Elevating Automotive Cyber security with Quantum Computing

A.Johnbasco Vijay Anand, Dr. S. Sukumaran
Ph.D. Research Scholar, Department of Computer Science, Erode Arts and Science College, Erode, TN, India
Associate Professor of Computer Science, Erode Arts and Science College, Erode 638009, TN, India

***Abstract*— The advent of connected and autonomous vehicles (CAVs) has revolutionized the automotive industry, but it has also increased the vulnerability to cyber security[1] threats[2]. Traditional cyber security measures are struggling to keep up with the evolving sophistication of attacks targeting CAVs, necessitating the exploration of cutting-edge technologies. Quantum computing offers a promising solution for enhancing automotive cyber security. This research paper investigates the potential of quantum computing in elevating CAV security through applications such as secure communication, data integrity, authentication, intrusion detection, and anomaly detection. By leveraging the unique computational power of quantum computing, we can strengthen the security framework of CAVs and ensure a safer future for connected and autonomous vehicles. Furthermore, customization of quantum approaches like Quantum Key Distribution (QKD), Quantum Optimization, and Quantum Data Encoding based on specific use cases becomes imperative to maximize their effectiveness in automotive cyber security. This research aims to shed light on the significance of quantum computing and the need for customization in order to address the complex security challenges posed by the next-generation automotive ecosystem.**

***Index Terms* —Automotive Cyber Security, ISO 21434, Quantum Computing, Security**

I. INTRODUCTION

As the automotive industry embraces rapid digital transformation, vehicles are becoming more connected and autonomous. The automotive industry has witnessed a revolutionary transformation with the introduction of connected and autonomous vehicles (CAVs). These vehicles have ushered in a new era of innovation, enabling advanced functionalities such as Vehicle-to-Vehicle (V2V) and Vehicle-to-Everything (V2X) communication. However, the increased connectivity in CAVs has also exposed them to a higher risk of cyber security threats. Traditional cyber security measures, which have proven effective for conventional vehicles, are struggling to cope with the evolving sophistication of attacks targeting the V2V and V2X capabilities of CAVs. As a result, there is an urgent need to explore cutting-edge technologies capable of bolstering automotive cyber security.

Quantum computing emerges as a compelling avenue for enhancing automotive cyber security in the context of V2V and V2X communication. With its remarkable computational power and unique properties, quantum computing offers promising solutions to the challenges posed by cyber threats in the automotive ecosystem.

This research paper aims to explore the potential of quantum computing in elevating the security of V2V and V2X communication, while also investigating its applications in data integrity, authentication, intrusion detection, and anomaly detection. By harnessing the inherent advantages of quantum computing, we can strengthen the security framework of CAVs and ensure a safer future for connected and autonomous vehicles.

Secure V2V and V2X communication is a critical aspect of automotive cyber security, as it forms the foundation for seamless and reliable information exchange among vehicles and their surrounding infrastructure. Quantum Key Distribution (QKD), a quantum-based cryptographic protocol, holds promise for establishing secure and unbreakable communication channels, safeguarding sensitive data exchanged in V2V and V2X scenarios from eavesdropping and interception.

Ensuring data integrity is another crucial concern in automotive cyber security, particularly in the context of V2V and V2X communication. The integrity and authenticity of data transmitted and received within CAVs must be guaranteed to maintain the reliability and trustworthiness of the entire system. Quantum data encoding techniques can provide robust mechanisms to detect and prevent unauthorized alterations or tampering of data, thereby preserving its integrity.

As the field of automotive cyber security advances, customization of quantum approaches becomes essential to tailor them to the specific requirements of V2V and V2X communication. Customization involves adapting quantum techniques, such as QKD and Quantum Optimization, to address the unique challenges and characteristics of V2V and V2X scenarios, ensuring their optimal performance and effectiveness in enhancing automotive security.

