International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

Vol. 42 No. 1 December 2023, pp. 410-419

Efficiency Analysis of Elliptic Curve Cryptography in Vital Information Infrastructure: Time, Security, and Resilience

Gilang Prakoso, Aulia Khamas Heikmakhtiar, Teddy Mantoro

Faculty of Defense Science and Technology, Cyber Defense Engineering
Republic of Indonesia Defense University
Jakarta, Indonesia
Email: gilang.prakoso.gp15@gmail.com

Abstract— Elliptic Curve Cryptography (ECC) is a contemporary form of asymmetric key cryptography widely employed in critical security domains, including encryption, decryption, and authentication. Its utilization has become increasingly prevalent in the Vital Information Infrastructure (IIV) to ensure secure communication and data exchange over time, driven by technological advancements and the growing size of data. This paper aims to provide a comparative relative efficiency analysis of ECC usage in the IIV, focusing on key aspects such as time efficiency, the relationship between curve size and security strength level, and the resilience of different curve sizes against Brute-Force attacks, Pollard Rho attacks, and Elliptic Curve Discrete Logarithm Problem (ECDLP) attacks. The results demonstrate that SECP521R1 features the largest key size and slowest key exchange time. Notably, SECP521R1 displays the highest level of resistance against various attacks, making it the most robust curve in terms of security.

Keywords— Elliptic Curve Cryptography, Vital Information Infrastructure, Security Strength, Cryptography, Asymmetric Key.

I. INTRODUCTION

Failures of critical infrastructure systems have serious repercussions. Beyond that, the impact might spread not just throughout the system of vital infrastructure (among interconnected components), but external to the mechanism, harming society and national goals such as national security, economic growth, and fundamental human necessities (Hromada, 2017). Several external and internal system elements affect the degree of impact, spreading throughout the consequences of vital malfunctions. While external elements such as societal resilience and character, as well as the magnitude or period of a crisis, are important, the type and scope of the failure within the system, as well as subsystem linkages, are important internal considerations, as well as component robustness. The breadth, structure, severity, length, and impact during an incident define the nature of the impacts. See Fig. 1 (Steven M. Rinaldi, 2001).

Many government agencies are still seeking ways to strengthen or establish robust security systems, owing to the regular incidence of failures and crimes that have had an impact both inside and outside critical infrastructure systems. The continuity of critical infrastructure services hinges on securing the Information Infrastructure (VII) system- making it imperative that effective measures are put into place. Cryptography serves as one such solution to prevent unwanted access to sensitive data (Government of Canada, 2021). It has now become an integral part of modern security systems. Elliptic Curve Cryptography (ECC) is being looked upon favorably in recent times for its superior performance to classic cryptographic mechanisms like RSA - It boasts smaller key sizes, faster encryption/decryption rates, and lower power consumption- making it a suitable option for software that has limitations in terms of available resources (Rashidi, 2017).

Cryptographic techniques are particularly significant in the global field of technological advances, especially in the Information Vital Infrastructure (IIV), for security for the country as well as its users, such as power networks, transportation systems, and the health sector (Mishall Al-Zubaidie, 2019). Elliptic Curve Cryptography (ECC) has risen in recent years as a

Corresponding Author: Gilang Prakoso

result of its capacity to meet high-security standards while using relatively small key sizes. Nevertheless, inside the Infrastructure of Vital Information (IIV), ECC has several issues, such as many ECC system components having insufficient computing capacity. Furthermore, ECC deployments have been at risk from attacks like power analysis and timing assaults, which could threaten system security.

