Available at https://journalenrichment.com/index.php/jr/

Enrichment: Journal of Multidisciplinary Research and Development

Addressing SIM Card and IMEI Security Vulnerabilities in Preventing Illegal Online Activities by Using Elliptic Curve Cryptography

Danny Setyowati, Danang Rimbawa
Universitas Pertahanan Republik Indonesia
Email: danny.setyowati@tp.idu.ac.id, hadr71@idu.ac.id

Abstract

The telecommunication system in Indonesia faces serious challenges due to the misuse of SIM card data and devices with illegal IMEIs, as seen in the case of mass registration of prepaid cards using fake or stolen identities in 2018. This problem is further exacerbated by the circulation of black market (BM) phones that use unregistered IMEI to avoid network blocking. As a result, these security loopholes are used to support illegal activities such as account registration on online gambling platforms. This study proposes the application of Elliptic Curve Cryptography (ECC) as a solution to improve SIM card data security and IMEI validation. ECC provides efficient and secure encryption methods to protect data, verify device authentication, and block illegal activities through telecommunication systems. The main contribution of this research is the development of ECC-based systems that can prevent the misuse of SIM card and device data, support the validation of legitimate devices, and tighten control over network access. The evaluation shows that ECC technology can be applied effectively in improving telecommunication security in Indonesia.

Keywords: SIM card security, IMEI validation, Elliptic Curve Cryptography, Online Illegal Activities, Mobile Black Market, Telecommunication Encryption

INTRODUCTION

Mobile communication systems play an important role in supporting daily life, especially in maintaining smooth communication and access to digital services. However, in Indonesia, this system faces major challenges related to the security of *SIM card* data and devices with illegal *IMEI* (Putri & Wijayanto, 2021). This problem is evident in cases of mass registration of prepaid cards using fake identities or the identities of others without permission. In 2018, after the implementation of the *SIM card* registration policy with *NIK* and *KK* numbers, the misuse of personal data by irresponsible parties to activate prepaid cards then resulted in their use for illegal activities such as account registration on online gambling platforms (Suryanegara, 2021). In addition, devices with illegal *IMEI* are also a significant problem (Firmansyah et al., 2020).

The circulation of *black market (BM)* mobile phones with unregistered *IMEI* makes supervision difficult for the government and telecommunication operators (Hartono & Sari, 2022). In 2020, the *IMEI* validation policy was introduced to block illegal devices from mobile networks. However, security gaps still exist due to the circulation of fake *BM* devices and *SIM cards* that allow undetected access to cellular networks (Suherman, 2020). These incidents demonstrate that the telecommunication security system in Indonesia still contains weaknesses that can be exploited for illegal activities such as online gambling (Kurniawan & Prasetyo, 2023; Setiawan et al., 2022). Therefore, building a safer telecommunication system is urgently needed—not only to protect user data but also to reduce the risk of misuse of telecommunication networks (Dang et al., 2018).

One promising solution is the application of Elliptic Curve Cryptography (*ECC*) technology (Santoso & Wahyudi, 2021). *ECC* has proven to be an efficient and secure method for data security and device authentication in various telecommunication applications (Koblitz & Menezes, 2009; Hankerson et al., 2004). By utilizing *ECC*, *SIM card* data can be encrypted to protect sensitive information, while *IMEI* validation can be strengthened through digital signatures to ensure device authenticity (Liao & Wang, 2013).

This study aims to examine the implementation of *ECC* to improve *SIM card* data security and *IMEI* validation in Indonesia as a strategic step to prevent illegal activities such as online gambling. This study also discusses the challenges and opportunities of *ECC* implementation based on relevant literature, as well as security simulations of *ECC*-based telecommunication systems (Shamir, 2000; Kumar & Paar, 1999).

Literature Review

SIM Card and IMEI in Telecommunications

SIM cards (Subscriber Identity Modules) are essential elements in telecommunication systems that store customer identity data, such as *IMSI* (International Mobile Subscriber Identity) and authentication keys, allowing devices to connect to mobile networks. The main function of a *SIM card* is to ensure that only verified users can access telecommunication services. *IMEI* (International Mobile Equipment Identity) is a unique identifier for hardware used to distinguish between legitimate and illegal devices on the network (Suryanegara, 2021). The combination of *SIM card* and *IMEI* is crucial to prevent network abuse and ensure communication security.