By conducting a comprehensive investigation into the applications of quantum computing in secure V2V and V2X communication, data integrity, authentication, intrusion detection, and anomaly detection, this research paper aims to shed light on the potential of quantum computing in strengthening the cyber security framework of CAVs. It also emphasizes the need for customization of quantum approaches to maximize their effectiveness in addressing the complex security challenges posed by the next-generation automotive ecosystem with V2V and V2X capabilities.

II. AUTOMOTIVE CYBER SECURITY CHALLENGES AND REMEDIATIONS FROM QUANTUM COMPUTING

The automotive industry's shift towards connected and autonomous vehicles has opened up new attack vectors for cybercriminals. These vehicles rely on complex software systems, communication networks, and sensors, making them susceptible to cyber threats [2] such as hacking, data breaches, and remote-control manipulation. Securing the vast amount of data generated by these vehicles, as well as ensuring the integrity and privacy of user information, presents a significant challenge. Quantum computing can play a vital role in addressing these vulnerabilities [3].

III. QUANTUM COMPUTING-A GAME CHANGER

Quantum computing leverages the principles of quantum mechanics to perform computations that are exponentially faster than classical computers. Its immense processing power enables it to tackle complex cryptographic problems, making it a potential game-changer in automotive cyber security. Here's how quantum computing can enhance security in various automotive domains:

A. Encryption and Cryptographic Systems:

Quantum computers have the potential to break conventional encryption algorithms, rendering existing security mechanisms obsolete. However, they can also provide more robust cryptographic solutions. Quantum-resistant algorithms, such as lattice-based or multivariate cryptography, can be implemented to protect sensitive data in connected vehicles and communication networks. These algorithms rely on mathematical problems that are difficult for both classical and quantum computers to solve, ensuring long-term security. The equation represents the probability of detecting an eavesdropper, Eve, in a quantum key distribution (QKD) protocol is

$$P\_d = 1 - (3/4)\verb|^|n$$

In this formula, P_d represents the probability of detecting Eve, n represents the number of key bits that Alice and Bob publicly compare, and (3/4)^n represents the probability that Eve's presence remains undetected for n key bits. By subtracting this probability from 1, we obtain the probability of successfully detecting an eavesdropper. To achieve a high probability of detecting Eve with a value of 0.999999999 (or 1 - 10^-9), the number of key bits that Alice and Bob need to publicly compare (n) is 72.

B. Secure Vehicle-to-Vehicle (V2V) and Vehicle-to-Everything (V2X) Communication:

Securing Next-gen disruptive technologies in the automotive industry including V2V and V2X required strong authentication and authorization of THINGS (Vehicles). Periodic firmware updates Over The Air (OTA) and SUMS needs fine tuning of the time at which these updates are to be pushed to vehicles. Eavesdropping is a major threat with possible MITM attacks unless strong protocols and handshaking methods are used in the process. Fig-a is an indicative image of how a typical OTA update happens. Apart from OTA, V2V and V2X communication systems enable vehicles to exchange vital information, improving road safety and traffic efficiency. However, these systems are susceptible to various attacks, including spoofing, tampering, and eavesdropping. Quantum key distribution (QKD) protocols [4] can leverage the unique properties of quantum mechanics to establish secure communication channels immune to eavesdropping attempts.

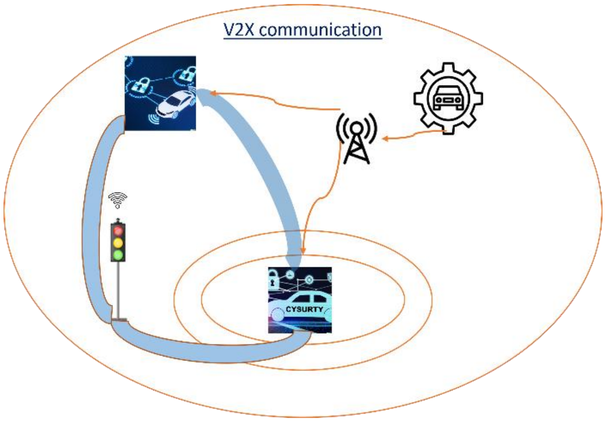

Fig-a: Indicative image of V2X enabling SOTA & SUMS

QKD ensures that the encryption keys used for secure communication cannot be intercepted or cloned, providing a higher level of security for V2V and V2X systems. This scenario can be addressed by making minor correction to the phase estimation calculation between the reference and received Quantum signals.

