Enhanced Data Security and Privacy in IoT devices using Blockchain Technology and Quantum Cryptography

Depavath Harinath [1] , Madhu Bandi [2] , Archana Patil [3] , M.V. Ramana Murthy[4] , AVS Raju[5]

[1]Dept of Computer Science, Ramnath Guljarilal Kedia College of Commerce, Hyderabad, Telangana, India.
mail id ;- harinath.depavath@gmail.com
[2]Independent researcher, &903, Elm, Ave Apts #257, Rancho Cuca Monga,CA 91730., U S A
mail id : madhu.bandi@gmail.com
[3]Dept of CSE, Rishi MS institute of Engineering and Technology for Women, Hyderabad ,Telangana, India ,
mail id ;- archanbpatil@gmail.com
[4]Dept. of Mathematics and Computer Science, Osmania University, Hyderabad, Telangana, India.
Mail id :- mv.rm50@gmail.com,
[4]Independent researcher ,Flat No 101,Aarna Residency, Nandanavanam colony, Bachupally, Hyderabad,India
Mail id :rajuvenkatasf@gmail.com

Abstract— Multimedia security encompasses the protection of audio, video, text, or images from unauthorized modification, access, or distribution. In today's interconnected world, the transmission of multimedia data over insecure channels on the internet exposes it to potential interception, tampering, or unauthorized dissemination by eavesdroppers. The ramifications of data breaches can be severe, resulting in substantial reputational and financial losses. Efficient key management is crucial for secure communication among smart devices in the Internet of Things (IoT). While existing security mechanisms can protect the network from various attacks, efficient key management schemes are necessary to ensure optimal network performance. With the proliferation of Internet of Things (IoT) devices, enormous volumes of data are collected from diverse sources. However, the inherent limitations in computational power and memory of IoT devices render them susceptible targets for malicious attacks. This study focuses on enhancing the security of multimedia data, encompassing audio, video, and images, obtained from IoT devices. Cutting-edge technologies such as blockchain and quantum cryptography are explored as promising avenues to bolster multimedia security and preserve privacy.

Keywords— Blockchain technology, Internet of Things (IoT), Security, Quantum Cryptography.

I. INTRODUCTION

Efficient key management is crucial for secure communication among smart devices in the Internet of Things (IoT). While existing security mechanisms can protect the network from various attacks, efficient key management schemes are necessary to ensure optimal network performance. Multimedia security encompasses the protection of audio, video, text, or images from unauthorized modification, access, or distribution. In today's interconnected world, the transmission of multimedia data over insecure channels on the internet exposes it to potential interception, tampering, or unauthorized dissemination by eavesdroppers. The ramifications of data breaches can be severe, resulting in substantial reputational and financial losses. The average cost of a data breach in India reached Rs 17.9 crore in 2023, according to the IBM Security report that classified it as an "all-time high" for the report and almost a 28 per cent increase since 2020. It is therefore imperative to implement robust security measures to protect multimedia data and mitigate the risks associated with unauthorized access and manipulation. Governments, organizations, and individuals must prioritize the implementation of robust security protocols and technologies to mitigate the risks and ensure the protection of valuable data from unauthorized access, manipulation, and exploitation. Various techniques have been employed in the past to provide authentication, integrity, and security to multimedia data. These techniques encompass digital signatures, watermarking, encryption, and more. Digital signatures serve as a means of verifying the authenticity and integrity of multimedia data, ensuring that it has not been tampered with during transmission. Watermarking techniques can be utilized to embed imperceptible markers within multimedia content, aiding in the identification of unauthorized use or distribution. Encryption, on the other hand, is a widely adopted method that transforms multimedia data into an unreadable form, thus protecting its confidentiality from unauthorized individuals. However, it is crucial to note that each technique possesses its own set of strengths and weaknesses.