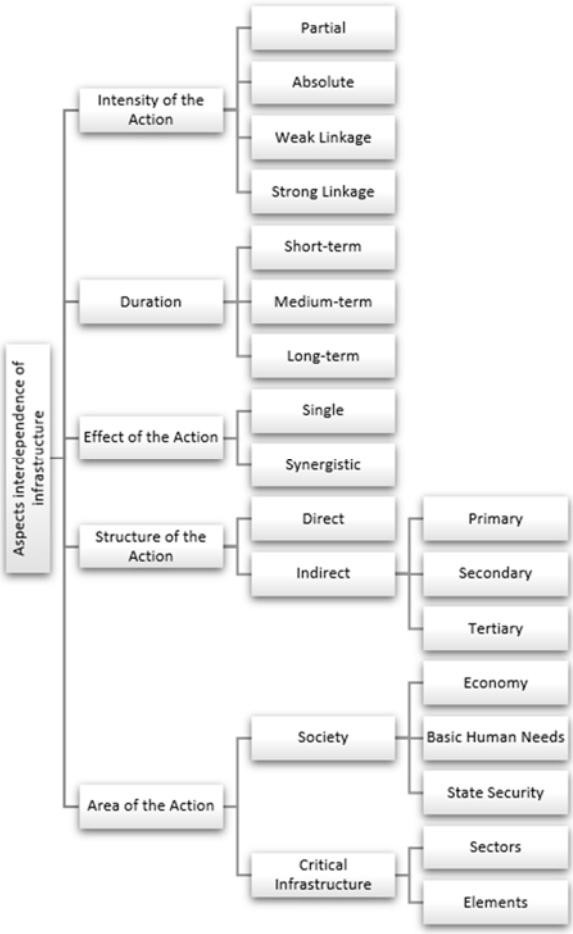

Fig. 1. Aspects to define the interdependence of infrastructure *(Steven M. Rinaldi, 2001)*.

In addition, handling key information is a critical aspect of implementing ECC, and it is especially problematic in a distributed environment like Vital Information Infrastructure. Finally, integration of prior encryption technologies and standards might be difficult, thus limiting ECC utilization in these systems. In this paper, we investigate and provide solutions to the problems associated with adopting ECC in Vital Information Infrastructure.

The authors focus on the application of ECC to the Vital Information Infrastructure (IIV) system, as well as the challenges and implementation of the approach in this article. Furthermore, this article will discuss the benefits and drawbacks of the ECC technique, compare the capabilities of several curves in the ECC technique, assess the capabilities and security of the curve on the Vital Information Infrastructure (IIV) system, and provide solutions to problems encountered when using the ECC technique on the Vital Information Infrastructure (IIV) system. The study's findings can be used to develop secure and efficient cryptographic approaches for use in the Vital Information Infrastructure (IIV) system.

II. RELATE WORK

2.1. Literature Review

Rodrigo Roman's article "The Role of Wireless Sensor Networks in the Area of Critical Information Infrastructure Protection" explores the significant use of a WSN, which is a wireless sensor network, in vital data infrastructure (CII) protection (Rodrigo Roman, 2007). Rodrigo Roman also discussed several attacks that occurred on CII. He also claimed that WSNs can detect and prevent many types of attacks. This study comprehensively examines WSNs and their components, such as base stations, sensor nodes, and sensor sinks. Of course, Rodrigo Roman recognizes the obstacles in developing a WSN as a CII protection endeavor, such as a trustworthy and secure communication protocol, as well as the enormous amount of data management by sensor nodes.

Vipul Gupta's article examines the use of elliptic curve cryptography (ECC) as vital information infrastructure, concentrating on the issues encountered and offering solutions to ensure robust system security (Vipul Gupta, 2004). The incorporation of elliptic curve cryptography (ECC) for secure website architecture is examined in this article. It goes over the benefits of ECC, such as better efficiency, faster encryption, and decryption speeds, and lower bandwidth requirements. It also examines the difficulties associated with the move from classical methods to ECC, such as the necessity for standardization, compatibility issues, and ECC key management. Additionally, Vipul Gupta talks about various methods and protocols for incorporating ECC into various aspects of web security, such as the secure socket layer protocol (SSL) and the transport layer security protocol (TLS), highlighting the importance of selecting an appropriate elliptic curve and key size, as well as implementing efficient key management. Thus, Vipul Gupta emphasizes the need to incorporate ECC into the web security infrastructure in this publication, as well as providing insight into the obstacles and solutions involved in this process. The paper examines the benefits of ECC and provides insights for enterprises interested in implementing ECC to improve web security.

