Efficient and secure data transmission: cryptography techniques using ECC

Abdullah Ahmad Alhaj[1], Adnan Alrabea[2], Omar Jawabreh[3]
[1]Department of IT, School of Information Technology and Systems, The University of Jordan, Aqaba, Jordan
[2]Prince Abdullah Bin Ghazi Faculty of Information and Communication Technology, Al-Balqa Applied University, Al-Salt, Jordan
[3]Department of Hotel Management, Faculty of Tourism and Hospitality, The University of Jordan, Aqaba, Jordan

Article Info

Article history:

Received Mar 8, 2024
Revised May 31, 2024
Accepted Jun 5, 2024

Keywords:

Cryptography
Data transmission
Decryption
ECC
Security encryption

ABSTRACT

Data transmission has become a crucial aspect of our daily lives in the current digital age. However, this transmission comes with the risk of security breaches, which can result in data theft and unauthorized access. This issue can be addressed by using cryptographic techniques such as elliptic curve cryptography (ECC). In comparison to other cryptosystems, ECC is a potent cryptographic tool that provides high levels of security with comparatively reduced key sizes. This paper discusses the use of ECC in efficient and secure data transmission. It provides a comprehensive overview of ECC, including its mathematical background and how it can be applied to encryption and decryption processes. The paper also presents a comparison of ECC with other cryptographic techniques and highlights its advantages, including its resistance to attacks and efficiency in resource-constrained environments. Finally, the paper discusses the implementation of ECC in real-world scenarios and its potential to revolutionize secure data transmission.

Corresponding Author:

Omar Jawabreh
Department of Hotel Management, Faculty of Tourism and Hospitality, The University of Jordan
Aqaba, Jordan
Email: o.jawabreh@ju.edu.jo

1. INTRODUCTION

In the current digital age, data transmission plays a vital role in our daily lives. From online shopping to internet banking, we constantly rely on the transmission of data through various electronic devices. However, the transfer of this data comes with the risk of security breaches, which can result in data theft, financial losses, and unauthorized access. To address this issue, cryptographic techniques have been developed to ensure secure transmission of data. One such cryptographic tool that has gained popularity in recent years is elliptic curve cryptography (ECC). In comparison with other cryptographic systems, ECC can be considered as a public-key cryptography that offers smaller key sizes thus possessing a relatively high state of security. This article gives a general introduction to ECC and how it can be used for secure and effective data transmission [1].

It is crucial to secure sensitive information as it is being sent in the increasingly linked digital world. ECC [2] is becoming a very effective method for transmitting data securely and efficiently. This paper investigates the foundational ideas of ECC and clarifies its uses to guarantee safe and efficient data transfer.

ECC is a subset of public-key cryptography that encrypts and decrypts data using the mathematical characteristics of elliptic curves. ECC provides similar security with far lower key sizes than classic cryptographic methods like rivest-shamir-adleman (RSA), which are dependent on the difficulty of factoring huge numbers. Because of this, ECC is especially well-suited for situations with limited resources, such as those found in mobile and internet of things (IoT) devices [3]-[6].

Elliptic curves: the algebraic structure of elliptic curves defined over finite fields is the subject of ECC operations. These curves' non-linearity and the difficulty of solving the discrete logarithm issue are among the qualities that make them appropriate for use in cryptography procedures. Public and private keys: ECC uses two keys, a public key that is openly published and a private key that has to be kept confidential, just like other public-key cryptosystems. These keys are used for both encryption and decryption; they are obtained from points on the elliptic curve. ECC operations include addition and multiplication of points that are specified on the elliptic curve. Fundamental operations like multiplication and addition serve as the foundation for ECC algorithms like the elliptic curve digital signature algorithm (ECDSA) for digital signatures and the elliptic curve diffie-hellman (ECDH) for key exchange. Alhaj *et al.* [7], ECC's advantages for data transmission to enhanced security: considering the key size being utilized, ECC provides a high degree of security. This implies that security may be maintained while using smaller key sizes, which lowers computational overhead and storage needs. Furthermore, ECC algorithms are impervious to a range of cryptographic techniques, including quantum and brute-force attacks [8].

