World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

A review of the cryptographic approaches to data security: The impact of quantum computing, evolving challenges and future solutions

Adeyemi Afolayan Adesola [1, *], Awele Mary-rose Ilusanmi [2] and Peter Chimee Oyirinnaya [3]

[1] Department of Computer Science; Stephen F. Austin State University; Nacogdoches; Texas; USA.
[2] Department of Multidisciplinary Studies, College and Liberal Arts; Stephen F. Austin State University; Nacogdoches; Texas, USA.
[3] Center for financial studies, Charter institute of Bankers of Nigeria, Victoria Island, Lagos, Nigeria.

World Journal of Advanced Research and Reviews, 2025, 25(02), 1916-1924

Publication history: Received on 29 December 2024; revised on 10 February 2025; accepted on 13 February 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.2.0434

Abstract

Cryptography plays a fundamental role in defending digital data against cyberthreats and emerging quantum computer capabilities. This review discusses core cryptographic techniques such as symmetric encryption, asymmetric encryption and cryptographic hashing, as well as advanced techniques like lattice-based cryptography , code-based cryptography, multi-variate polynomial cryptography and hash-based cryptography that are quantum resistant. The review share insight into the applications of cryptographic techniques in securing communications, encrypting databases, blockchain technology, and health care ensuring that the confidentiality and integrity of data is maintained while also addressing the current need for continuing resistance to future quantum attacks. Additionally, this review discusses critical problems in implementation, usability, and the threat that quantum computing poses to existing cryptographic techniques and offers insights into quantum resistant algorithms.

Keywords: Cryptography; Data privacy; Quantum attacks; Data protection; Data security; lattice-based cryptography; code-based cryptography; multi-variate polynomial cryptography

1. Introduction

In today's interconnected digital world, information is shared across borders and platforms at high speeds, it becomes paramount to protect data. Given the fact that potentially billions of people store and actively exchange massive amounts of various personal and often significantly sensitive data, the threats of data leakage, unauthorized users' access, and cyber-attacks remain not only constantly rising, but continually evolving as well. Cryptography is the branch of science that aims to provide confidentiality and integrity of information using various mathematical methods. Cryptography implies the conversion of readable data into unreadable forms and only those with the proper authorization can read or make changes to such information [1].

The primary, and most effective, techniques for encryption include symmetric encryption, asymmetric encryption and hash function all of which help to secure data in transit as well as at rest. The security of data is achieved through ciphers. Ciphers is a set of algorithms used for encrypting data. The Cipher with key is known as symmetric encryption and it is in use in most systems, such as databased encryption and secure file systems where the same secret key is used for encrypting and decrypting data. Also, public and private key encryption allows for secure transmission of messages and forms a foundation for such protocols, as HTTPS. Hash functions also introduce another level of security in that they provide irreversible transformation which is a main element required when checking for data integrity. This review

[*] Corresponding author: Adeyemi Afolayan Adesola

discusses the evolution, applications and difficulties with cryptographic techniques for data privacy, and the ever-changing digital world for the continued use of such techniques [2].

2. Overview of Cryptographic Techniques

2.1. Symmetric Encryption

Symmetric encryption, also known as private key encryption, encrypt and decrypt information using the same secret key. This approach is efficient and fast, and it's appropriate for data security, e.g. database or file storing systems. The Advanced Encryption Standard (AES), Data Encryption Standard (DES) as well as the Triple data encryption standard (3DES), are examples of symmetric encryption algorithms. These algorithms guarantee that a message intercepted, in transit, cannot be understood unless the correct key is also obtained [3]. The major weakness of symmetric encryption is that of the key distribution difficulty since the two parties required to decrypt the message must share the same key. It can sometime be complex when sharing this key via over insecure communication channels. To overcome this problem, different cryptographic techniques are employed simultaneously such as symmetric encryption and asymmetric encryption for key exchange. The speed and simplicity of symmetric encryption makes it an indispensable part of data protection despite the challenges mentioned above [4].