In his article "Analysis of Standard Elliptic Curves for the Implementation of Elliptic Curve Cryptography in Resource-Constrained E-commerce Applications," Javed R. Shaikh presents a brief examination of ECC. In his article, he claims that ECC has safety and effectiveness improvements over other cryptographic approaches and algorithms like RSA. He also addressed some of the issues that arise when implementing ECC to constrained in resources e-commerce applications, such as those with limited CPU power and memory. Based on the Koblitz curve, this experiment creates and tests an uncommon elliptic curve for constrained in resources e-commerce applications. According to the authors, the designed Koblitz curve is a viable solution for constrained resources e-commerce applications, delivering higher safety and effectiveness than several conventional NIST curves (Shaikh, 2017).

Alowolodu et al.'s article "Elliptic Curve Cryptography for Securing Cloud Computing Applications" focuses on elliptic curve cryptography (ECC) as a security method for cloud computing applications (Olufunso Alowolodu, 2013). The authors emphasize the growing use of cloud-based computing and the importance of efficient safeguards for securing sensitive data and user privacy. It provides a thorough explanation of ECC by comparing it to other cryptography techniques like RSA, ECC has been shown in studies to provide greater privacy with smaller key sizes while being less costly in terms of CPU resources and bandwidth use. They noted that ECC is ideally suited for resource-constrained cloud computing scenarios. They describe how ECC may reduce numerous security issues in the cloud, such as data breaches and illegal access, and emphasize the benefits of ECC in terms of privacy, integrity, and non-denial. Meanwhile, this article highlights the difficulties connected with adopting ECC in cloud computing, such as dealing with key management and connectivity problems. The authors propose solutions to these difficulties, such as the utilization of efficient key-generating and disseminating algorithms, secure key storage systems, and standardized interoperability protocols.

Sangram Ray mentioned in his article "Design of Mobile Public Key Infrastructure (M-PKI) Using Elliptic Curve Cryptography" that many electronic services have used applications and facilities that provide an internet connection to aid each community's operations. As a result, many people can readily access the internet via cell phones to obtain information and make payments via e-banking, mobile application facilities in the health sector, and business. So, according to Sangram Ray, there is a security vulnerability in wireless networks that is not a problem, particularly on personal cell phones. As a result, he created Mobile Public Key Infrastructure (M-PKI) for mobile devices. In his concept, he updated the existing PKI by introducing ECC as a short key/message, low computation/communication cost, and the inclusion of MHA per mobile user to carry the majority of the burden associated with certificates and RA to collaborate with CA. He also recommended the use of customized URLs. Thus, according to his findings, M-PKI provides adequate security and is appropriate for mobile phones running any application (Sangram Ray, 2013).

2.2. Relative Efficiency

Relative efficiency is a method of comparing the levels of efficiency of two or more systems or processes concerning various elements that influence them. It describes how well a system performs in terms of performance against multiple influencing elements to reach the same aim and outcome (Marcos P. C. Medeiros, 2015). In this paper, the author tries to implement the equation of relative efficiency to calculate how the ECC curves give some relative efficiency with the indicator time efficiency, security strength, and resilience of asymmetric key cryptography. The equation is:

$$efficency\ relative = \frac{method\ times}{execution\ times} \quad (1)$$

2.3. Elliptic curve cryptography

Elliptic curve cryptography (ECC), a type of public key encryption, is based on the mathematical properties of elliptic curves over finite fields. It is commonly employed for digital signatures and secure communication protocols such as SSL/TLS for online data transmission (Kristin Lauter, 2004). The difficulty of solving the elliptic curve discrete logarithm problem (ECDLP) determines cryptography. Given a point, P, and a public point Q, the value of k must be determined, where k is the scalar multiplier that generates point P on the elliptic curve. Because ECDLP is a computationally difficult problem, ECC is a secure encryption technology. A planar algebraic curve with all points x and y is described in mathematics by the equation:

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Iy + J = 0 \quad (2)$$

Elliptic curves are described by the equation:

$$y^2 = x^3 + ax + b \quad (3)$$

In this equation, a and b are constants, and x and y are variables. The curve's points form a group, and the point addition operation is used in ECC. ECC uses a finite field to limit the range of values for x and y, making point addition and scalar multiplication faster and more efficient.

