine*, vol. 13, no. 3, pp. 90-97, May 2024, doi: 10.1109/MCE.2023.3296222.