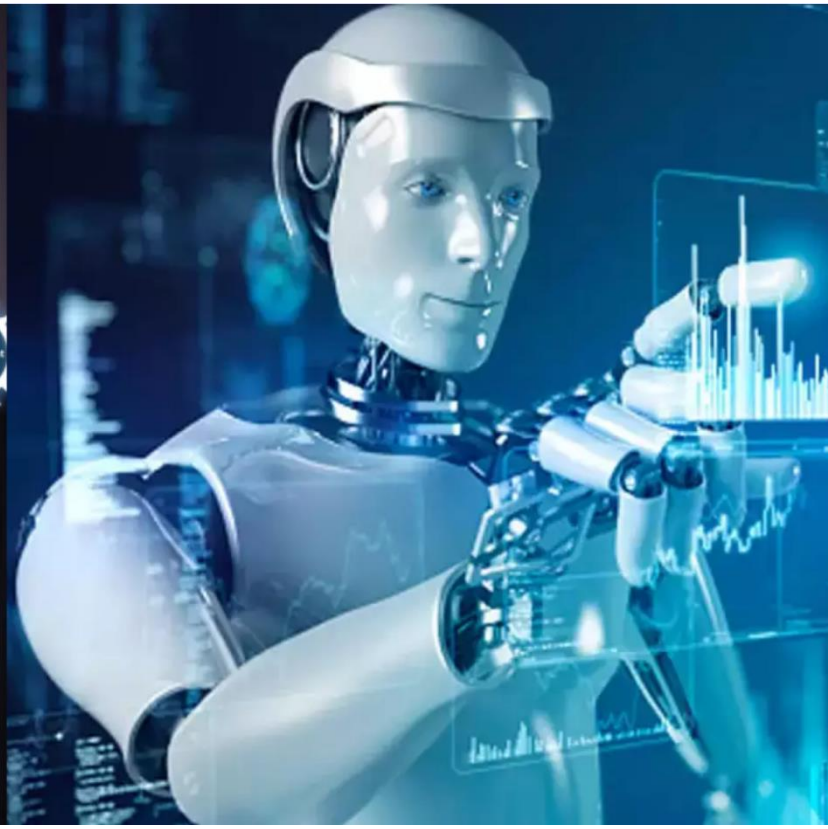
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503410|

CyberQ – Quantum-enhanced Cybersecurity Simulator

V Chandra Sekhar Reddy[1], K Nishitha[2], R Sushma[3], A Neha[4]

Associate Professor, Department of CSE, ACE Engineering College, Hyderabad, Telangana, India[1]

IV B.Tech Students, Department of CSE, ACE Engineering College, Hyderabad, Telangana, India [2,3,4]

ABSTRACT: Cyber-attacks and understanding them has become a very important concept for security. Classical simulators use classical computer algorithms to develop cybersecurity systems. Although quantum acts as a easy route to hack using quantum enabled cyber-attacks it also provides answer to this by providing quantum secure cryptographic algorithms. This project discusses a quantum enhanced cybersecurity simulator which is a lightweight and modular framework. It uses quantum concepts to improve classical systems. The system consists of two modules respectively. The first module analyses classical cybersecurity and the second module develops quantum-inspired high-randomity encryption key generation. This is possible with the help of quantum concepts and tools such as Qiskit. These keys are evaluated with the help of simulated classical brute force attacks. This system is also equipped with an attack classification method using rules. The results obtained from the attack simulation are also visualized in terms of bar graphs to have a better understanding.

KEYWORDS: Cybersecurity, Quantum-Inspired Computing, Brute-Force Attack Simulation, Key Generation, Modular Architecture, Attack Classification, Data Visualization, Secure Systems

I. INTRODUCTION

The research will be conducted within the framework of the development of a modular cybersecurity platform using methods of classical analysis, as well as ideas based on quantum computing to better comprehend the behaviours of security systems. The developed platform will include a web interface for interaction with users and for attack classification, as well as a simulator for key generation and brute force attack analysis.

II. LITERATURE SURVEY

Cybersecurity has attracted significant attention in research owing to the rising complexity and incidence of cyberattacks. Conventional approaches in the field of cybersecurity mainly involve signature-based approach, rules-based approach, and conventional encryption methods. These approaches have helped identify existing threats but tend to falter when dealing with emerging attacks that are new. A number of studies have tried to utilize techniques such as data analysis and visualization to enhance detection of threats as well as to better understand cyberattack patterns.

QKD systems used at present are heavy and no simulation is available. There is no such thing as an integrated platform that would incorporate both the conventional cybersecurity approach and the quantum-inspired cybersecurity approach in one coherent platform. This problem can be addressed through the design of a system that integrates rule-based attack categorization with quantum-inspired key creation and attack modeling.