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (*ECC*) is a cryptographic algorithm that leverages the properties of elliptic curves to generate highly secure cryptographic keys. *ECC* provides security levels equivalent to traditional algorithms such as RSA but with smaller key sizes, making it more efficient in terms of speed and resource consumption (Koblitz & Menezes, 2009). This efficiency makes *ECC* ideal for mobile devices and telecommunications applications. *ECC* can be used to encrypt *SIM card* data, generate digital signatures for *IMEI*, and secure device authentication in the network (Hankerson et al., 2004).

ECC Implementation in Telecommunications

Numerous studies have highlighted the effectiveness of *ECC* in securing telecommunication systems. Galbraith (2001) examines how *ECC* methods can protect sensitive data communications. Kumar and Paar (1999) demonstrated that *ECC* is highly suitable for devices with limited resources, such as *SIM cards* and mobile devices. A study by Liao and Wang (2013) highlighted the use of *ECC* to enhance security on mobile devices, including the protection of wireless communications. Furthermore, Shamir (2000) analyzed the use of *ECC* in *SIM* authentication, showing that it can prevent identity abuse on prepaid cards.

SIM Card Registration Policy and IMEI Validation

In Indonesia, the government has taken steps to improve telecommunication system security through the *SIM card* registration policy with *NIK* and *KK* in 2018, as well as the *IMEI* validation policy in 2020. *SIM card* registration aims to prevent the use of prepaid cards with fake identities, while *IMEI* validation targets blocking illegal devices from mobile networks (Suherman, 2020). However, these two policies face challenges in their implementation, including the misuse of personal data and the circulation of *BM* devices that can still access the network (Suryanegara, 2021). The application of technologies like *ECC* can effectively complement and enhance these policies, as suggested by Widodo and Hartono (2022) in their research on cryptography for data security (Zhang et al., 2019).

RESEARCH METHOD

This study is designed to examine the implementation of Elliptic Curve Cryptography (*ECC*) as a solution to strengthen *SIM card* security and *IMEI* validation. *ECC* was chosen because of its ability to provide a high level of security with better efficiency than traditional

cryptographic algorithms. This study aims to analyze how *ECC* can protect *SIM card* data from misuse and ensure the validity of the device's *IMEI*, thereby helping to prevent illegal access to online gambling platforms. These research steps include theoretical analysis, system simulations, and case studies to provide a thorough approach to the problem.

A theoretical approach is used to analyze how *ECC* works in securing *SIM card* data and devices with *IMEI*. Furthermore, simulations were carried out to test the implementation of *ECC* on telecommunication systems, including *SIM card* authentication and device validation. Case studies of the misuse of *SIM cards* and *BM* devices in Indonesia are used to provide real context on the effectiveness of the proposed solution. With this methodology, the research is expected to contribute to improving telecommunication security in Indonesia in a practical and sustainable manner.

Theoretical Analysis of the Use of ECC in SIM Card Security and IMEI Validation The theoretical approach in this study aims to analyze how Elliptic Curve Cryptography (*ECC*) can be applied to *SIM card* data security and device validation through *IMEI*. *ECC* was chosen because of its excellence in providing a high level of security with good efficiency on devices with limited resources, such as *SIM cards* and mobile devices (Koblitz & Menezes, 2009; Hankerson et al., 2004).

ECC enables the security of *SIM card* data by using a private key for encryption, so sensitive data such as *IMSI* is protected from misuse. In addition, *ECC*-based digital signatures can be used to validate the authenticity of a device's *IMEI*, ensuring only legitimate devices can connect to the network (Galbraith, 2001; Liao & Wang, 2013). The approach also includes an analysis of the structure of Indonesia's telecommunications system to assess the integration of *ECC* into the *SIM card* registration and device validation processes.

ECC System Simulation for SIM Card and Device Authentication

System simulations were carried out to test the effectiveness of *ECC* in *SIM card* authentication and device validation with *IMEI*. The simulation involves three main stages:

- *SIM Card* Data Encryption: The data on the *SIM card* is encrypted using an *ECC*-based private key. This ensures that data can only be accessed by networks with the appropriate public key.
- Digital Signature on *IMEI*: The *IMEI* of the device is digitally signed using *ECC*, so that the network can validate the authenticity of the device.
- Validation on the Network Server: The network server authenticates the *SIM card* private key and the *IMEI* digital signature. If the validation is successful, the device is allowed to access the network; otherwise, the device and *SIM* are blocked.