Actual calculation: $\Delta\varphi = \varphi\_received - \varphi\_reference$

Error correction : $\Delta\varphi = (\varphi\_received+0.27) - \varphi\_reference$

This correction factor shall enable early signals in case of V2V or V2X thereby invoking the protection factor of the keys stored in the Trusted platform Modules (TPM) of the vehicles.

C. Threat Detection and AI-Driven Security:

Quantum computing can also enhance threat [2] detection and analysis capabilities in automotive cyber security. With its exceptional processing power, quantum algorithms can quickly identify patterns and anomalies in large datasets, allowing for faster and more accurate detection of cyber threats. Furthermore, quantum machine learning algorithms can enhance anomaly detection and improve predictive capabilities, helping automakers stay one step ahead of evolving cyber threats.

IV. QUANTUM COMPUTING - ISO 21434 COLLABORATIVE OFFERINGS

A.ISO 21434: A Framework for Automotive Cyber security:

ISO 21434 provides a comprehensive framework to manage cyber security risks throughout the automotive lifecycle. It outlines processes, activities, and requirements necessary for the development, production, operation, maintenance, and decommissioning of vehicles. Key elements of ISO 21434 [19] include risk assessment, security requirements engineering, and validation and verification of cyber security measures. Integrating quantum computing into this framework can enhance cyber security in multiple areas.

B. Quantum Computing for Risk Assessment:

Risk assessment is a fundamental aspect of ISO 21434, aiming to identify potential vulnerabilities and threats throughout the automotive ecosystem. In addition to TARA(Threat Assessment and Risk Analysis - a kind of Threat modelling), Quantum computing can significantly augment risk assessment processes by enabling faster and more accurate analysis of complex scenarios and datasets. Quantum algorithms[5], such as quantum Monte Carlo simulations or Grover's algorithm, can accelerate the identification of vulnerabilities and the estimation of their impact, facilitating proactive cyber security measures.

C. Quantum-Resistant Cryptography:

ISO 21434 emphasizes the importance of cryptography in securing automotive systems. However, with the emergence of quantum computers, traditional cryptographic algorithms may become vulnerable. To address this concern, ISO 21434 encourages the adoption of quantum-resistant cryptographic solutions. Lattice-based cryptography[6] and multivariate cryptography are examples of post-quantum cryptographic schemes that can withstand attacks from both classical and quantum computers. Integrating these quantum-resistant algorithms into automotive systems aligns with ISO 21434's objective of ensuring long-term security.

D.Quantum Key Distribution (QKD) for Secure Communication:

ISO 21434 recognizes the significance of secure communication in automotive networks, including V2V and V2X systems. Quantum Key Distribution (QKD)[4] can enhance secure communication by leveraging quantum principles to establish unbreakable encryption keys. QKD protocols, such as the BB84 protocol, enable the exchange of cryptographic keys[7] while ensuring that any eavesdropping attempts are immediately detected. By integrating QKD into ISO 21434's guidelines for secure communication, automotive stakeholders can enhance the confidentiality and integrity of data transmission.

E. Quantum-Powered Threat Detection and Artificial Intelligence:

ISO 21434 emphasizes the importance of continuous monitoring and detection of cyber security threats.