2.2. Asymmetric Encryption

Asymmetric encryption, also known as public-key cryptography uses two related keys. It means a public key for encryption and a private key for decryption. Since the public key can be disseminated without loss of security in this method, the key distribution problem that is encountered in symmetric encryption is eliminated. Confidentiality guarantees only encrypted information will be seen by the receiver who holds the private key. Asymmetric encryption is used by protocols such as Secure Sockets Layer (SSL), and its improved version the Transport Layer Security (TLS), in order to create secure communication channels [5]. Asymmetric encryption is extremely secure, however slow, and requires much server resources. As a result of this asymmetric encryption is usually used for tasks such as secure key exchange rather than encrypting large volumes of data. Asymmetric and symmetric methods can be combined to build systems that select the best features of both approaches, as performed by hybrid encryption used in secure web browsing and email encryption [6].

Data integrity cannot happen without cryptographic hash functions. The hash functions takes file or message as an input and provide a fixed size output called hash value or digest. Because of their design they are ideal for detecting tampering. A change to the input, even a single character, results in a completely different hash value. Algorithms such as SHA256 and MD5 are popular, and are used in password storage, digital signatures, and the technology behind the blockchain [7]. Hash functions are one way process, meaning that original input cannot be retrieved from its hash value. Unlike encryption where data encrypted can be decrypted. A demerit of hash functions is that hashing functions such as MD5 are prone to collision attacks, where two different inputs result in the same hash. Therefore, researchers keep developing and improving hashing algorithms to prevent the latest emerging threats [8].

3. Applications of Cryptographic Techniques

Modern digital security is built on cryptographic techniques. Cryptographic techniques are the backbone of a considerable number of applications that secure sensitive data, ensure secure communications, and maintain system integrity. The different applications of cryptological methods are discussed in this section to show how they can be used to tackle the problems that our ever more connected and data dependent world is struggling against.

Secure communications rely on cryptography. Cryptography allows users to securely exchange information by exchanging information. Cryptographic techniques are used by protocols like HTTPS, TLS and SSL to protect data that’s passed over the internet and thus sensitive data such as login credentials, credit card details and personal messages. Cryptography is the basis behind Virtual Private Networks (VPNs) which provide encrypted communication tunnels that are used to create a safe remote employee access to corporate resources. Cryptography offers protection to newer technologies such as secure email encryption platforms, like ProtonMail or encrypted file sharing services [9-10].

A database is an organized collection of data stored electronically to facilitate efficient retrieval, management and update. An encrypted database is a database that contains sensitive information that’s protected on a server by converting that data to unreadable formats. In sectors like healthcare, finance and ecommerce, large volumes of highly sensitive data are stored in databases and so it is essential. Encryption is implemented to minimize risk of a breach or access to confidential data by a threat actors [11].

Additionally, database encryption is employed in cloud computing environments where data is stored on servers that are located in remote places. To maintain the confidentiality of the data stored on these cloud servers, homomorphic encryption is widely being adopted. Homomorphic encryption is an encryption that supports computational operation over encrypted data without decryption [12].

End to end encryption or E2EE means that data is encrypted from the time it leaves the sender's device up to the time it gets to the recipient device. The E2EE model ensures that no third parties can decrypt the content of the messages being transmitted between the sender and the receiver. This model is adopted by WhatsApp, and email services to ensure that threat actors cannot intercept and read the information being transmitted between the sender and the receiver. E2EE goes beyond just messaging and is increasingly being used for video conferencing software like Zoom and Microsoft Teams, as concerns over data privacy in the remote working age have increased. Google Drive and Dropbox are also catching up and adding in these E2EE features to files that are being shared. E2EE can protect the data produced by smart home devices and wearables from being intercepted or used wrongly [13]

Data stored and processed in a cloud platform is secured by cryptography techniques. Encryption is used by cloud providers to protect data at rest, in transit and sometimes in computation. If client-side encryption has been implemented, the users encrypt the data before uploading to the cloud which even the provider cannot have access to. In addition, encryption provides more trust in multi or hybrid cloud environments where the data goes between private and public clouds. Secure token and digital signature are just two of the cryptographic access controls that keep cloud storage hidden from unauthenticated and unauthorized users. In an era when cloud usage continues to grow rapidly, these techniques are critical for protecting personal information, trade secrets and intellectual property [14].