Efficient resource utilization: because ECC keys are tiny, they allow for the efficient use of computational resources [9]. Which makes them ideal for devices like smartphones and IoT devices that have limited processing and memory capacity. This efficiency improves system performance overall by enabling quicker cryptographic operations and using less energy.

Compatibility with current standards: ECC has been widely used in a number of cryptographic protocols and standards, including ECDSA and transport layer security (TLS), which secure internet connections. Its interoperability with the current infrastructure enables its simplicity of integration into a variety of platforms and applications [10]. ECC's use in data transmission applications: secure communication: to provide secure channels of communication between clients and servers over unsecured networks, ECC is used in protocols like TLS and secure shell (SSH) [11], [12]. ECC guarantees the confidentiality and integrity of data exchanged between parties by encrypting it to prevent manipulation and eavesdropping.

Digital signatures: to confirm the legitimacy and integrity of digital documents and transactions, ECC-based digital signatures, such as ECDSA, are used. Digital signatures made using ECC provide strong cryptographic guarantees, enabling non-repudiation and trust in electronic transactions. Key exchange: the safe transfer of cryptographic keys between parties is facilitated by ECC-based key exchange protocols such as ECDH. Through the use of the elliptic curve discrete logarithm problem's computational difficulty, ECDH allows parties to determine a shared secret key without disclosing private information to prying eyes.

A notable development in cryptographic methods is ECC, which provides an attractive trade-off between security and throughput for data transfer. Through the use of elliptic curves' mathematical features, ECC makes a broad variety of applications possible, including digital signatures, key exchange, and secure communication. ECC will continue to be an essential tool for protecting sensitive data and guaranteeing the integrity of digital transactions as the digital world changes.

2. BACKGROUND

In modern times, cryptography has evolved to use mathematical algorithms to convert plain text into a non-readable form (cipher text), which can only be decrypted by an authorized recipient with the correct key. The RSA algorithm, which depends upon the challenge of considering larger values, is the very drastically used cryptographic system [13]. However, RSA key sizes are relatively large, which can result in slower processing times and higher memory requirements. To address this issue, ECC was introduced in the mid-1980s. Secure communication, digital signatures, and payment systems are just a few of the applications where ECC is frequently used. Its usage is anticipated to rise along with IoT, which necessitates secure transmission among gadgets with constrained processor and memory capabilities. ECC uses the algebraic structure of elliptic curves to create a public-private key pair. It provides a higher level of security with smaller key sizes compared to other cryptographic systems, making it an ideal solution for resource-constrained environments. ECC is currently widely utilized in many different applications, including as payment systems, digital signatures, and secure communication.

2.1. Cryptography techniques and its types using ECC

Elliptic curve-based cryptography techniques are a type of cryptographic system that uses elliptic curves to offer a high level of security with comparatively smaller key sizes than other cryptographic systems. It is a variety of public key cryptography that provides cryptographic keys using elliptic curves [14]. ECC is superior to other public key encryption methods like RSA and Diffie-Hellman in a number of ways, including smaller key sizes, quicker computation times, and greater attack resistance. ECC is utilized in many different applications, including key exchange systems, digital signatures, and secure communication [15].

2.2. ECDSA

To offer data authentication and non-repudiation, the digital signature technique ECDSA makes use of elliptic curve cryptography. ECDSA generates a public and a private key, using elliptic curve mathematics. The sender creates a digital signature using the private key and attaches it to the message to sign it using ECDSA. Employing the sender's public key, the recipient can confirm the transmitted data's legitimacy [16].

2.3. ECDH

Elliptic curve cryptography is used by the key exchange technique known as ECDH to safely exchange cryptographic keys between two parties. Using elliptic curve mathematics, ECDH creates a public and a private key. The private key is kept a secret while the public key is made accessible to all. To exchange keys, the two parties exchange their public keys and use their private keys to compute a shared secret. Messages between the two parties can then be encrypted and decrypted using the shared secret [17].

ECDH and ECDSA are the two main ECC-based cryptographic methods [16], These methods, which have several advantages over other public key cryptography methods, are employed in several applications, such as key exchange protocols, secure communication, and digital signatures.