Table 1: Challenges and solutions in cryptography

Challenges	Solutions
Security	Symmetric encryption, asymmetric encryption, cryptographic algorithms, cryptographic protocols
Authentication	Digital signatures, public key infrastructure (PKI), authentication protocols (e.g., OAuth, Kerberos)
Privacy	Private key encryption, secure key exchange, secure multiparty computation
Integrity	Hash functions, message authentication codes (MAC), digital certificates

Key Management	Key distribution centers (KDC), key derivation functions, key escrow
Non-repudiation	Digital signatures, timestamping, non-repudiation protocols

In addition to these approaches (see Table 1), the emergence of the Internet of Things (IoT) has introduced a new dimension of concern for multimedia security. As IoT devices become increasingly prevalent in our daily lives, they generate vast amounts of multimedia data. However, the limited computational power and memory of these devices often render them susceptible targets for attackers. Furthermore, the transmission of multimedia data from IoT devices through insecure channels further amplifies the security risks. To tackle these challenges, innovative solutions are being explored to enhance the security of multimedia data in the context of IoT. These solutions incorporate elements such as device authentication, secure communication protocols, and robust encryption algorithms specifically tailored for resource-constrained IoT devices. By implementing effective security measures at both the device and network levels, the integrity, confidentiality, and availability of multimedia data can be better protected within the IoT ecosystem. Sustained research and development in the realm of multimedia security, encompassing both traditional multimedia data and the distinct challenges presented by IoT devices, is imperative to proactively combat evolving threats. Achieving a harmonious equilibrium between usability, efficiency, and steadfast security is an ongoing pursuit that necessitates the exploration of innovative techniques and the continual enhancement of established ones. Through the mitigation of vulnerabilities and the utilization of emerging technologies, it becomes feasible to reinforce the security of multimedia data, encompassing conventional environments as well as the rapidly expanding IoT landscape.

Several standard encryption algorithms can be utilized to secure data, but their effectiveness relies on the encryption key remaining uncompromised and undisclosed to potential attackers. However, a significant challenge arises if an attacker manages to gain access to the hidden key and intercepts encrypted messages within the network. In such scenarios the attacker can decrypt the message, read its contents, re-encrypt it, and send it back to the recipient undetected. Neither the sender nor the receiver would be aware that their data was accessed or distributed by an unauthorized party. To address this critical issue, Quantum Key Distribution (QKD) emerges as a vital solution. QKD ensures that any attempt to steal the encryption key will be detectable, providing a high level of security. This technology holds exceptional significance in contexts where security is paramount, such as government, military, or financial data. In India, the Indian Institute of Technology (IIT) Kanpur has made significant advancements in the field of Quantum Key Distribution (QKD). They have successfully developed a QKD network by utilizing the existing optical fiber cable network, establishing a secure key exchange between two devices located 25 kilometers apart. To further enhance the security and privacy aspects, this paper also includes Blockchain and Zero Knowledge Proof technologies. Blockchain, in particular, has the potential to provide an advanced level of security to multimedia data by offering a secure, decentralized, and tamper-proof platform.

II. RELATED WORK

In the paper [1], the authors conducted a comprehensive survey on the security and privacy of multimedia data, providing valuable insights into the classification of data based on varying security requirements and different application domains. Moreover, they extensively analyzed and discussed several multimedia security schemes specifically designed for IoT devices. Their analysis encompassed traditional approaches like watermarking and cryptography, which have been widely employed in the field, as well as emerging technologies such as federated learning and blockchain. By examining both established and novel methods, the authors offered a holistic view of the evolving landscape of multimedia security, highlighting the diverse range of techniques available to address the unique challenges faced by IoT devices in safeguarding multimedia data.

The authors' work in [2] centers around addressing the security concerns associated with surveillance recordings. They recognize that traditional methods like steganography or watermarking often introduce significant latency and complexity when analyzing real-time data. To overcome these limitations, the authors propose a novel approach based on blockchain technology for protecting surveillance recordings. In their study, they develop a real-time system that utilizes blockchain and virtualization techniques to create a distributed ledger. By leveraging the immutability and transparency provided by blockchain, their model aims to enhance the security and integrity of surveillance recordings, ensuring that they are tamper-proof and resistant to unauthorized modifications. The authors in [3] have developed a privacy-preserving authentication system that relies on advanced cryptography techniques known as Zero Knowledge Proof (ZKP). In domains like healthcare, it is crucial to ensure the privacy of sensitive data, preventing unauthorized access while allowing for verification by authorized parties. ZKP proves to be an essential tool in safeguarding the privacy of various types of data. Similar research has been conducted by authors in [4,5], and [6], where they have utilized blockchain technology in conjunction with ZKP to protect multimedia data. The combination of blockchain and ZKP offers robust security and privacy measures, allowing for secure storage, transmission, and verification of sensitive information across various applications.