More and more electronic voting systems are employing cryptographic techniques to guarantee secure and trusted elections. Also, they guarantee confidentiality by encrypting votes so that no one can link a vote to a specific voter. Digital signatures and secure multi-party computation assists the determination of integrity of the votes and the election process to eliminate fraud or tampering. This technology makes electronic voting transparent as well as private, which is key to building trust in such systems [15].

New innovations such as blockchain voting ensure the votes cast are backed up with an irreversible record. Through Blockchain, any vote that is registered electronically cannot be changed, deleted or manipulated as they contain links to previous votes in the Blockchain. To ensure that anonymity of the ballot is maintained, cryptographic technologies also enable voters to confirm that their votes were counted. The goal of these innovations is to provide secure and scalable electronic voting systems for large elections and to build public trust in the democratic process [16].

The digital identity systems rely on cryptographic techniques to assure the security of personal identifiable information (PII). The common way to verify and authenticate digital identities is to use public key infrastructure (PKI), so that identity theft and illegitimate access doesn't occur. Digital certificates and cryptographic tokens securely show users' identity without revealing personal information, enabling access to these types of services like banking, healthcare and on government platforms. There is a new development in this area, the use of zero knowledge proofs, which allow users to verify certain attributes without exposing the rest of the information. Decentralized identity systems, which place users in control of their data rather than relying on central authorities, are also being mixed with cryptographic solutions for digital identity, making them more private and resistant to breaches [17]

With so many IoT devices, smart home systems, to industrial sensors, it introduces a whole new world in terms of cybersecurity challenges. Cryptography is a critical building block to secure IoT Ecosystems by encryption of communication between devices and authentication of identity. To address the limiting computing power possible on many IoT devices, lightweight encryption algorithms are being formulated to remain efficient while maintaining security. In addition to that, cryptographic techniques also prevent malicious actors from controlling the IoT devices or gaining access to sensitive data. With the number of IoT devices increasing cryptography will continue to play a fundamental role in maintaining the security of Internet of Things networks [18].

Cryptography plays an important role as an essential tool for digitally securing supply chain transactions thereby protecting data against fraud, data alteration and forgery. Due to this, blockchain technology applies cryptographic hash to generate unalterable record of each transaction that increases trust throughout the chain among all users. To minimize the risk of fraud that is common with paper-based proof like shipping manifests or invoices, they are replaced by digital signatures. Digital signatures provide authenticity and integrity check of transactions by ensuring that the corresponding public key or private key pair that was used to encrypt the data are used in decrypting the data [18].

Furthermore, through the use of encrypted communication, the suppliers, manufacturers and distributors are confident that communication and the business data shared cannot be tampered with. In order to achieve a safe and effective cyber supply chain free from cyber threats, cryptography cannot be eliminated as global supply networks become more complex [19].

Cryptography is greatly used in healthcare organizations in a bid to ensure that the patient's information is well protected. Encryption helps to protect the information in Electronic Health Records (EHRs), test results, medical data stored on the server or transferred from one healthcare professional to another. They also include cryptographic protocol for communications between medical devices and monitoring systems, data that is transmitted from a wearable or from an implanted device such as a pacemaker. [20]

In addition to defending individual patient information, Cryptography is used in clinical research to secure trial data and guarantee that only those having permission can access what is perceived as proprietary data. Since there is a growing trend in the provision of telemedicine and other remote health care services cryptographic solutions will come in handy in maintaining confidentiality and integrity in the services [21]. As quantum computing becomes more of a reality, hence the need for quantum resistance cryptographic systems becomes more than ever. This threat may impact core, innovative, and complex infrastructures and systems that rely on secure encryption. As a result, it is critical to understand how quantum-resistant cryptography can be used to defend essential systems, secure recent technologies, guard the blockchain, and form the standards for a safe future in a quantum age [22].