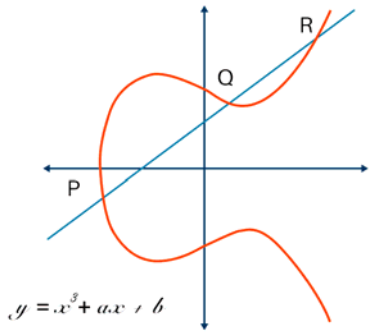

Fig. 2. Basic Elliptic Curve.

2.4. SECP192R1

In elliptic curve cryptography (ECC), the elliptic curve SECP192R1 is employed (The Mbed TLS Contributors, n.d.). It belongs to the NIST family of curves, which consists of elliptic curves recommended by a committee of the National Institute of Standards and Technology (also known as NIST) of the United States for use in security-related applications that involve encryption and digital signatures. SECP192R1 is a 192-bit symmetric algorithm designed to provide the same satisfactory protection as 80-bit symmetric algorithmic methods.

NIST has also evaluated and validated this curve to verify its safety and efficacy in security applications. SECP192R1 curves are commonly employed in resource-constrained security applications, including mobile phones and the Internet of Things (IoT). It can also be used as a substitute for other elliptic curves in encrypted systems which require security levels of 80 bits.

2.5. SECP224R1

SECP224R1 is a cryptographic elliptic curve with a fundamental field of 224 bits (The Mbed TLS Contributors, n.d.). It is recommended by the National Institute of Standards and Technology (NIST) for use in elliptic curve encryption. SECP224R1 is an SECG (Standards for Efficient Cryptography Group) elliptic curve family member, often known as P-224. The curve has a generator point G in elliptic curve cryptography, which acts as the basis for scalar multiplication operations. The point G's coordinates (x, y) are also standardized. The order of the curve, or the number of points on the curve, is a high prime number, which makes it ideal for cryptographic applications.

SECP224R1 is a cryptographic protocol that is extensively used in SSL/TLS, digital signatures, and key agreement protocols. It offers a superb balance of security and efficiency, therefore becoming an attractive option for a variety of applications. The security of SECP224R1 is predicated on the intricate nature of the elliptic curve's unique logarithm issue, which is regarded to be difficult. Despite its extensive use, SECP224R1 is vulnerable to assaults, and experts are continuing to scrutinize the curve for faults and suggestions for improvements.

2.6. SECP256R1

SECP256R1 is an elliptic curve defined in the Standards for Efficient Cryptography (SEC) by the National Institute of Standards and Technology (NIST) (The Mbed TLS Contributors, n.d.). The P-256 curve, as it is often known, is used in many modern cryptographic protocols and applications. The SECP256R1 curve depends on elliptic curve concepts in math, allowing cryptographic operations such as key exchange and digital signatures to be conducted. The curve is a Weierstrass curve, which is a type of elliptic curve with a set of parameters that affect its security and efficiency. The curve is widely used in industry, such as the Transport Layer Security, also known as TLS, protocol, which is utilized for securing connections to the internet and is regarded to provide a significant amount of confidentiality.

The SECP256R1 curve outperforms previous curves in several ways, including enhanced efficiency in cryptographic operations and compatibility with existing cryptographic protocols and applications. The curve's 256-bit key size provides a high level of security, making it resistant to brute-force attacks. In addition, the curve is optimized for processing and storage utilization, thus being appropriate for application in limited resources situations like systems embedded and smartphones. Overall, the SECP256R1 curve is a well-known and secure elliptic curve with strong cryptographic capabilities that may be used in a variety of applications.

2.7. SECP384R1

SECP384R1 is a well-known elliptic curve in cryptography with public keys (The Mbed TLS Contributors, n.d.). It is one of the curve shapes proposed by the National Institute of Standards and Technology (NIST) in the United States and is widely used in modern cryptographic protocols. Because the curve is specified over a limited space of prime order, it can be used in high-security cryptographic systems. SECP384R1 is a Koblitz curve, a type of elliptic curve with unique properties that allow it to perform cryptographic operations faster than other types of curves. Because it is a 384-bit elliptic curve, SECP384R1 has 384 bits of security. This provides an identical level of authentication equivalent to a 7680-bit RSA key or a 256-bit symmetric key.