Quantum computing can bolster these efforts by enabling advanced threat detection and analysis capabilities. Quantum algorithms, such as the Quantum Support Vector Machine (QSVM) or Quantum K-means algorithm [8], can process large datasets more efficiently, identifying patterns and anomalies that may indicate cyber threats. Integrating quantum-powered threat detection with artificial intelligence techniques can further enhance anomaly detection, making it easier to detect and mitigate emerging threats in real-time. The Quantum language models when updates on periodic basis, shall ensure that the most up to date libraries are loaded and thus enabling the vehicle to stay intelligent. The quantum language model shall be invoked so that even the NLP libraries are auto updated at specific interval of time. The model to be invoked will generally be

$|\psi(\theta)\rangle = U(\theta)|\psi_0\rangle$, where

ψ: Represents the parameters or angles associated with the source task or domain.

$\theta5$: Represents the parameters or angles associated with the quantum language model.

$\theta6$: Represents the parameters or angles associated with the quantum explanation circuit.

however, this article suggests that the invoke procedure shall be part of the Quantum Transfer Learning Embedding represented by

$|\psi(\theta, \psi)\rangle = U(\theta)U(\psi)|\psi_0\rangle$

so that all updated intelligence modules shall be transferred to the vehicle system.

Where, *ψ: Represents the quantum state encoding or representation of the environment state in reinforcement learning.*

a: Represents the action performed in the reinforcement learning policy.

z: Represents the latent variables or code used in the variational autoencoder.

z: Represents the latent variables or code used in the variational autoencoder.

θ: Represents the parameters or angles associated with the quantum variational autoencoder.

F. Quantum Machine Learning (QML) for Enhanced Cyber security:

Another promising application of quantum computing in automotive cyber security lies in the field of quantum machine learning (QML). ISO 21434 recognizes the importance of leveraging advanced technologies to enhance cyber security measures. QML combines the power of quantum computing and machine learning [10] to improve anomaly detection, predictive analysis, and decision-making processes, thereby strengthening the overall cyber security posture. Reinforcement learning can be triggered by

$\pi(\psi, a) = U(a)U(\psi)|\psi_0\rangle$ where ψ: Represents the quantum state encoding or representation of the environment state in reinforcement learning.

a: Represents the action performed in the reinforcement learning policy.The boot loader must contain the Quantum Approximate Optimization Algorithm (QAOA) as indicated below:

$|\psi(\gamma, \beta)\rangle = e^{(-i\beta B)}e^{(-i\gamma C)}|\psi_0\rangle$

Where, *α, β: Refers to the probability amplitudes or coefficients associated with the quantum state encoding. They determine the relative contributions of the basis states $|0\rangle$ and $|1\rangle$.*

γ: Represents the angles or parameters associated with the problem-specific cost Hamiltonian.

β: Represents the angles or parameters associated with the problem-independent mixing Hamiltonian.

➢ Anomaly Detection and Pattern Recognition:

Quantum machine learning algorithms, such as quantum support vector machines (QSVM) or quantum neural networks, can analyze vast amounts of data generated by automotive systems to detect anomalies and patterns that may indicate cyber threats [2]. By harnessing quantum computing's parallel processing capabilities, QML[11] algorithms can identify subtle deviations from normal behavior, enabling faster and more accurate detection of potential security breaches.

➢ Predictive Analysis and Risk Assessment:

Quantum computing's ability to handle complex computations can greatly enhance predictive analysis and risk assessment in automotive cyber security[1]. By analyzing historical data and considering various factors, QML algorithms can generate more accurate predictions regarding future cyber security threats and vulnerabilities. This capability enables proactive measures to be implemented, reducing the likelihood of successful cyber attacks and enhancing the overall resilience of automotive systems.