4. Future Applications of Quantum-Resistant Cryptography

Quantum-safe encryption is expected to be necessary for the security of applications, which require protection, including financial ones, health care networks, and the government. These systems primarily depend on encryption for protection of information and system functionality. When these quantum computers are fully implemented, current cryptographic standards such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) can be easily broken which poses a threat to infrastructures and applications. Post-quantum cryptography related algorithms as lattice-based or hash-based cryptography will keep essential systems secure in the age of hacking with quantum computers and protect the identity of sensitive information [23].

Another big concern associated with these infrastructures is the capability to secure data over a long-time span. Some industries, especially government and defense, need data to be well protected to become available for decades. Quantum-resistant cryptography gives a condition for future-proofing data from being decrypted if the authors start to use quantum computers in the future. Incorporation of quantum-resistant techniques in infrastructure calls for prioritization since quantum-related risk impacts critical infrastructure [24].

As the IoT devices continue to increase, billions of these devices continue to manage everyday applications and industrial processes, there is a dire need to enhance its resistance to quantum attacks. IoT devices are actually simple computing devices characterized by low computational and energy power which makes it even more complicated to protect. These constraints are solved with new lightweight quantum-resistance algorithms which offer secure protection from both classical and quantum attacks [25].

Like other technologies, artificial intelligence (AI) and autonomous systems are emerging technologies and have their unique security challenges. The AI models trained on future sensitive good data like medical or financial data have to be safe from future quantum threats. Self-driving cars and drones also function on encrypted communication and use algorithms for their functioning; hence these vehicles also require quantum-safe communication protocols for the future world [26].

Quantum-resistant cryptography will also be a key in blockchain technology as used in cryptocurrencies and decentralized finance. Cryptographic techniques are primarily used in the blockchain system with special emphasis placed on the public key cryptographic technique to enhance transaction security and other functions of the system. Currently, many systems utilize cryptographic methods to secure their information, and due to quantum computer capabilities, these computers might be able to corrupt these methods and enable attackers perform fake transactions or even corrupt the blockchain [27].

To safeguard blockchain systems against these threats it becomes necessary for the entire system to move towards quantum resistant cryptographic techniques. The integration of quantum-resistant algorithms to blockchain poses a significant challenge to computational complexity and scalability since executing existing blockchain requires significant computational resources [28].

5. Evolving Challenges in Cryptographic Techniques

Cryptography provides the required means to protect data and systems, but it has its challenges. This section dive into some of common challenges that have been observed to affect cryptographic methods as they are implemented

Ensuring proper implementation is one of the most important challenges in cryptography. Implementing cryptographic algorithms incorrectly can make even the most advanced algorithms fail. The failure of systems to utilize properly managed encryption keys or use weak random number generators can lead to vulnerabilities causing the system to be attacked [29]. Integrating cryptographic techniques into existing systems without significantly disrupting those systems is another problem. The challenges many organizations face with modern encryption tools is that many organizations simply cannot update legacy systems with modern encryption protocols without disruption of critical infrastructure. On top of that, there are specific problems with ensuring compatibility between disparate systems and software relying on cryptographic techniques, which leaves some areas of security potentially exposed. These implementation challenges call for adequate training, stringent testing and compliance with cryptographic measures [30].

Current cryptographic solutions are effective, but they often come with usability problems for end users. Managing encryption keys can be a complex process, and processes such as multi factor authentication can discourage adoption or result in user error. Also, when users choose weak passwords or fail to handle recovery keys securely, they might compromise the security of the cryptographic system. Ensuring that cryptographic tools are robust while being easy to use is a recurring challenge [32].

However, some cryptographic measures may provide delays in processes, especially in apps that are energy-demanding such as mobile devices or the IoT systems. This can make the users become frustrated and in turn avoid using such measures in enhancing their security. To address these challenges, new cryptographic systems must seek user friendly designs, automated key management and seamless integration of encryption into everyday applications without compromising security [33].