III. METHODOLOGY

This suggested model is based on a modular design that includes conventional cybersecurity analysis along with quantum-inspired simulation modules. The framework has been segmented into several steps for ensuring effective data flow.

At first, the system will be used by users via the website designed with Django. Here, users will be able to sign up and log in, while providing the necessary inputs regarding cybersecurity. These inputs are then analyzed by an attack

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503410|

classification engine based on the rule-based approach. It classifies the attacks by analyzing text inputs with respect to pre-defined keywords.

Similarly, there is also an inclusion of a simulation module that uses quantum randomness principles to create keys for encryption purposes. These keys are subjected to simulations of a brute-force attack and analyzed based on certain parameters, which may include number of attempts taken, as well as the time taken to crack the code. The data obtained is then presented in various chart forms.

The modular approach guarantees that every element can operate independently but still contribute to the functionality of the whole system. This methodology also enables the seamless incorporation of real quantum computing tools like Qiskit into the future.

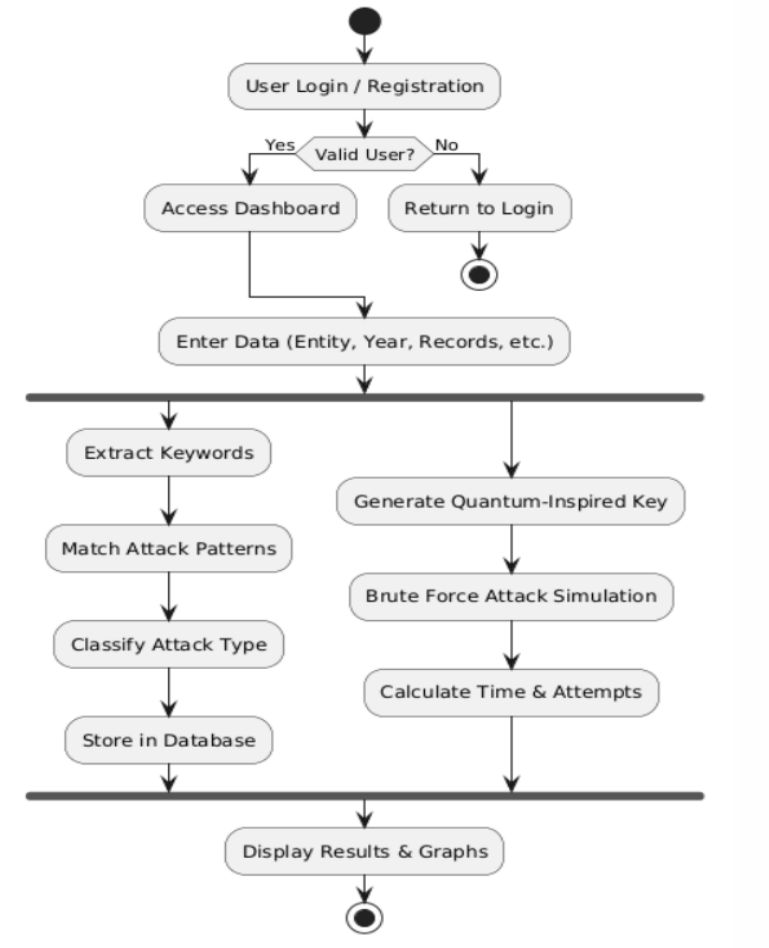


Fig 3.1 CyberQ Methodology

IV. SYSTEM ARCHITECTURE

The suggested system adopts a modular and hierarchical architecture incorporating a web-based cybersecurity analysis module along with a quantum-motivated simulation module. Initially, users go through the system using web interface developed in the Django framework in the simulator. It is responsible for handling the authentication of users, input data, and navigation. The second level has two parallel processing units. One of them is the analysis module that analyses the input data of the users based on a rule-based attack classification process for the mean time.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503410|

These classified results are saved in a relational database (MySQL). The other part of this application is the quantum-inspired simulation module that generates very random encryption keys acting like a key generated using Quantum hardware. Then we test their strength through simulation by brute force attacks. Both components work independently but together help achieve the required analysis process.

In the lower layer, the results provided from this system include visualization and results of the analysis to make it easier for user to have a better understanding of the output. This structure was chosen specifically as it made future integration with a real quantum framework like Qiskit possible.