The use of cloud services is on the rise due to their storage capacity, collaborative environment, and security features. Due to its short key size, public key cryptography, in particular ECC, is essential for protecting cloud applications. However, despite recent contributions to enhancing the security of ECC in cloud services, a review integrating recent studies and providing research directions is missing. This paper addresses this gap by reviewing recent studies and analyzing various approaches and techniques in ECC. The review identifies several research directions and open problems for future relevant research in this area [18]. A difficult task is to protect wireless sensor networks (WSNs) from numerous security risks and threats given their widespread use in many different fields. A recommended method using the ECDSA cryptographic system has been devised to provide security for node-to-node communication in WSNs. Key management and communication security on the node level are handled by the algorithm for wireless secure communication (ASCW), which also lowers the expense of security risks. The results of experiments have demonstrated that ASCW is an appropriate and innovative method for safeguarding data on nodes during communication in WSNs, offering a quick and efficient method to secure data [19]. Cloud computing is a widely used technology, but it comes with security challenges. Services are distributed among servers and users, making file protection difficult. Cloud providers struggle to ensure data security, which can result in unauthorized access, misuse, or destruction of data [20]. These limitations highlight the importance of addressing cloud security concerns in the cloud computing environment.

3. ECC FOR SECURE AND EFFICIENT DATA TRANSMISSION

Cryptography techniques using ECC are widely used to secure data transmission over public networks, such as the internet. Smaller key sizes and quicker encryption and decryption times are only a couple of the benefits that ECC has over conventional public-key cryptography systems [21]. There are some ways in which ECC makes data transmission secure and efficient such as smaller key sizes, fast encryption and decryption, resistance to attack, forward secrecy, and key agreement.

3.1. Smaller key sizes

ECC requires smaller key sizes than conventional public-key encryption methods like RSA for security. This is due to the fact that the mathematics underlying ECC is built on elliptic curves, a mathematical structure that is more intricate than the prime numbers employed in RSA. Because of this, ECC keys can be shorter without sacrificing security [22]. Shorter keys mean less data needs to be transmitted during encryption and decryption, which can lead to faster and more efficient communication.

3.2. Fast encryption and decryption

ECC is a faster algorithm than traditional public-key cryptography systems like RSA. This is because the mathematics behind ECC is simpler and more efficient than RSA [23]. Due to its quick processing and low power consumption, ECC is therefore more suited for use in contexts with limited resources, such mobile devices.

3.3. Resistance to attacks

ECC is more resistant to attacks than traditional public-key cryptography systems like RSA. This is because the mathematics behind ECC is based on elliptic curves, which are harder to attack than the prime numbers used in RSA [24]. ECC is also resistant to certain types of mathematical attacks, such as the number field sieve and the elliptic curve discrete logarithm problem.

3.4. Forward secrecy

Some cryptographic systems have a feature called forward secrecy that makes sure that even if an attacker gets hold of the private key used for a specific transmission. They cannot read the message, and they will not be able to use it to decrypt past or future messages [25].

3.5. Key agreement

ECC can be used for key agreement, which means that two can agree on a shared secret key without transmitting it over the network. This can provide additional security and efficiency benefits, as it eliminates the need for key distribution [26]. Specifically, with the help of the Diffie Hellman key exchange, which is supported by ECC, two parties can decide on a shared secret key without sending it over the Internet.

4. RESULTS

The results of the study show that ECC outperforms other popular cryptographic algorithms in several key areas, including key size, speed, resistance to attacks, forward secrecy, and key agreement. ECC’s advantages make it a popular choice for various industries, including finance, healthcare, and e-commerce, where secure data transmission is critical. ECC’s potential also extends to emerging technologies such as the IoT, where its resource efficiency and security make it an ideal choice for secure communication protocols. The implementation of ECC in real-world scenarios has the potential to revolutionize secure data transmission, providing a more efficient and secure alternative to traditional cryptographic techniques [27]. As technology continues to evolve, ECC’s potential will likely continue to expand, making it an essential tool for ensuring secure communication protocols in various industries.