In [7], the authors have developed an innovative simulation model that utilizes quantum key distribution to enhance the security of cloud data. They employed Non-Abelian Encryption (NAE) as the encryption technique, and quantum keys were utilized for data decryption or access in the cloud. The distribution of keys was achieved through a quantum channel using fiber optic cables. The authors addressed various challenges related to data privacy, reliability, data confidentiality, and authorization in their model.

Another solution proposed in [8] involves the use of Advanced Encryption Standard (AES) combined with quantum key cryptography to enhance cloud security. The results demonstrated that the complex keys generated by quantum keys are highly unpredictable, making it extremely

difficult to compromise the security of data stored in the cloud. In a similar vein, in [9], the authors employed quantum cryptography to secure the cloud environment and provided a faster computation of keys. By leveraging the principles of quantum mechanics, they were able to enhance the efficiency and effectiveness of key generation for cloud security purposes.

III. SECURITY ATTACKS

A. The following are the different types of attacks are-

i. *Eavesdropping:* The use of QKD for key generation and satellite communication for qubit transmission enhances the security of the system against eavesdropping attacks. The quantum properties of the qubits and the secure satellite channel protect the confidentiality and integrity of the encryption keys and data during transmission.

ii. *Man-in-the-Middle (MitM) Attacks:* The framework employs various security measures to prevent MitM attacks. The QKD process ensures secure key exchange, while zero-knowledge proofs and lightweight ring signatures establish the authenticity and integrity of the communication between the cloud and IoT devices. These measures reduce the risk of unauthorized interception, tampering, or impersonation.

iii. *Cryptographic Attacks*: The ASCON cipher used for data encryption is a well-vetted and secure algorithm that provides confidentiality and integrity. Its resistance against known cryptographic attacks ensures the protection of data during transmission and storage. Proper key management and secure implementation practices mitigate potential cryptographic vulnerabilities.

iv. *Data Tampering: The* blockchain technology used in the framework provides tamper-resistance for stored data. The hash values of the data are recorded on the blockchain, making it difficult for attackers to modify the data without detection. The decentralized and distributed nature of the blockchain adds an additional layer of security, as multiple nodes validate and verify the integrity of the data.

v. *Sybil Attacks*: The use of blockchain technology helps mitigate Sybil attacks by providing a decentralized and consensusdriven system. Multiple nodes in the network validate transactions and maintain the integrity of the blockchain, making it difficult for an attacker to create multiple fake identities to manipulate the data.

vi. *Physical Attacks*: Physical attacks on the IoT devices, satellite infrastructure, or quantum key distribution components can compromise the security of the system. Implementing robust physical security measures, such as tamper-resistant hardware, secure facilities, and strong access controls, is crucial to prevent physical attacks and maintain the overall security of the system.

It is important to note that while the proposed framework offers significant security measures, regular security audits, updates, and patches are necessary to address emerging vulnerabilities and maintain the system's security over time. Secure development practices and adherence to industry standards further enhance the resilience of the framework against potential attacks.

B. The following are the Challenges in quantum key distribution implementation –

Implementing Quantum Key Distribution (QKD) introduces several cybersecurity and associated challenges that need to be addressed for a secure and effective deployment. Here are some of the key challenges:

1. **Quantum Channel Security:**
   - *Channel Vulnerabilities*: QKD relies on the transmission of quantum bits (qubits) over a physical channel. Ensuring the security of this channel against eavesdropping and interference is critical.
   - *Physical Attacks:* Quantum channels, such as optical fibers, are susceptible to physical attacks. Adversaries could tap into or manipulate the channel to intercept or modify qubits.
   - Quantum Trojan Horses: Attackers might try to introduce malicious components (quantum Trojan horses) into the communication setup, compromising the security of the quantum channel.

2. Device Security and Reliability:
   - Side-Channel Attacks: Quantum devices used in QKD implementations can leak information through side channels, which attackers might exploit to gather secret keys.
   - Device Calibration and Misalignment: Accurate device calibration and alignment are crucial for maintaining qubit integrity. Errors in these areas can lead to key leakage or loss.

3. **Photon Detection and Noise**:
   - *Photon Detection Efficiency:* Accurate and efficient photon detection is necessary for reliable QKD. Lower photon detection efficiency can lead to information leakage.
   - *Noise and Loss:* Noise and loss in the quantum channel affect qubit transmission, reducing the signal-to-noise ratio and potentially enabling attackers to intercept or manipulate qubits.

Addressing these challenges requires a multidisciplinary approach involving quantum physics, cryptography, network security, and engineering. As quantum technologies advance, ongoing research and collaboration are essential to ensure the security and reliability of QKD implementations.