6. Threats from Quantum Computing

Traditional cryptographic techniques are under attack from quantum computing. With their great processing power, quantum computers could compromise the security of well-used encryption methods like RSA and ECC. This calls for need urgent quantum resistant cryptographic algorithms to keep secured sensitive information from possible quantum attacks. Despite the fact that the technology of quantum computers at the moment is still in progress, the threats that it carries are considered threatening enough to urge researchers to start focusing on post-quantum cryptography. New cryptographic algorithms such as lattice-based cryptography and Multivariate Polynomial Cryptography are meant to protect data and systems against quantum-based threats of attacks [34].

Key management is often considered one of the most important and at the same time most difficult problems in cryptography. As organizations grow, they struggle to scale their key management systems. Keys have to be generated, distributed, stored and destroyed securely, so specialized tools and procedures have to be used. Cloud based key management systems have come into being to simplify these assignments but incur other hazards, for instance trust of remote third-party service providers and meeting government regulations requirements. PKI, which is used in securing online communications require web scalability to accommodate a growing number of devices in a network without the effect of degrading its performance or introducing new web level vulnerabilities. Cryptographic systems that are not properly managed through key management practices have no better chance of working well than do the systems that are not based on cryptographic systems [35].

While these cryptographic techniques are available, they are frequently not adopted because they are too costly, too complex, and integration barrier with legacy systems. Small and medium sized businesses (SMB) that cannot afford new cryptographic methods consequently use outdated or inadequate methods, as a consequence, their system becomes open susceptible to attack [36]. Also, to protect data there are region-specific laws like GDPR, HIPAA or PCI DSS that require encryption for any data that is to be stored. That is why effective compliance that can be adjusted to various regional and industry demands becomes challenging. Non-compliance not only opens organizations to breaches but also pay penalties for breaches [38].

Applying cryptographic approaches is often a computational challenge, especially when it is deployed on low computing capacity devices like IoT and mobile platforms. High encryption can demand a considerable number of computational procedures, which in turn affects the energy consumption and battery durability in portable devices. However, there is still a challenge of how to incorporate these solutions into currently formatted systems and a challenge of compatibility with the other systems. As devices continue to get connected, concern for low power and resource constraint devices without hindering their utility or battery life could become critical [39].

7. Quantum Resistant Cryptographic Algorithms

With the rapid improvement of quantum computing, a new breed of cryptographic algorithms is being developed for resisting quantum-based attack. In this section we explore these cutting-edge algorithms and their importance in providing robust security for the future.

7.1. Lattice-Based Cryptography

Lattice-based cryptography solves problems in high-dimensional lattices such as the Learning with Errors (LWE) problem, or the Shortest Vector Problem (SVP). These problems are difficult for classical and quantum computers; therefore, lattice-based cryptography can be considered as the candidate for the post-quantum standards. Lattice-based cryptography's major advantage is its adaptability as a cryptographic scheme. It also supports functionalities such as fully homomorphic encryption that allow for the computations on encrypted data. This offers new possibilities for privacy preserving data analysis and secure cloud computing. Nonetheless, difficulties persist in deploying these algorithms for such use, as lattice-based systems are normally more computational than other forms of cryptography [40]

7.2. Code-Based Cryptography

Code-based cryptography is predicated on the hardness of decoding random linear codes, a problem extensively researched over the last century and believed to be quantum resistant. One of the strongest candidates for post-quantum encryption is classic McEliece, one of the earliest and best studied code based cryptographic systems. It provides high security and has proved to be stable; however, large key sizes present some difficulties with storage and messaging. Code-based cryptography can be very useful in providing the long-term data security desired. Advances like BIKE and HQC utilize quasi-cyclic codes with the aim of shrinking key sizes and making the algorithms more computationally efficient and able to resist threat from quantum computer [41].

7.3. Multivariate Polynomial Cryptography

Multivariate polynomial cryptography is based on the possibility of solving a system of multivariate quadratic equations which is hard for both classical and quantum computers. Examples of such an approach are Rainbow, a digital signature scheme and Generalized Multivariate Signature Scheme (GeMSS). Rainbow has attracted considerable attention because of its effectiveness in producing and verifying signatures even in limited resources environment such as IoT devices [42].