4.1. Comparison of elliptic curve cryptography with cryptographic algorithms

In general, ECC offers smaller key sizes and faster encryption and decryption times than RSA, while also providing stronger resistance to attacks and support for forward secrecy and key agreement. AES is a symmetric-key encryption algorithm that is generally faster than public-key algorithms like RSA and ECC. ChaCha20 is another symmetric-key encryption algorithm that is created to be efficient on several variety of platforms. SHA-256 is a hash function that is used for data integrity and is not used for encryption or decryption. Table 1 compares five key features of ECC with four other popular cryptographic algorithms: RSA, AES, ChaCha20, and SHA-256 [28].

Table 1. Comparison of elliptic curve cryptography with cryptographic algorithms

Features	ECC	RSA	AES	ChaCha20	SHA-256
Smaller key sizes	30-50% smaller than RSA	RSA keys are longer	-	-	-
Fast encryption and decryption	2-4 x faster than RSA	Slower than ECC	10-20 x faster than RSA	2-3 x faster than AES	-
Resistance to attacks	Stronger than RSA	Vulnerable to some attacks	Strong against brute-force	Strong against quantum attacks	Strong against collisions
Forward secrecy	Supported	Not supported	-	-	-
Key agreement	Supported	Supported	-	Supported	-

ECC offers smaller key sizes than RSA, typically 30-50% smaller, while still providing the same level of security. This indicates that ECC is more effective in terms of memory and computing power, making it appropriate for devices and situations with limited resources. AES, ChaCha20, and SHA-256 are all symmetric-key or hash algorithms that do not use public-key cryptography, so key sizes are not directly comparable. ECC is generally faster than RSA for encryption and decryption, typically 2-4 x faster. In general, ECC is more resistant to assaults than RSA, including side-channel attacks, quantum computer attacks, and brute-force attacks. Because each session utilizes a different key, forward secrecy in ECC ensures that even if a private key is compromised in the future, previous conversations will still be safe. Key agreement is supported by ECC and enables two to create a shared secret key without disclosing it to a third party. Overall, ECC offers a balance of security and efficiency, making it a popular choice for many applications. The optimal option will rely on the particular needs of each use case because each cryptographic method has advantages and disadvantages of its own.

4.2. Implementation of ECC in real-world scenarios and its potential to revolutionize secure data transmission

The implementation of ECC in real-world scenarios has the potential to revolutionize secure data transmission. ECC’s advantages, including smaller key sizes, high resistance to attacks, and support for key agreement protocols, make it an ideal choice for various industries, including finance, healthcare, and e-commerce [29]. For example, in the finance industry, ECC can be used for secure online transactions, including mobile banking and credit card transactions. ECC’s smaller key sizes make it a more efficient choice for mobile devices, while its resistance to attacks ensures that transactions remain secure. Similarly, in the healthcare industry, ECC can be used to secure patient records and communication between healthcare providers.

Figure 1 shows that, the ECC can be implemented in various real-world applications across different industries. In the healthcare industry, ECC can be used to secure patient records and communication between healthcare providers. The patient’s medical records can be encrypted using ECC to ensure that they are protected from unauthorized access and breaches [30]. Similarly, healthcare providers can use ECC to secure their servers and communication channels, ensuring that sensitive information is kept confidential. In the finance industry, ECC can be used for secure online transactions, including mobile banking and credit card transactions. ECC’s smaller key sizes make it a more efficient choice for mobile devices, while its resistance to attacks ensures that transactions remain secure. ECC can be implemented in smartphones to secure mobile banking transactions, while banking servers can use ECC to secure their communication channels and protect against data breaches. In e-commerce, ECC can be used in payment gateways to ensure that online transactions are secure and protected against fraud. Digital signatures can also be implemented using ECC to verify the authenticity of digital documents, contracts, and agreements. This helps to ensure that the documents have not been tampered with and that they are authentic. Thus, ECC has the potential to provide a more efficient and secure alternative to traditional cryptographic techniques in various real-world applications across different industries.

ECC’s potential is not limited to traditional industries but also extends to emerging. The implementation of ECC in IoT devices can enhance security and privacy, ensuring that sensitive data is protected from unauthorized access and breaches. Therefore, the implementation of ECC in real-world scenarios has the potential to revolutionize secure data transmission by providing a more efficient and secure alternative to traditional cryptographic techniques. As technology continues to evolve, ECC’s potential will likely continue to expand, making it an essential tool for ensuring secure communication protocols in various industries.