The elliptic curve discrete logarithm problem (ECDLP), which is the issue of finding a scalar multiple of a given point on the curve, is the foundation of the curve's security. This problem is regarded to be computationally demanding, which indicates that it cannot be solved for large curves such as SECP384R1. It is used in many cryptographic applications, including electronic signatures, key transfer, and encryption. This usually works in conjunction with the Elliptic Curve Digital Signature Algorithm (ECDSA), an elliptic curve-based digital signature technique that is widely employed. The curve is also used to secure internet communication in Transport Layer Security, also known as TLS. SECP384R1 is a popular choice for a wide range of applications because of its exceptional combination of security and efficiency.

2.8. SECP521R1

SECP521R1 is an elliptic curve domain parameter that has been specified by the National Institute of Standards and Technology (NIST) for use in cryptographic applications (The Mbed TLS Contributors, n.d.). It is a curve with a field size of 521 bits formed over a finite field of prime order. The curve was chosen by NIST due to its large size, which makes it more resistant to certain types of attacks, as well as its efficient arithmetic properties. Over GF(p), when p is a 521-bit unique and a and b are

standard constants. The curve has a generator point G, which is also given in the standard, and the issue of discrete logarithms in the curve's group of points determines the security of the elliptic curve encryption system based on this curve.

SECP521R1 is frequently used in cryptographic protocols and applications such as SSL/TLS, VPN, and digital signatures. It is a strong candidate for high-security applications requiring sophisticated cryptographic primitives due to its large size and efficient arithmetic. However, it may necessitate more processing resources than smaller-sized curves, which should be taken into account when choosing a curve for a certain application.

2.9. Elliptic Curve Decision

Each of the global guidelines that are now available concerned with deciding on reliable and secure elliptic curves for ECC implementation. The goal of each curve standard is to make the Elliptic Curve Discrete Logarithm Problem (ECDLP) as difficult as feasible (Lein Harn, 2014) (Rolla Subrahmanyam, 2023). Each requirement specifies the form of the elliptic curve as well as the particulars of the main sectors and coefficients in the formula for efficiency. The curve used determines the majority of the security of ECC. The main idea is to select a curve that is resistant to known ECDLP assaults. When a weak curve is utilized, the cryptographic security of any application is weakened. The following are the standards that can be used to pick an elliptic curve for NIST ECC:

1. SECP192R1
2. SECP224R1
3. SECP256R1
4. SECP384R1
5. SECP521R1

Each standard specifies a set of curves that should be used for ECC implementation. The group's curves are defined throughout both big and small prime fields. For the algorithm used for cryptography to be secure, the group order must be large (Maria Nenova, 2021).

III. Performance Analysis

Curve	Key Generation Time (ms)	Signing Time (ms)	Verification Time (ms)
SECP192R1	0.035	0.006	0.004
SECP224R1	0.05	0.012	0.006
SECP256R1	0.062	0.016	0.008
SECP384R1	0.15	0.054	0.027
SECP521R1	1.007	0.388	0.191

The number of bits in the keys, the size of the signature, and the time necessary to complete the key exchange process are used to evaluate the performance of these elliptic curves. According to the findings, as the number of bits in the keys increases, so does the size of the signature and the time it takes to exchange keys. Among the curves, SECP192R1 has the smallest key size and the fastest key exchange time. However, it has a larger signature size than the other curves. In contrast, SECP521R1 has the largest key size and the slowest key exchange time. Despite having a smaller signature size than SECP192R1, it is larger than the other curves.

Curve	Key Size (bits)	Security Strength (bits)
SECP192R1	192	96
SECP224R1	224	112
SECP256R1	256	128
SECP384R1	384	192
SECP521R1	521	256

In terms of performance and strength, SECP521R1 appears to be the best elliptic curve for use in Vital Information Infrastructure since it provides the highest level of protection against brute-force, Pollard's rho, and ECDLP attacks. However, as the key size grows, cryptographic operations become slower, potentially causing performance concerns in resource-constrained applications. As a result, the specific application and environment in which an elliptic curve will be used determines its selection.