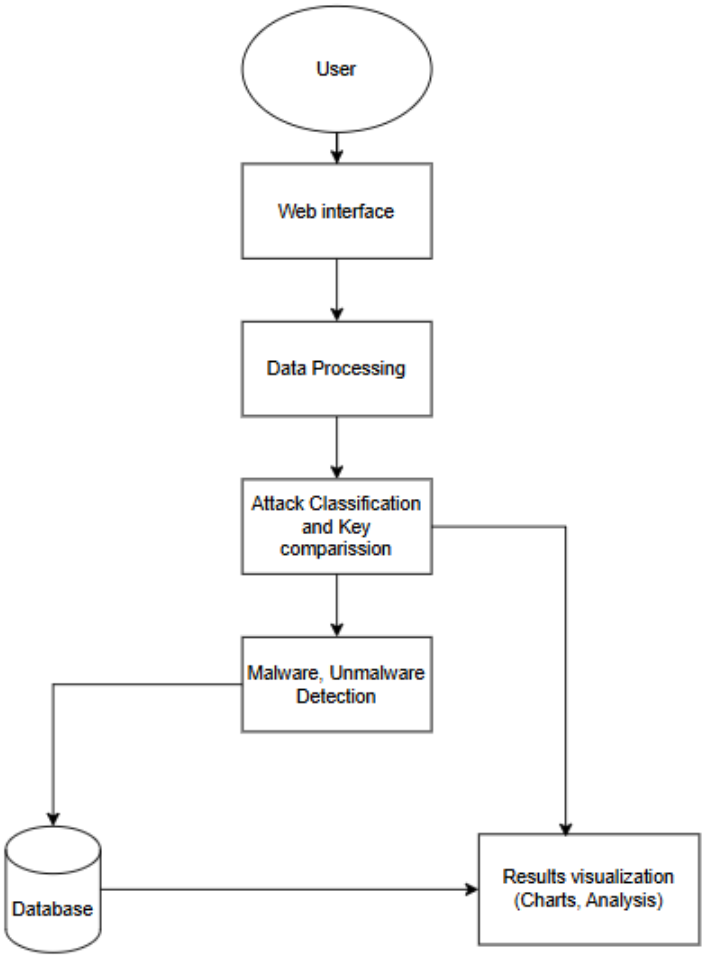


Fig 4.1 System Architecture

V. RESULTS

Various input values were used for testing purposes, and the performance of the attack classifier and quantum-inspired simulation model were assessed. The findings indicate that the rule-based technique is capable of grouping different attacks through their respective input values.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503410|

It was shown that the performance of the classical and quantum-inspired encryption techniques was nearly equal due to their randomness, and the efficiency was determined using time and attempts. The outcomes were represented using diagrams.

Fig 5.1 CyberQ Login Page

Fig:5.2 User Interface Page

Fig 5.3 Output page

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503410|

Fig 5.4 CyberQ Analysis Page

VI. CONCLUSION

The developed solution has proved that it is possible to design a modular security system by combining classical analysis with quantum simulation. People enter needed information and run the system. This helps in detection, and

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503410|

also simulation of how keys and attacks work. Although the quantum aspect has been designed to work as a simulation model, its use proves successful in explaining enhanced randomness in key generation processes. This solution can be considered a useful means for educational purposes to understand current cybersecurity problems.

VII. FUTURE SCOPE

This could also be extended further by incorporating actual quantum computing systems like Qiskit, which would enable replacing the simulated quantum computing component with a true quantum key distribution system. Furthermore, the attack detection component may also be improved through the application of machine learning methods. We plan to add attack simulation on networks and integrate both modules to produce a system that works as a tool which helps people understand how quantum and classical can work together.

REFERENCES

[1] Nielsen, M. A., and Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press.
Link: https://doi.org/10.1017/CBO9780511976667
[2] Cross, A. W., Bishop, L. S., Smolin, J. A., and Gambetta, J. M. (2018). Open Quantum Assembly Language. arXiv.
Link: https://arxiv.org/abs/2005.11401
[3] Qiskit Development Team (2023). Qiskit: An Open-source Framework for Quantum Computing.
Link: https://arxiv.org/abs/2508.11867
[4] Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson Education.
Link: https://arxiv.org/abs/2508.06401
[5] Scarfone, K., and Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology (NIST).
Link: https://ijcesen.com/index.php/ijcesen/article/view/4248
[6] Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3. IETF RFC 8446.
Link: https://datatracker.ietf.org/doc/html/rfc8446
[7] Gajbhiye, M., and Dumbere, D. (2016). Diffie-Hellman Key Exchange Algorithm with Man-in-the-Middle Attack (MITM).
Link: https://www.researchgate.net/publication/303548131
[8] Adu-Kyere, A., Nigussie, E., and Isoaho, J. (2020). Quantum Key Distribution: Modeling and Simulation through BB84 Protocol Using Python3.
Link: https://doi.org/10.1007/s11277-020-07330-0

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details