Post-quantum cryptographic applications of multivariate polynomial cryptography are seen to hold a lot of promise, especially due to small key sizes when compared to other cryptographic algorithms. Its implementation has been slow but steady and current research are constantly improving the stability and flexibility to be able to prevent quantum attacks. These contributions seek to enhance its defense against higher-level cryptographic attacks and also try to simplify and enhance deeper multivariate cryptographic schemes for uses in the future [42-43].

7.4. Hash-Based Cryptography

Security of hash-based cryptography depends on the robustness of cryptographic hash functions. They are resistant to quantum attacks and can be used for applications without compromising performance. Unlike the traditional public-key systems such as RSA and ECC, recent hashing approaches like SPHINCS+ primarily lay emphasis on the identification of secure and efficient signatures. SPHINCS+ is a stateless hash-based signature scheme that will reduce efficiency challenges in traditional systems and at the same time guarantee security. SPHINCS+ is also suitable for use by systems that need to secure files containing software updates and digital archives over a long period [44]. Another benefit of using hash-based cryptography is that it is quite simple and based on basic integer arithmetic operations. That makes it a good option for applications that has to be robust and trustworthy, but its disadvantage is that hash-based signature schemes take more storage space than traditional schemes and can be a problem for systems that have limited bandwidth. However, its strong resistance to quantum threats keeps it as an essential component of a post quantum cryptographic paradigm [45].

7.5. Isogeny-Based Cryptography

Isogeny-based cryptography can be based on a mathematical structure of elliptic curve isogenies and is relatively light-weighted. To facilitate this, algorithms such as Isogeny Key Encapsulation (SIKE) are known to offer secure key exchange, which has little computational and bandwidth costs. This makes isogeny-based cryptography particularly suitable for resource-constraint application environments needed in IoT devices, and embedded systems [46].

8. Research Implications

This review finds the need for continued research in cryptographic techniques to address both the existing and newly emerging challenges. There is the need for urgent improvements in quantum resistant algorithms in response to the rapid development of quantum computing such as the protection of data for the future. The advancement in lightweight cryptography could bridge the security resource gap between robust security and resource constraints of the IoT devices.

9. Conclusion

Cryptography is one of the core building blocks of current information security used for protecting data, ensuring confidentiality of communications, and verifying system integrity across a range of uses. Starting from the basic principles including symmetric and asymmetric encryption, up to advanced techniques such as lattice and hash based quantum resistant ways, cryptography has been changing to address the new threats. The increasing problems associated with implementation factors, usage of more limited resources, and the potential threats of quantum computing call for continuous research and development. Thus, through the implementation of secure, effective, and quantum-protection cryptographic technologies, organizations can be ready for future threats.

Compliance with ethical standards

Disclosure of conflict of interest

There is no conflict of interests

References

[1] Maqsood F, Ahmed M, Ali MM, Shah MA. Cryptography: a comparative analysis for modern techniques. International Journal of Advanced Computer Science and Applications. 2017;8(6).

[2] Jirwan N, Singh A, Vijay S. Review and analysis of cryptography techniques. International Journal of Scientific & Engineering Research. 2013 Mar;4(3):1-6.

[3] Alenezi MN, Alabdulrazzaq H, Mohammad NQ. Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security. 2020 Aug 1;12(2):256-72.

[4] Abd Elminaam DS, Abdual-Kader HM, Hadhoud MM. Evaluating the performance of symmetric encryption algorithms. International Journal of Network Security. 2010 ;10(3):216-22.

[5] Simmons GJ. Symmetric and asymmetric encryption. ACM Computing Surveys (CSUR). 1979 Dec 1;11(4):305-30.

[6] Paulevé L, Jégou H, Amsaleg L. Locality sensitive hashing: A comparison of hash function types and querying mechanisms. Pattern recognition letters. 2010 Aug 1;31(11):1348-58.

[7] Saez Y, Estebanez C, Quintana D, Isasi P. Evolutionary hash functions for specific domains. Applied Soft Computing. 2019;78:58-69.