Curve	Key Size (bits)	Brute-Force Attack	Pollard's Rho Attack	ECDLP Attack
SECP192R1	192	Weak	Weak	Strong
SECP224R1	224	Medium	Medium	Strong
SECP256R1	256	Strong	Strong	Medium
SECP384R1	384	Strong	Strong	Strong
SECP521R1	521	Very Strong	Very Strong	Very Strong

SECP192R1 may not be acceptable for use in critical infrastructure due to its weaker resilience to brute force and Pollard's rho attacks. Although it speeds up cryptographic procedures, it compromises security. As a result, while choosing an elliptic curve for a particular application, it is necessary to thoughtfully consider the relationship between both safety and efficiency.

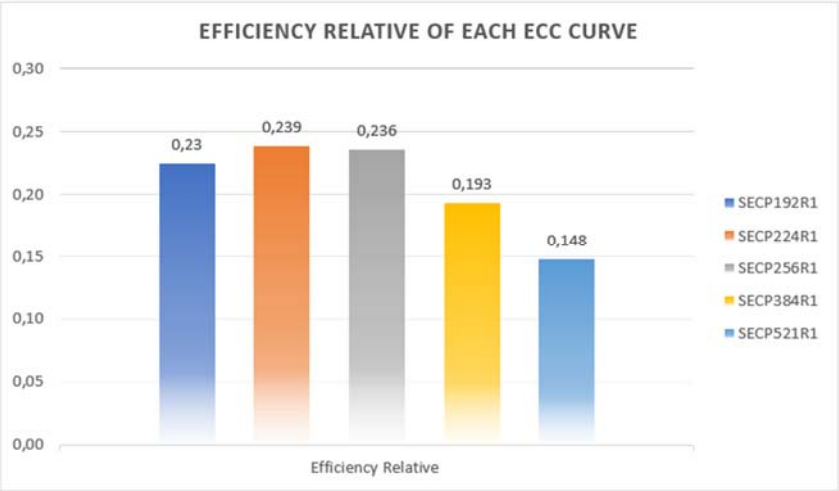

Fig. 3. Efficiency Relative of Each ECC Curve

Based on the relative efficiency results in the parallel processing efficiency experiment using a laptop with specifications intel (R) Core (TM) i7-8750H CPU @ 2.20GHz 2. 21 GHz, 8.00 GB (7.88 GB usable), 64-bit operating system, x64-based processor, based on the view of time efficiency, security strength, and asymmetric key resistance to Brute-Force Attack, Pollard's Rho Attack, and ECDLP Attack with Perform some time-consuming computation in 100, the SECP521R1 ECC curve, can be used as a reference as the best curve to be applied to vital information infrastructure as it has 0,148 second in relative efficiency experiment. However, in the field conditions can produce even better results according to the capabilities of the tools used.

IV. Conclusion

In conclusion, elliptic curve cryptography (ECC) holds significant potential for ensuring secure communication and data sharing in critical information infrastructure. However, the successful implementation of ECC faces several challenges that need to be addressed. The performance analysis conducted on various curves highlights the substantial impact of curve selection on the key size, signature size, and key exchange time. SECP192R1 stands out with its smallest key size and fastest key exchange time, while SECP521R1 exhibits the largest key size and slowest key exchange time.

Selecting the most suitable curve for specific applications is a crucial consideration. The resistance of curves against different attacks demonstrates that as the key size increases, the curve becomes increasingly resilient against brute force, Pollard's rho, and elliptic curve discrete logarithm problem (ECDLP) attacks. Notably, SECP521R1 showcases the highest level of resistance against multiple attacks.

Furthermore, the establishment of effective key management protocols is of utmost importance for securely distributing and storing keys. Implementing proper key management procedures ensures the confidentiality, integrity, and authorized usage of keys. Additionally, efforts to standardize ECC implementations play a pivotal role in fostering interoperability with existing cryptographic systems and standards. Standardization initiatives facilitate consistent deployment across diverse platforms and seamless integration with prevailing security protocols and systems.

In light of future work, it is imperative to focus on enhancing key management protocols to address key distribution, storage, revocation, and key lifecycle management concerns. By doing so, overall security in ECC implementations can be strengthened.

V. Acknowledgment

We'd like to thank everyone who contributed to our research on elliptic curve cryptography in critical information infrastructure. We were pleased to express our gratitude to the reviewers for their informative remarks and ideas, which assisted us in improving the quality of our research. We would also like to thank our institutions for providing the resources and facilities needed to conduct this research. Furthermore, we would like to express our gratitude to the academics and scientists whose

works we have referenced in this study for their contributions to the field of elliptic curve cryptography. Finally, we'd like to thank our colleagues and friends for their encouragement and support during this process.