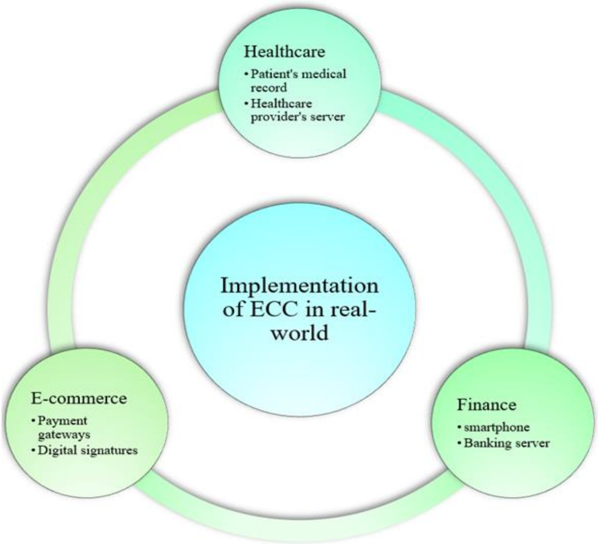

Figure 1. Implementation of ECC in the real world

5. CONCLUSION

In conclusion, ECC is an essential tool for ensuring efficient and secure data transmission in the digital era. With its powerful encryption and decryption capabilities, ECC is an effective option for contexts with limited resources because it offers high levels of security with relatively modest key sizes. The comparison of ECC with other cryptographic techniques highlights its advantages, including its resistance to attacks, forward secrecy, and key agreement support. Additionally, the implementation of ECC in real-world scenarios shows its potential to revolutionize secure data transmission. Therefore, the use of ECC should be considered when implementing secure communication protocols in various industries, including finance, healthcare, and e-commerce. Future studies might examine how well ECC works in conjunction with other cryptographic methods to increase the security of data transfer. Finally, there is a need for a detailed analysis of the potential vulnerabilities of ECC and their mitigation strategies. The study does not address the regulatory and legal aspects of ECC, which can have significant implications for its widespread adoption. Finally, the study focuses only on ECC, and therefore, the comparison of ECC with other cryptographic techniques is limited to those discussed in the study.

PRACTICAL APPLICATIONS

IoT and embedded systems: ECC’s efficiency makes it ideal for securing communications in IoT devices and other embedded systems, which often have limited computational power and memory. ECC is widely used in securing web communications through protocols like HTTPS. It provides robust security for transactions, data exchanges, and sensitive communications without imposing heavy computational loads on servers and clients.

REFERENCES

[1] P. William, A. Choubey, G. S. Chhabra, R. Bhattacharya, K. Vengatesan, and S. Choubey, “Assessment of hybrid cryptographic algorithm for secure sharing of textual and pictorial content,” in *Proceedings of the International Conference on Electronics and Renewable Systems, ICEARS 2022*, Mar. 2022, pp. 918–922, doi: 10.1109/ICEARS53579.2022.9751932.

[2] I. Nazeeh, T. H. Hadi, Z. Q. Mohammed, S. T. Ahmed, and Q. K. Kadhim, “Optimizing blockchain technology using a data sharing model,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 29, no. 1, pp. 431–440, Jan. 2023, doi: 10.11591/ijeecs.v29.i1.pp431-440.

[3] M. M. A. Saleh, O. A. A. Jawabreh, R. Al Om, and N. Shniekat, “Artificial intelligence (AI) and the impact of enhancing the consistency and interpretation of financial statement in the classified hotels in Aqaba, Jordan,” *Academy of Strategic Management Journal*, vol. 20, no. SpecialIssue3, pp. 1–18, 2021.

[4] A. Jahmani, R. Abokhoza, R. N. Zghyer, and O. Jawabreh, “The influence of traveler reviews on mobile applications on travel decision-making to Dubai,” *Journal of Theoretical and Applied Information Technology*, vol. 98, no. 15, pp. 3162–3175, 2020.

[5] E. Malkawi, E. A. Al Fahmawee, and O. Jawabreh, “Assessments of guest technologies in five stars hotel at aqaba special economic zone authority (ASEZA),” *Information Sciences Letters*, vol. 12, no. 8, 2023, doi: 10.18576/isl/120834.