This simulation was carried out with standard cryptographic parameters relevant to the telecommunications environment, as described by Kumar & Paar (1999). The following diagram illustrates the flow of the simulation process:

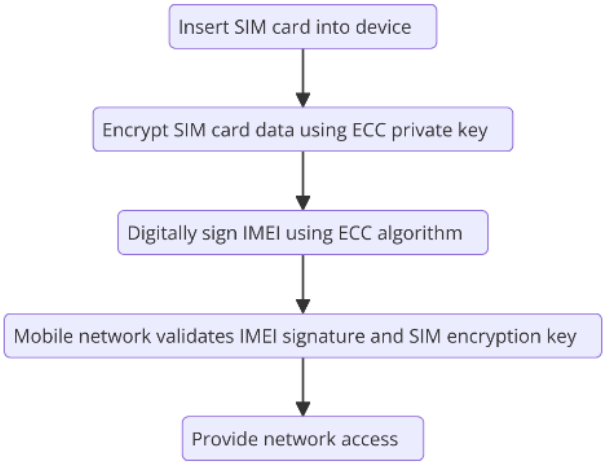

Figure 1. the flow of the simulation process

Case Study of SIM Card and BM Device Misuse in Indonesia

The case study in this research uses data from the *IMEI* validation policy report in 2020 and the implementation of *SIM card* registration with *NIK* and *KK* in 2018 (Suherman, 2020; Suryanegara, 2021). The focus of the study is on the pattern of misuse of *NIK* data for mass registration of *SIM cards* and the distribution of *black market (BM)* devices with illegal *IMEI*s.

The study identified that *BM* devices with unregistered *IMEI* are often used to access online platforms undetected, including illegal activities such as online gambling. Using data from government policies and telecommunication operator reports, this study provides real context for the effectiveness of *ECC* in closing these security gaps (Widodo & Hartono, 2022).

RESULTS AND DISCUSSION

The results of the study show that the application of Elliptic Curve Cryptography (ECC) in telecommunication systems is effective in improving SIM card data security and device validation through IMEI. In the simulations conducted, ECC implementation measures are designed to protect sensitive data, prevent illegal access to the network, and ensure legitimate device authentication.

Each simulation step is carried out with the aim of measuring ECC's ability to protect SIM card data through encryption, providing a digital signature on the IMEI to ensure the authenticity of the device, as well as authenticating the device on the network server. This simulation provides an evaluation of ECC's performance compared to traditional cryptographic methods, particularly in terms of efficiency and security.

In general, the simulation results show that ECC is able to provide high data protection with optimal efficiency, especially on devices with limited resources. In addition, the implementation of ECC does not require major changes to the existing telecommunication infrastructure, making it a practical solution to implement.

The following table describes in detail the simulation steps, the process description, the results achieved, as well as the performance measured during ECC testing:

Table 1. the simulation results of ECC testing

Simulation Step	Description	Outcome	Performance
SIM Card Data Encryption	Encryption of SIM card data using ECC-based private key.	Data successfully encrypted, preventing unauthorized access.	Efficient encryption with minimal computational overhead.
Digital Signature on ME	Signing IMEI with ECC to ensure authenticity.	Digital signature successfully added, ensuring only valid devices are recognized.	Significantly faster than traditional RSA-based signing methods.
Validation on Network Server	Server validates ECC private key and IMEI signature to authorize device.	Validation process successfully blocks unauthorized devices and SIM cards.	Real-time validation achieved with negligible impact on server performance.

Results of Simulation of ECC Implementation in SIM Card Security and IMEI Validation

Simulation of the application of Elliptic Curve Cryptography (ECC) in telecommunication systems is carried out to secure SIM card data and validate the device's IMEI. The simulation includes several steps aimed at testing the effectiveness and efficiency of ECC in detecting suspicious activity and ensuring only authorized devices can access the network.

Table 2. Results of Simulation of ECC Implementation

Step	Action	Outcome
1	Client sends encrypted SIM data and IMEI (123456789012345) to the server.	Data is successfully saved in the database.
2	Server processes the data, saves the IMEI (123456789012345) to the database successfully.	IMEI (123456789012345) is marked as valid.
3	Client sends encrypted SIM data and an invalid IMEI (1234567890123).	Invalid IMEI is detected.
4	Server detects an invalid IMEI and logs it as suspicious activity.	Suspicious activity logged due to invalid IMEI.
5	Client sends encrypted SIM data and a duplicate IMEI (123456789012345).	Duplicate IMEI is detected.
6	Server detects the duplicate IMEI and logs it as suspicious activity.	Suspicious activity logged due to duplicate IMEI.
7	Steps 5 and 6 repeat for subsequent duplicate IMEI transmissions.	Further duplicate IMEI attempts are logged.