➢ Quantum-Based Intrusion Detection Systems:

Intrusion detection systems (IDS) play a critical role in automotive cyber security, monitoring network traffic for suspicious activities and potential intrusions. Quantum-inspired algorithms, such as quantum clustering or quantum anomaly detection, can enhance the capabilities of IDS[14] by improving the accuracy and efficiency of detecting malicious activities. These algorithms can analyze network data in real-time, swiftly identifying deviations from normal behavior and enabling timely response to potential cyber threats. No cloning theorem when updated with Ket 1[|1>] in the formula $U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$ (represented in Fig-b below)

will alert the quantum-based systems when duplicate entries of intrusions than the whitelisted endpoints attempt to update the configuration files. In the above equation Where, *ψ: Represents the quantum state encoding or representation of the environment state in reinforcement learning.*

a: Represents the action performed in the reinforcement learning policy.

z: Represents the latent variables or code used in the variational autoencoder.

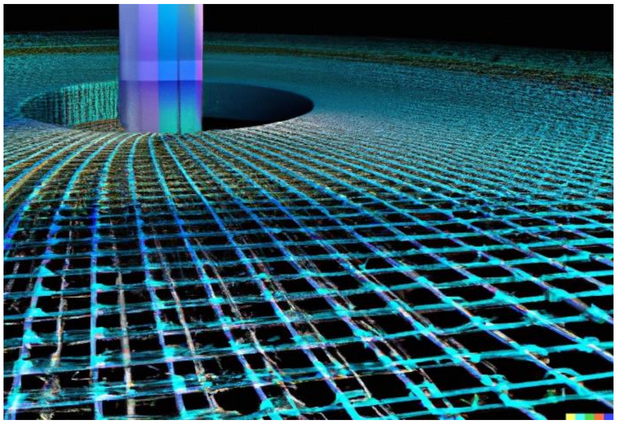

Fig-b: Representation of a Quantum system the moment phase estimation correction is applied – No cloning.

➢ Secure Data Sharing and Privacy Preservation:

Quantum machine learning techniques can also contribute to secure data sharing and privacy preservation in the automotive industry. Federated learning, a decentralized approach to machine learning, can leverage quantum computing to enable secure collaboration between multiple parties without the need to share sensitive data. Quantum secure multi-party computation (MPC) protocols can facilitate privacy-preserving analysis of combined datasets, ensuring data privacy and protection while enabling collective cyber security improvement across the industry.

V. SECURING V2V, V2X AND SDV: QUANTUM COMPUTING’S DEFENCE AGAINST THREATS

Connected and autonomous vehicles, including V2V, V2X, and Software Defined Vehicles (SDV) [9], are susceptible to various security threats. Quantum computing can play a crucial role in addressing these threats, providing robust solutions to enhance cyber security and protect these systems from attacks such as spoofing, injection attacks, replay attacks, denial-of-service (DoS), and Man-in-the-Middle[13] (MitM) attacks.

A. Spoofing Attacks:

Spoofing attacks involve deceiving a vehicle's communication system by impersonating a legitimate entity. Quantum computing can contribute to secure authentication protocols, making it more difficult for attackers to impersonate trusted entities. Quantum-resistant [15]cryptographic techniques, such as lattice-based or multivariate cryptography, can be employed to ensure secure verification and prevent spoofing attempts.

B. Injection Attacks:

Injection attacks involve maliciously injecting false or unauthorized data into the communication network, compromising the integrity and reliability of the transmitted information. Quantum-resistant encryption algorithms can protect the integrity of data transmissions, preventing unauthorized modifications and ensuring that injected data is detected and rejected by the system.

C. Replay Attacks:

Replay attacks occur when an attacker intercepts and later replays legitimate messages, leading to unauthorized actions or disruptions in the system. Quantum key distribution (QKD) protocols can be employed to establish secure communication channels between vehicles, making it practically impossible for attackers to intercept and replay legitimate messages. QKD ensures that encryption keys are distributed securely and cannot be replicated or tampered[16] with, thereby thwarting replay attacks.

D. Denial-of-Service (DoS) Attacks:

DoS attacks aim to disrupt or disable vehicle communication systems, rendering them incapable of performing critical functions. Quantum computing's superior processing power can contribute to anomaly detection and real-time monitoring of network traffic.