[6] F. F. Al-Hosaini, B. J. A. Ali, A. M. Baadhem, O. Jawabreh, A. A. B. Atta, and A. Ali, “The impact of the balanced scorecard (BSC) non-financial perspectives on the financial performance of private Universities,” *Information Sciences Letters*, vol. 12, no. 9, pp. 2903–2913, Sep. 2023, doi: 10.18576/isl/120901.

[7] A. A. Alhaj *et al.*, “Improving the smart cities traffic management systems using VANETs and IoT features,” *Journal of Statistics Applications and Probability*, vol. 12, no. 2, pp. 405–414, May 2023, doi: 10.18576/jsap/120207.

[8] S. Handore, P. Kolapkar, P. Chavan, and P. Chavan, “Cost-effective anonymous data sharing with forward security using improved authentication,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 1, pp. 129–136, Apr. 2023, doi: 10.11591/ijeecs.v30.i1.pp129-136.

[9] V. Desai and D. H. Annappaiah, “Reputation-based security model for detecting biased attacks in big data,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 29, no. 3, pp. 1567–1576, 2023, doi: 10.11591/ijeecs.v29.i3.pp1567-1576.

[10] G. Shankar *et al.*, “Improved multisignature scheme for authenticity of digital document in digital forensics using edward-curve digital signature algorithm,” *Security and Communication Networks*, vol. 2023, pp. 1–18, Apr. 2023, doi: 10.1155/2023/2093407.

[11] A. B. Semma, M. Ali, M. Saerozi, Mansur, and Kusrini, “Cloud computing: google firebase firestore optimization analysis,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 29, no. 3, pp. 1719–1728, Mar. 2023, doi: 10.11591/ijeecs.v29.i3.pp1719-1728.

[12] S. E. S. Castelo, R. J. L. Apostol, D. M. A. Cortez, R. M. Dioses, M. C. R. Blanco, and V. A. Agustin, “Modification of SHA-512 using Bcrypt and salt for secure email hashing,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 33, no. 1, pp. 398–404, Jan. 2024, doi: 10.11591/ijeecs.v33.i1.pp398-404.

[13] Y. Xu, S. Wu, M. Wang, and Y. Zou, “Design and implementation of distributed RSA algorithm based on Hadoop,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1047–1053, Mar. 2020, doi: 10.1007/s12652-018-1021-y.

[14] Y. Yan, “The overview of elliptic curve cryptography (ECC),” *Journal of Physics: Conference Series*, vol. 2386, no. 1, p. 012019, Dec. 2022, doi: 10.1088/1742-6596/2386/1/012019.

[15] C. Patel, A. K. Bashir, A. A. AlZubi, and R. Jhaveri, “EBAKE-SE: a novel ECC-based authenticated key exchange between industrial IoT devices using secure element,” *Digital Communications and Networks*, vol. 9, no. 2, 2023, doi: 10.1016/j.dcan.2022.11.001.

[16] N. Mehibel and M. Hamadouche, “Authenticated secret session key using elliptic curve digital signature algorithm,” *Security and Privacy*, vol. 4, no. 2, Mar. 2021, doi: 10.1002/spy2.148.

[17] R. I. Chang, C. W. Chiang, and Y. H. Hung, “Grouping sensors for the key distribution of implicit certificates in wireless sensor networks,” *Electronics (Switzerland)*, vol. 12, no. 13, p. 2815, Jun. 2023, doi: 10.3390/electronics12132815.

[18] J. S. Baladhay and E. M. De Los Reyes, “AES-128 reduced-round permutation by replacing the MixColumns function,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 33, no. 3, pp. 1641–1652, Mar. 2024, doi: 10.11591/ijeecs.v33.i3.pp1641-1652.

[19] R. Qazi, K. N. Qureshi, F. Bashir, N. U. Islam, S. Iqbal, and A. Arshad, "Security protocol using elliptic curve cryptography algorithm for wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 547–566, Jan. 2021, doi: 10.1007/s12652-020-02020-z.

[20] P. Chinnasamy, S. Padmavathi, R. Swathy, and S. Rakesh, "Efficient data security using hybrid cryptography on cloud computing," in *Lecture Notes in Networks and Systems*, vol. 145, 2021, pp. 537–547.