[8] Henriques MS, Vernekar NK. Using symmetric and asymmetric cryptography to secure communication between devices in IoT. In2017 International Conference on IoT and Application (ICIOT) 2017 19 (pp. 1-4). IEEE.

[9] Henriques MS, Vernekar NK. Using symmetric and asymmetric cryptography to secure communication between devices in IoT. In2017 International Conference on IoT and Application (ICIOT). 2017; 19 (pp. 1-4). IEEE.

[10] Xu H, Thakur K, Kamruzzaman AS, Ali ML. Applications of cryptography in database: a review. In2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS). 2021; (pp. 1-6). IEEE.

[11] Maurer U. The role of cryptography in database security. InProceedings of the 2004 ACM SIGMOD international conference on Management of data 2004 Jun 13 (pp. 5-10).

[12] Chatterjee R, Chakraborty R, Mondal JK. Design of lightweight cryptographic model for end-to-end encryption in IoT domain. IRO Journal on Sustainable Wireless Systems. 2019; 1(4):215-24.

[13] Vegesna VV. Investigations on Different Security Techniques for Data Protection in Cloud Computing using Cryptography Schemes. Indo-Iranian Journal of Scientific Research (IIJSR) Volume. 2019;3:69-84.

[14] Kho YX, Heng SH, Chin JJ. A review of cryptographic electronic voting. Symmetry. 2022 Apr 21;14(5):858.

[15] Aidynov T, Goranin N, Satybaldina D, Nurusheva A. A Systematic Literature Review of Current Trends in Electronic Voting System Protection Using Modern Cryptography. Applied Sciences. 2024; 14(7):2742.

[16] Yan L, Rong C, Zhao G. Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. InCloud Computing: First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings 1 2009 (pp. 167-177). Springer Berlin Heidelberg.

[17] Rana M, Mamun Q, Islam R. Lightweight cryptography in IoT networks: A survey. Future Generation Computer Systems. 2022; 129:77-89.

[18] Azeez M, Ugiagbe UO, Albert-Sogules I, Olawore S, Hammed V, Odeyemi E, Obielu FS. Quantum AI for cybersecurity in financial supply chains: Enhancing cryptography using random security generators. World Journal of Advanced Research and Reviews. 2024;23(1):2443-51.

[19] Alassaf N, Gutub A. Simulating light-weight-cryptography implementation for IoT healthcare data security applications. International Journal of E-Health and Medical Communications (IJEHMC). 2019; 10(4):1-5.

[20] Singh AK, Anand A, Lv Z, Ko H, Mohan A. A survey on healthcare data: a security perspective. ACM Transactions on Multimidia Computing Communications and Applications. 2021; 17(2s):1-26.

[21] Ullah S, Zheng J, Din N, Hussain MT, Ullah F, Yousaf M. Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. Computer Science Review. 2023; 47:100530.

[22] Tsantikidou K, Sklavos N. Threats, Attacks, and cryptography frameworks of cybersecurity in critical infrastructures. Cryptography. 2024; 8(1):7.

[23] Oliva delMoral J, deMarti iOlius A, Vidal G, Crespo PM, Martinez JE. Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective. IEEE Internet of Things Journal. 2024 Jun 6.

[24] Raeisi-Varzaneh M, Dakkak O, Alaidaros H, Avci İ. Internet of Things: Security, Issues, Threats, and Assessment of Different Cryptographic Technologies. Journal of Communications. 2024; 19(2).

[25] Mousavi SK, Ghaffari A, Besharat S, Afshari H. Security of internet of things based on cryptographic algorithms: a survey. Wireless Networks. 2021; 27(2):1515-55.

[26] Hagui I, Msolli A, ben Henda N, Helali A, Gassoumi A, Nguyen TP, Hassen F. A blockchain-based security system with light cryptography for user authentication security. Multimedia Tools and Applications. 2024; 83(17):52451-80.