Quantum machine learning algorithms can identify patterns associated with DoS attacks, enabling timely detection and mitigation of such threats to ensure uninterrupted vehicle communication.

E. Man-in-the-Middle (MitM) Attacks:

MitM attacks involve intercepting and altering communication between two parties without their knowledge. Quantum key distribution (QKD) protocols can establish secure communication channels immune to eavesdropping[17] and MitM attacks. By utilizing QKD, vehicles can securely exchange encryption keys, ensuring the confidentiality and integrity of communication in V2V, V2X, and SDV environments.

F. CAN (Controller Area Network) injection attack:

These are a significant concern for the security of connected and autonomous vehicles. These attacks involve maliciously injecting unauthorized or false data into the CAN bus, potentially compromising the integrity and functionality of the vehicle's systems. Quantum computing can play a crucial role in defending against CAN injection attacks by employing robust cryptographic techniques and secure communication protocols. Quantum-resistant encryption algorithms can ensure the integrity and authenticity of data transmitted over the CAN bus, preventing unauthorized modifications or injections. Furthermore, quantum-based anomaly detection[18] methods can identify anomalous data patterns and detect potential injection attacks, enabling timely response and mitigation. By harnessing the power of quantum computing, V2V, V2X, and SDV environments can strengthen their defenses against CAN injection attacks, enhancing overall cyber security and safeguarding the integrity of vehicle communications.

VI. CHALLENGES AND FUTURE CONSIDERATIONS

Adopting quantum computing within the context of ISO 21434 presents several challenges. The development of scalable quantum hardware, integration with existing automotive systems, and the establishment of standardized quantum cyber security protocols are among the key obstacles. Collaborative efforts between automotive manufacturers, researchers, and regulatory bodies are necessary to address these challenges and align quantum computing with the principles outlined in ISO 21434.

VII. CONCLUSION

In conclusion, the incorporation of quantum computing in automotive cyber security has the potential to revolutionize the security landscape of connected and autonomous vehicles (CAVs), encompassing Self-Driving Vehicles (SDVs) as well as Vehicle-to-Vehicle (V2V) and Vehicle-to-Everything (V2X) communication. By delving into the applications of quantum technologies like Quantum Key Distribution (QKD), Quantum Optimization, and Quantum Data Encoding, the article highlights the significance of customization techniques to address the specific security requirements of diverse automotive use cases.

The customization of quantum approaches as disused in the articles allows for the adaptation and fine-tuning of these technologies to meet the unique challenges and demands posed by the CAV ecosystem. By tailoring quantum solutions to individual use cases, such as SDVs, V2V, and V2X communication, a more effective and robust security framework can be established.

Quantum QKD provides a secure means of key exchange, ensuring the confidentiality and privacy of sensitive information shared among vehicles. Quantum Optimization techniques enable the efficient allocation of resources and decision-making processes, enhancing the overall cyber security posture of CAVs. Quantum Data Encoding techniques offer robust mechanisms for detecting and preventing unauthorized data tampering or alteration, ensuring data integrity and authenticity.

The application of customization techniques to quantum computing methodologies ensures that automotive security measures align with the specific needs of CAVs. This tailored approach guarantees optimal performance and effectiveness in addressing the complex security challenges of the next-generation automotive ecosystem. By leveraging the computational power and unique properties of quantum computing, CAVs can achieve a higher level of security, mitigating the risks associated with cyber threats. The customization-driven approach not only enhances the protection of sensitive data but also fosters trust and confidence among manufacturers, service providers, and end-users. As the automotive industry continues to embrace the advancements in quantum computing, the realization of a safer and more secure future for CAVs becomes increasingly attainable.