[21] H. Kadry, A. Farouk, E. A. Zanaty, and O. Reyad, "Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security," *Alexandria Engineering Journal*, vol. 71, pp. 491–500, May 2023, doi: 10.1016/j.aej.2023.03.072.

[22] J. Bao, "Research on the security of elliptic curve cryptography," in *Proceedings of the 2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022)*, 2022, vol. 652, doi: 10.2991/aebmr.k.220405.164.

[23] D. B. Roy, "Security aware architectural exploration of public key algorithms," 2019.

[24] J. Gao, Y. Chen, and X. Du, "Research hotspots and evolution context of digital platforms based on citespace," in *Atlantis Highlights in Computer Sciences*, 2023, pp. 421–428.

[25] C.-X. Wang *et al.*, "On the road to 6G: visions, requirements, key technologies, and testbeds," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 905–974, 2023, doi: 10.1109/COMST.2023.3249835.

[26] C. T. Poomagal and G. A. S. Kumar, "ECC based lightweight secure message conveyance protocol for satellite communication in internet of vehicles (IoV)," *Wireless Personal Communications*, vol. 113, no. 2, Jul. 2020, doi: 10.1007/s11277-020-07285-3.

[27] A. Kakkar, "A survey on secure communication techniques for 5G wireless heterogeneous networks," *Information Fusion*, vol. 62, pp. 89–109, Oct. 2020, doi: 10.1016/j.inffus.2020.04.009.

[28] P. Kietzmann, L. Boeckmann, L. Lanzieri, T. C. Schmidt, and M. Wählisch, "A performance study of crypto-hardware in the low-end iot," *International Conference on Embedded Wireless Systems and Networks*, 2021.

[29] R. Kumar, P. Kumar, M. Aloqaily, and A. Aljuhani, "Deep-learning-based blockchain for secure zero touch networks," *IEEE Communications Magazine*, vol. 61, no. 2, pp. 96–102, Feb. 2023, doi: 10.1109/MCOM.001.2200294.

[30] S. Mohan M and L. Sujihelen, "An efficient chain code for access control in hyper ledger fabric healthcare system," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 5, p. 100204, Sep. 2023, doi: 10.1016/j.prime.2023.100204.

BIOGRAPHIES OF AUTHORS

Dr. Abdullah Ahmad Alhaj received B.Sc. and M.Sc. degree in computer engineering from Lviv polytechnic institute-USSR, in 1988, PhD in Computer Science from Bradford University UK, in 2008. Currently, he is an associate professor in the Information Technology department at The University of Jordan, Aqaba branch. His research interests include computer architecture, networks, IT security, machine learning, and AI. He can be contacted at email: aa.alhaj@ju.edu.jo.

Dr. Adnan Alrabea received the Dr. Eng. Degree in 2004 from the Electronic and Communication Department, Faculty of Engineering, Donetsk University, Ukraine. He is a visiting Associate Professor and Assistant dean of Prince Abdullah Bin Ghazi Faculty of Science and Information technology at Al-Balqa Applied University, Assalt, Jordan. His research interests cover: analyzing the various types of analytic and discrete event simulation techniques, performance evaluation of communication networks, application of intelligent techniques in managing computer communication network, and performing comparative studies between various policies and strategies of routing, congestion control, sub netting of computer communication networks. He published 30 articles in various refereed international journals and conferences covering: computer networks, expert systems, software agents, e-learning, image processing, wireless sensor networks and pattern recognition. Also, in the current time, he is too interested in making a lot of scientific research in wireless sensor networks in view point of enhancing its algorithms of congestion control as well as routing protocols. He can be contacted at email: dr.alrabea@bau.edu.jo.

Dr. Omar Jawabreh a Professor at the Department of Hotel Management, Faculty of Tourism and Hospitality Management, The University of Jordan, Aqaba Branch. He got his PhD in hospitality and tourism management from the Faculty of Economics and Business (JNVU), India. Field study and interests: tourism accounting, culture and sustainable tourism, marketing, and hospitality. He can be contacted at email: o.jawabreh@ju.edu.jo.