[27] Pelluru K. Cryptographic Assurance: Utilizing Blockchain for Secure Data Storage and Transactions. Journal of Innovative Technologies. 2021; 4(1).

[28] Teh JS, Alawida M, Sii YC. Implementation and practical problems of chaos-based cryptography revisited. Journal of Information Security and Applications. 2020; 50:102421.

[29] Scarani V, Kurtsiefer C. The black paper of quantum cryptography: real implementation problems. Theoretical Computer Science. 2014; 560:27-32.

[30] Acar Y, Backes M, Fahl S, Garfinkel S, Kim D, Mazurek ML, Stransky C. Comparing the usability of cryptographic apis. In2017 IEEE Symposium on Security and Privacy (SP) 2017 May 22 (pp. 154-171). IEEE.

[31] Li X, Samaka M, Chan HA, Bhamare D, Gupta L, Guo C, Jain R. Network slicing for 5G: Challenges and opportunities. IEEE Internet Computing. 2017 Sep 18;21(5):20-7.

[32] Lawrence TS, Oyirinnaya, P, Adesola AA, Iguodala OD. The crucial role of artificial intelligence in fintech for suptech and regtech supervision in banking and financial organizations. International Journal of Artificial Intelligence Research and Development. 2025; 3:1;38-50.

[33] Kirsch Z, Chow M. Quantum computing: The risk to existing encryption methods. Retrieved from URL: http://www. cs. tufts. edu/comp/116/archive/fall2015/zkir sch. pdf. 2015.

[34] Kilber N, Kaestle D, Wagner S. Cybersecurity for quantum computing. arXiv preprint arXiv:2110.14701. 2021.

[35] Areo G. The Future of Cybersecurity for Critical Infrastructure: Emerging Trends and Key Challenges.

[36] Jones AJ. LLMs for Enhancing Privacy and Data Protection in Quantum Computing Environments. InLeveraging Large Language Models for Quantum-Aware Cybersecurity 2025 (pp. 67-104). IGI Global Scientific Publishing.

[37] Awan U, Hannola L, Tandon A, Goyal RK, Dhir A. Quantum computing challenges in the software industry. A fuzzy AHP-based approach. Information and Software Technology. 2022; 147:106896.

[38] Adeosun OA, Fakeyede MO, Adesola, AA, Akingbulere G and Anifowoshe DO. Security Implication of network slicing in 5g-Enabled IoT environment. World Journal of Advanced Research and Reviews. 2024; 24(03)2359-2373.

[39] Micciancio D, Regev O. Lattice-based cryptography. InPost-quantum cryptography 2009 (pp. 147-191). Berlin, Heidelberg: Springer Berlin Heidelberg.

[40] Widodo AM, Pappachan P, Sekti BA, Anwar N, Widayanti R, Rahaman M, Bansal R. Quantum-Resistant Cryptography. InInnovations in Modern Cryptography 2024 (pp. 100-130). IGI Global.

[41] Ding J, Gower JE, Schmidt DS. Multivariate public-key cryptosystems. In International conference on the Algebra and its application 2005 Mar (pp. 79-94).

[42] Dey J, Dutta R. Progress in multivariate cryptography: Systematic review, challenges, and research directions. ACM Computing Surveys. 2023; 55(12):1-34.

[43] Tambe-Jagtap SN. A Survey of Cryptographic Algorithms in Cybersecurity: From Classical Methods to Quantum-Resistant Solutions. SHIFRA. 2023; 2023:43-52.

[44] Tambe-Jagtap SN. A Survey of Cryptographic Algorithms in Cybersecurity: From Classical Methods to Quantum-Resistant Solutions. SHIFRA. 2023; 2023:43-52.

[45] Widodo AM, Pappachan P, Sekti BA, Anwar N, Widayanti R, Rahaman M, Bansal R. Quantum-Resistant Cryptography. In Innovations in Modern Cryptography 2024 (pp. 100-130). IGI Global.

[46] Wijethilaka S, Liyanage M. Survey on network slicing for Internet of Things realization in 5G networks. IEEE Communications Surveys & Tutorials. 2021; 23(2):957-94.