IV. SYSTEM FRAMEWORK

i. **IoT Devices**: These are the physical devices embedded with sensors, actuators, and communication capabilities to interact with the physical world. They collect data from the environment and send it to the cloud for processing and storage. Examples of IoT devices could include temperature sensors, motion detectors, smart appliances, and industrial machines

ii. **Cloud Infrastructure**: The cloud infrastructure provides the computational and storage resources required to process and store the data generated by

the IoT devices. It consists of servers, databases, and networking infrastructure hosted in a data center or a cloud service provider. The cloud infrastructure handles the processing, storage, and analysis of the data.

iii. **Quantum Key Distribution (QKD)**: Quantum key distribution is a cryptographic protocol that allows two parties to securely exchange encryption keys using the principles of quantum mechanics. In this framework, QKD is used to generate a secure key for encrypting the data transmitted from the IoT devices to the cloud. QKD ensures the confidentiality and integrity of the encryption keys.

iv. **Satellite Communication**: A satellite is used to deliver the quantum bits, known as qubits, required for QKD. The satellite acts as a relay between the IoT devices and the cloud infrastructure, enabling secure transmission of the qubits over long distances. The satellite communication system ensures the integrity and authenticity of the qubits during transmission.

v. **Blockchain**: The blockchain is a decentralized and distributed ledger that records and stores transactional data in a secure and tamper-resistant manner. In this framework, the hash of the data generated by the IoT devices is stored on the blockchain. The blockchain provides immutability and transparency, ensuring that the integrity of the data cannot be compromised.

V. CRYPTOGRAPHIC ALGORITHMS

The following are the cryptographic elements that are employed to enhance the security of this model. By implementing these elements, we aim to bolster the overall protection and ensure the integrity of the system.

A. Digital ring signature

We employ lightweight Ring signature technology [10], which enables a signer to anonymously sign data. In a ring signature the signature is mixed with signatures from other members of a group (referred to as a ring), making it impossible for anyone, except the actual signer, to determine the identity of the signer. The concept of Ring Signature was initially proposed by Rivest in 2001 [11]. We can successfully achieve both the objectives of ensuring Signers' Anonymity and guaranteeing Signature Correctness.

- Signature Correctness: Our approach ensures that a signature is considered valid if it meets the required criteria, and any signature that fails to meet the criteria is always rejected.
- Signers Anonymity: With our method, a signature is generated by a member selected from a set of public key holders. As a result, the identity of the actual signer remains concealed within the network, preventing anyone from determining the true signer based solely on the signature.

The digital ring signature algorithm allows an IoT device to securely transfer data to a cloud server while preserving the anonymity of the device. The algorithm utilizes a ring signature scheme, where a group of users collectively sign the data, and the cloud server can verify the signature without knowing the specific signer.

Algorithm 1 :Digital Ring Signature Algorithm

Input: Data D, Set of public keys $PK = \{PK_1, PK_2, ..., PK_n\}$, Signer's secret key SK_i
Output: Digital ring signature σ
procedure SIGN(D, PK, SK_i)
    Randomly select a subset of public keys $PK' \subset PK$ such that $PK_i \in PK'$
    Compute the ring signature σ using D, PK', and SK_i
    return σ
end procedure
procedure VERIFY(D, PK, σ)
    for all $PK_i \in PK$ **do**
        if Verification of σ using D, PK_i succeeds **then**
            return *valid*
        end if
    end for
    return *invalid*
end procedure

B. *Zero-knowledge proofs*

Zero-Knowledge Proofs (ZKPs) are cryptographic protocols that allow one party (the prover) to prove to another party (the verifier) that a certain statement is true, without revealing any specific information about the statement itself. In other words, a ZKP allows the prover to demonstrate knowledge of something without revealing what that knowledge is. This concept ensures privacy and security in scenarios where proving knowledge is necessary without disclosing sensitive information.

Key concepts:

1. **Completeness:** If the statement is true, an honest verifier will be convinced by an honest prover.

2. **Soundness:** If the statement is false, no dishonest prover can convince an honest verifier otherwise.

3. **Zero-Knowledge:** The verifier learns nothing about the underlying information except the fact that the statement is true.

Use Cases:

1. **Authentication:** A user can prove knowledge of a password without revealing the actual password.

2. **Digital Signatures:** A signer can prove the validity of a signature without disclosing the private key.