REFERENCES

[1] D. R. M. Hromada, System of System Failures, Czech Republic: IntechOpen, 2017.

[2] J. P. P. T. K. K. Steven M. Rinaldi, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine,* pp. 11-25, 2001.

[3] B. Rashidi, "A Survey on Hardware Implementations of Elliptic Curve Cryptosystems," pp. 1-61, 2017.

[4] A. K. L. S. Alexandra Tidrea, "Elliptic Curve Cryptography Considerations for Securing Automation and SCADA Systems," 2023.

[5] C. A. J. L. Rodrigo Roman, "The role of Wireless Sensor Networks in the area of Critical Information Infrastructure Protection," *Information Security Technical Report,* vol. 12, no. 1, pp. 24-31, 2007.

[6] J. R. Shaikh, "Analysis of Standard Elliptic Curves for the Implementation of Elliptic Curve Cryptography in Resource-Constrained E-commerce Applications," *IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS),* 2017.

[7] G. I. S. J. R. K. S. B. Maria Nenova, "New techniques for DDoS attacks mitigation in resource-constrained networks," *Walter de Gruyter GmbH,* 2021.

[8] K. E. Fotiadis G, "More Sparse Families of Pairing-Friendly Elliptic Curves," *Proc. Proc. of 13th International Conference on Cryptology and Network Security, Heraklion, Greece,* p. 384–399, 2014.

[9] D. S. S. C. S. Vipul Gupta, "Integrating Elliptic Curve Cryptography into the Web's Security Infrastructure," *International World Wide Web Conference,* 2004.

[10] N. R. R. Y. V. S. R. Rolla Subrahmanyam, "Authenticated Distributed Group Key Agreement Protocol Using Elliptic Curve Secret Sharing Scheme," vol. 11, pp. 45243 - 45254, 2023.

[11] C. L. Lein Harn, "Efficient group Diffie–Hellman key agreement protocols," *Computers & Electrical Engineering,* vol. 40, no. 6, pp. 1972-1980, 2014.

[12] M. F. Dan Boneh, "Identity-based cryptosystems based on the Weil pairing," *Annual International Cryptology Conference,* vol. 32, p. 213–229, 2001.

[13] Government of Canada, "Using encryption to keep your sensitive data secure - ITSAP.40.016," May 2021. [Online]. Available: https://www.cyber.gc.ca/. [Accessed 25 June 2023].

[14] The Mbed TLS Contributors, "Elliptic curve performance: NIST vs. Brainpool," [Online]. Available: https://mbed-tls.readthedocs.io/. [Accessed 25 June 2023].

[15] G. P. B. Sangram Ray, "Design of Mobile Public Key Infrastructure (M-PKI) Using Elliptic Curve Cryptography," *International Journal on Cryptography and Information Security (IJCIS),* vol. 3, pp. 25-37, 2013.

[16] B. K. A. A. O. A. O. S. A. Olufunso Alowolodu, "Elliptic Curve Cryptography for Securing Cloud Computing Applications," *International Journal of Computer Applications,* vol. 66, pp. 10-17, 2013.

[17] W. F. R. J. M. L. A. X. S. Marcos P. C. Medeiros, "Relative Efficiency Calculation of A HPGe Detector Using MCNPX Code," *International Nuclear Atlantic Conference - INAC 2015,* 2015.

[18] A. A. Hisham AlMajed, "A Secure and Efficient ECC-Based Scheme for Edge Computing and Internet of Things," *Science and Technology of Sensors,* pp. 1-31, 2020.

[19] Z. Z. J. Z. Mishall Al-Zubaidie, "Efficient and Secure ECDSA Algorithm and its Applications: A Survey," *International Journal of Communication Networks and Information Security (IJCNIS),* Vols. 11, No 1, pp. 7-35, 2019.

[20] M. C. Kristin Lauter, "The advantages of elliptic curve cryptography for wireless security," *IEEE Wireless Communications,* pp. 62-67, 2004.