REFFERENCES

[1] André Weimerskirch "An Overview of Automotive Cyber security: Challenges and Solution Approaches". TrustED 2015 – Trustworthy Embedded Devices October 16, 2015, pp. 14-32, 2015.

[2] Roman, Rodrigo et al. "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges". Future Generation Computer Systems, vol. 78, pp. 680-698, 2018.

[3] Sivanathan, Aruna et al. "A Survey of Cyber Security Issues and Solutions for Internet of Things (IoT)". Journal of Network and Computer Applications, vol. 84, pp. 1-20, 2017.

[4] Vlacheas, Panagiotis et al. "A Comprehensive Survey on Secure Device-to-Device Communication in Cellular-enabled Massive IoT". Journal of Network and Computer Applications, vol. 146, pp. 1-18, 2019.

[5] Robert S. Sutor, "A Brief Introduction to Quantum Computing", Springer International Publishing, Springer Optimization and Its Applications, vol. 124, pp. 1-19, 2016.

[6] Atzori, Luigi et al. "The Internet of Things: A Survey". Computer Networks, vol. 54, no. 15, pp. 2787-2805, 2010.

[7] Christian Baun, Dominic Breuker, and Marcel Pohl, "A Survey on Security and Privacy Issues in Internet-of-Things", Springer International Publishing, International Journal of Information Security and Privacy (IJISP), vol. 9, no. 2, pp. 125-134, 2015.

[8] Carole-Jean Wu and Keshab K. Parhi, "Exploration of Quantum Computing for Speech Recognition", Springer International Publishing, Springer Handbook of Speech Processing, 2020.

[9] Lin Dong, Chunqiang Hu, and Yaliang Zhang, "A Survey of IoT Cloud Security: Architecture, Applications, and Approaches", Springer International Publishing, Journal of Network and Systems Management, vol. 27, no. 4, pp. 1060-1081, 2019.

[10] Jens Eisert, "A Beginner's Guide to the Mathematics of Quantum Computing", Springer International Publishing, Springer Briefs in Mathematical Physics, 2018.

[11] Jens Eisert, "A Beginner's Guide to the Mathematics of Quantum Computing", Springer International Publishing, Springer Briefs in Mathematical Physics, 2018.

[12] Battista Biggio, Igino Corona, and Fabio Roli, "Security Evaluation of Support Vector Machines in Adversarial Environments", IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 4, pp. 787-799, 2014.

[13] Ram Shankar Siva Kumar and Jingchao Yan, "Understanding Artificial Intelligence Adversarial Examples and Their Security Implications", 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 903-908, 2018.

[14] John R. Crandall and others, "Anomaly Detection in Network Traffic Based on Statistical Inference and Machine Learning", ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 4, pp. 1-29, 2009.

[15] Anthony B. Smullen and others, "Cognitive Cyber security: Using Artificial Intelligence to Identify Suspect Network Traffic", Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pp. 1197-1204, 2018.

[18] Tugkan Tuglular and others, "A Survey of Artificial Intelligence for Cyber security", ACM Computing Surveys (CSUR), vol. 52, no. 3, pp. 1-38, 2019.

[19] https://www.iso.org/standard/70918.html

AUTHOR PROFILE

Dr. S. Sukumaran, working as Associate Professor, Department of Computer science (Aided) in Erode Arts and Science College, Erode, Tamilnadu, India. He is a member of Board of studies in various Autonomous colleges and universities. In his 35 years of teaching experience, he has supervised more than 55 M.Phil. research works, guided 21 Ph.D. research works and still continuing. He has presented, published around 80 research papers in National, International Conferences and Journals. His area of research interest includes Digital Image Processing, Networking and Data mining.

Johnbasco Vijay Anand is a Ph.D. scholar (part time), Department of Computer science in Erode Arts and Science College, Erode, Tamilnadu, India. He received his Master degree in Computer Application in 2001 from Bharathiar University. He is interested in advanced research in cyber security hardening using Quantum Computing and Artificial Intelligence.