3.**Privacy-Preserving Transactions:** Proving possession of certain attributes (like being over 18) without revealing other personal information.

4. **Anonymous Credentials:** Verifying attributes like age or membership without disclosing identity.

Zero-Knowledge Proofs provide a powerful tool for privacy-preserving authentication and verification. They have applications in blockchain, digital identity, secure voting systems, and more, ensuring information can be verified without exposing sensitive data.

Algorithm 2: Zero-Knowledge Proof for Data Verification

Input: IoT data d, Proof parameters P
Output: Verification result **True** or **False**
Initialize: $s \leftarrow 0$
Choose a random secret: $r \leftarrow$ Random number
Compute the commitment: $c \leftarrow \text{ComputeCommitment}(d, r, P)$
Send the commitment: c to the cloud
Receive a challenge: x from the cloud
Compute the response: $s \leftarrow r + x \cdot d$
Send the response: s to the cloud
Receive the cloud's verification result: V from the cloud
if V is **True then**
    Output: True
else
    Output: False
end if

C .Lightweight encryption algorithm

To encrypt the data, we propose to use lightweight cipher ASCON [12]. ASCON is a symmetric key encryption algorithm designed for lightweight and resource constrained devices, making it suitable for applications in the Internet of Things (IoT) and multimedia systems. ASCON emerged as a result of the CAESAR competition, which aimed to find new authenticated encryption schemes suitable for lightweight devices.

The encryption process encompasses four distinct phases:

1. Initialization: The state is initialized with the key K and nonce N.

2. Associated Data Processing: The state is updated with the associated data blocks A_i.

3. Plaintext Processing: Plaintext blocks P_i are injected into the state, producing corresponding ciphertext blocks C_i.

4. Finalization: The key K is injected once again, and the resulting tag T is extracted for authentication purposes.

The use of ASCON in multimedia and IoT systems brings several benefits. Firstly, its lightweight nature ensures that it can be efficiently implemented on resource-constrained devices without consuming excessive power or memory. This makes it suitable for low-power IoT devices, where energy efficiency is crucial. Secondly, ASCON provides authenticated encryption, which guarantees the integrity and authenticity of the transmitted data. This is particularly important in multimedia applications, where tampering with or modifying the content can result in significant consequences. Furthermore, ASCON offers a high degree of flexibility. It supports various key sizes and can accommodate different security requirements based on the specific use case. This adaptability makes it well-suited for multimedia systems that handle diverse types of data, such as images, audio, and video.

VI. ROBUSTNESS AND RESILIENCE IN A QUANTUM KEY DISTRIBUTION (QKD) SYSTEM

i. Robustness in QKD:

A robust system [13] can handle both anticipated and unanticipated situations without failing or compromising its functionality. In the context of security, a robust system can withstand various attacks, vulnerabilities, and attempts to breach its defenses.

- Robustness in a QKD system refers to its ability to operate reliably under various conditions, including potential attacks, noise, and other uncertainties inherent to quantum systems.
- Implement error correction and fault tolerance mechanisms to counteract errors and imperfections introduced during the transmission of quantum states. This ensures that even in the presence of noise or disturbances, the system can still generate accurate and secure key material.
- Use advanced quantum protocols that are resilient against common attacks, such as the BB84 protocol with decoy states to mitigate photon number splitting attacks.

ii. Resilience in QKD:

Resilience [14] refers to the ability of a system or organization to absorb shocks, recover from disruptions, and continue operating effectively. A resilient system can bounce back from adverse events, such as cyber attacks, natural disasters, or hardware failures, while minimizing the impact on its functionality and integrity.

- Resilience in a QKD system is about its ability to recover and continue functioning after facing disruptions, attacks, or unexpected events.
- Develop comprehensive incident response plans that outline steps to take in case of security breaches or system failures. These plans should include procedures for detecting and containing attacks, recovering from security incidents, and restoring normal operations.
- Implement redundancy and backup measures to ensure that communication can continue even if certain components fail or are compromised. This might involve having backup QKD devices, communication paths, and authentication mechanisms.

iii. Integration of robustness and resilience:

- Integrate robustness and resilience considerations from the design phase of the QKD system. This includes selecting reliable hardware components, designing fault-tolerant protocols, and establishing secure communication channels.
- Regularly update and upgrade the QKD system's software and hardware to address emerging vulnerabilities and to stay ahead of potential threats.
- Implement continuous monitoring to detect unusual activities or patterns that might indicate an attack. Rapid detection allows for quick response and containment.

Testing and verification:

- Rigorously test the QKD system under various conditions, including simulated attacks and unexpected inputs, to ensure its robustness.
- Conduct penetration testing and vulnerability assessments to identify potential weaknesses and vulnerabilities in the system. Address the findings to improve the system's overall resilience.

iv. Education and training:

- Train personnel who are responsible for operating and maintaining the QKD system in security best practices, incident response procedures, and techniques for detecting and mitigating attacks.
- Foster a security-aware culture within the organization to encourage everyone to contribute to the robustness and resilience of the QKD system.

VII. CONCLUSION

The proposed framework, which combines IoT devices, blockchain, and cloud technology, along with quantum key distribution, satellite communication, zero-knowledge proofs, lightweight ring signatures, and the ASCON cipher, offers a robust and secure solution for data collection, transmission, and storage in IoT systems. It addresses key security concerns such as eavesdropping, man-in-the-middle attacks, cryptographic vulnerabilities, data tampering, Sybil attacks, and physical attacks. The integration of quantum key distribution and satellite communication ensures secure key generation and transmission, while zero-knowledge proofs and lightweight ring signatures establish communication authenticity and integrity and blockchain technology enhances data tamper-resistance. Therefore, regular security audits, updates, and adherence to secure implementation practices are necessary to maintain the framework's security over time.

REFERENCES

[1] W. Yang, S. Wang, J. Hu, N.M. Karie, Multimedia security and privacy protection in the internet of things: research developments and challenges, Int. J. Multim. Intell. Secur. 4 (1) (2022) 20–46, http://dx.doi.org/10.1504/IJMIS.2022.121282.

[2] Z. Ma, L. Zhu, F.R. Yu, J. James, Protection of surveillance recordings via blockchain-assisted multimedia security, Int. J. Sens. Netw. 37 (2) (2021) 69–80, http://dx.doi.org/10.1504/IJSNET.2021.118486.

[3] A.D. Dwivedi, R. Singh, U. Ghosh, R.R. Mukkamala, A. Tolba, O. Said, Privacy preserving authentication system based on non-interactive zero knowledge proof suitable for internet of things, J. Ambient Intell. Humaniz. Comput. 13 (10) (2022) 4639–4649, http://dx.doi.org/10.1007/s12652-021-03459-4.

[4] R. Singh, A.D. Dwivedi, R.R. Mukkamala, W.S. Alnumay, Privacy-preserving ledger for blockchain and internet of things-enabled cyber-physical systems, Comput. Electr. Eng. 103 (2022) 108290, http://dx.doi.org/10.1016/j.compeleceng.2022.108290.

[5] R. Singh, A.D. Dwivedi, G. Srivastava, P. Chatterjee, J.C.-W. Lin, A privacy preserving internet of things smart healthcare financial system, IEEE Internet Things J. (2022) 1, http://dx.doi.org/10.1109/JIOT.2022.3233783.

[6] S. Dhar, A. Khare, R. Singh, Advanced security model for multimedia data sharing in internet of things, Trans. Emerg. Telecommun. Technol. (2022) http://dx.doi.org/10.1002/ett.4621, Epub ahead of print. Published online: 07 August 2022..

[7] S. Sasikumar, K. Sundar, C. Jayakumar, M.S. Obaidat, T. Stephan, K.-F. Hsiao, Modeling and simulation of a novel secure quantum key distribution (SQKD) for ensuring data security in cloud environment, Simul. Model. Pract. Theory 121 (2022) 102651, http://dx.doi.org/10.1016/j.simpat.2022.102651, URL https://www.sciencedirect.com/science/article/pii/S1569190X22001216.

[8] G. Sharma, S. Kalra, A novel scheme for data security in cloud computing using quantum cryptography, in: Proceedings of the International Conference on Advances in Information Communication Technology & Computing, AICTC '16, Association for Computing Machinery, New York, NY, USA, 2016, http://dx.doi.org/10.1145/2979779.2979816.

[9] S. Fatima, S. Ahmad, Quantum key distribution approach for secure authentication of cloud servers, Int. J. Cloud Appl. Comput. 11 (3) (2021) 19–32, http://dx.doi.org/10.4018/IJCAC.2021070102.

[10] L. Malina, J. Hajny, P. Dzurenda, S. Ricci, Lightweight ring signatures for decentralized privacy-preserving transactions, in: P. Samarati, M.S. Obaidat (Eds.), Proceedings of the 15th International Joint Conference on E-Business and Telecommunications, ICETE 2018 - Vol. 2: SECRYPT, Porto, Portugal, July 26-28, 2018, SciTePress, 2018, pp. 692–697, http://dx.doi.org/10.5220/0006890506920697.

[11] R.L. Rivest, A. Shamir, Y. Tauman, How to leak a secret, in: C. Boyd (Ed.), Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings, in: Lecture Notes in Computer Science, vol. 2248, Springer, 2001, pp. 552–565, http://dx.doi.org/10.1007/3-540-45682-1_32.

[12] C. Dobraunig, M. Eichlseder, F. Mendel, M. Schläffer, Ascon v1.2: Lightweight authenticated encryption and hashing, J. Cryptol. 34 (3) (2021) 33, http://dx.doi.org/10.1007/s00145-021-09398-9.

[13] W.J. Zhang, Y. Lin, On the principle of design of resilient systems – application to enterprise information systems, Enterp. Inf. Syst. 4 (2) (2010) 99–110, http://dx.doi.org/10.1080/17517571003763380, arXiv:10.1080/17517571003763380.

[14] W. Lin, M. Xu, J. He, W. Zhang, Privacy, security and resilience in mobile healthcare applications, Enterp. Inf. Syst. 17 (3) (2023) 1939896, http://dx.doi.org/10.1080/17517575.2021.1939896, arXiv:10.1080/17517575.2021.1939896.

[15] Depavath Harinath, et.al, "Lattice Cryptography- A NTRU Cryptosystem Providing a Quantum Attack Resistant Security System for Cloud Computing", in GIS Science Journal, Volume 11, Issue 4, 2024, ISSN No: 1869-9391 Page No. 159 – 168. DOI:20.18001.GSJ.2024.V11I5.24.41185420

[16] Depavath Harinath, et.al, "Enhancing Security and Malware Detection in IoT Devices using Random Forest Algorithm", Technische Sicherheit (Technical Security) Journal, Volume 24 Issue 3, 2024, ISSN:1434-9728 and Page No. 169 – 176, DOI:22.8342.TSJ.2024.V24.3.01304

[17] Depavath Harinath, et.al, "Blowfish Algorithm – An Efficient Data Encryption Technique to Ensure Data Confidentiality", in Elsevier publications- Journal of Engineering and Technology Management, Volume 72 issue April-June 2024, ISSN-1879-1719

[18] Depavath Harinath,et.al,"A Review on Security Issues and Attacks in Distributed Systems," Journal of Advances in Information Technology(JAIT), California, USA, Vol. 8, No. 1, pp. 1-9, February, 2017. doi: 10.12720/jait.8.1.1-9

Author Profile

Depavath Harinath, Assistant Professor, received Master of Computer Applications degree from Sreenidhi Institute of Science and Technology, an autonomous institution approved by UGC, Accredited by NAAC with 'A+' grade and accredited by NBA, AICTE, New Delhi – permanently affiliated to JNTU, Hyderabad, Telangana, India. Having more than twelve years of experience in teaching, already published 24 manuscripts in different international journals with good citation and have one United Kingdom based international patent on AI Drone for Quantum UAV Farming. Now working as Assistant Professor, Dept. of Computer Science, Ramnath Guljarilal Kedia College of Commerce, Hyderabad, Telangana, India. Research field

includes Computer Networks, Network Security, Artificial Intelligence and Machine Learning.

Prof. M. V. Ramana Murthy, Professor in department of mathematics and computer science, Osmania University, since 1985. Obtained PhD degree from Osmania University in 1985 and visited many a countries across the globe in various capacities and participated in many academic programs. Research fields includes computational plasma, Artificial Neural Networks, and Network securities.

Dr. Archana Patil, B.E, MTech(CSE) & Ph.D.(CSE)working as assistant professor in Rishi MS Institute of Engineering & Technology for Women, Hyderabad. She has 12+ years of teaching experience. She has completed Ph.D. from VTU Belagavi, Karnataka. Area of research is Green Cloud Computing. She has published many papers in reputed International and National Journals and Conferences with good citation. She already published many books and more than 10 Patents on different area of Computer Science and engineering. Her area of interest includes Cloud Computing, Data structure, Computer Graphics, IOT, Mobile Adhoc Network, Cyber Security,andmachinelearning.