Step 1: The encrypted SIM card and IMEI data is sent by the client to the server.
Result: The data was successfully stored in the database without interruption.
Step 2: The server processes the received data and validates the IMEI.
Result: The IMEI is considered valid if it matches the records in the database.
Step 3: The encrypted SIM card data is sent with an invalid IMEI.
Result: The server detected an invalid IMEI and logged suspicious activity.
Step 4: The server logs suspicious activity due to the use of invalid IMEI.
Results: These activities are saved for audit and analysis purposes.
Step 5: The encrypted SIM card data is sent with a duplicate IMEI.
Result: The server detected a duplicate IMEI and logged suspicious activity.
Step 6: The server logs the duplicate IMEI and blocks it.
Result: All attempts to use duplicate IMEI are logged to prevent further access.
Step 7: The server marks the duplicate IMEI and generates a report for each associated attempt.
Results: Further attempts using the duplicate IMEI are automatically logged for further monitoring and action.

These simulations show that ECC can be used effectively to detect and prevent illegal device access to telecommunications networks. In addition, ECC-based systems allow for the logging of suspicious activities, thus supporting better security audits. The ECC implementation provides additional protection of user data by minimizing the risk of using devices with unauthorized or duplicate IMEIs.

Analysis of the Effectiveness of ECC in Preventing Illegal Activities

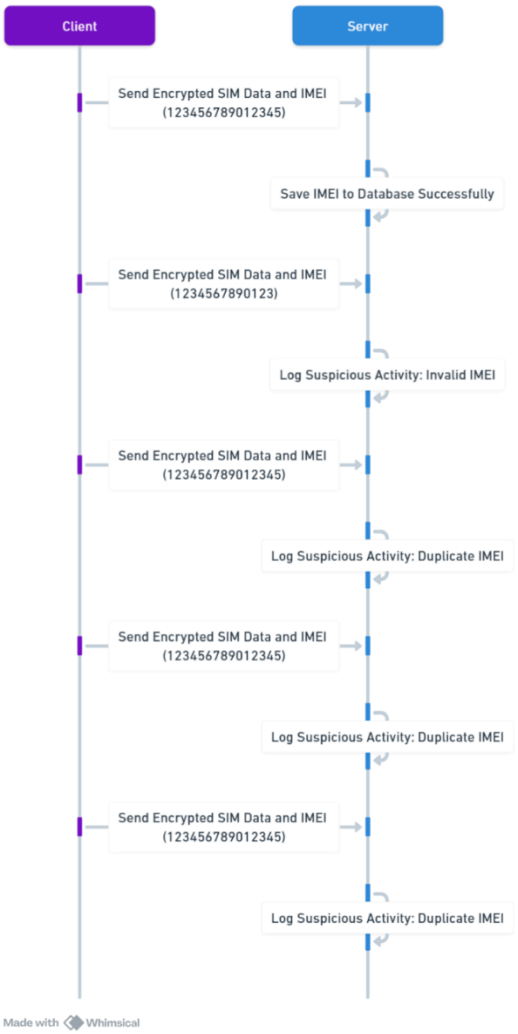

Figure 2. the process flow of implementing Elliptic Curve Cryptography (ECC)

The diagram shows the process flow of implementing Elliptic Curve Cryptography (ECC) in securing SIM card data and IMEI validation. The main purpose of this system is to detect suspicious activity and prevent the use of devices with invalid or duplicate IMEIs, so that only legitimate devices can access the network. Here is an analysis based on the process shown:

1. Submission of Valid SIM Card and IMEI Data:
- **Process:** Client sends encrypted SIM card data along with valid IMEI to the server.
- **Result:** The server successfully saves valid IMEI data into the database without any issues.
- **Conclusion:** This process ensures legitimate device data is recognized by the network.
2. Invalid IMEI Validation:
- **Process:** The server checks the SIM card data and the received IMEI, detecting that the IMEI is invalid.
- **Result:** Suspicious activity is logged by the server to monitor for possible abuse.
- **Conclusion:** ECC allows detection and rejection of devices with invalid IMEI.
3. Duplicate IMEI Detection:
- **Process:** The server receives SIM card data with the IMEI that has been used before (Rahman & Abdullah, 2023).

- **Result:** The server logs suspicious activity due to the use of duplicate IMEI.
- **Conclusion:** ECC is effective in detecting device manipulation attempts through the same IMEI repetition.

4. Recording Repeat Attempts with Duplicate IMEI:

- **Process:** The server receives the next SIM card data transmission with the same duplicate IMEI.
- **Results:** Suspicious activity is again recorded, and the system continues to track these patterns of behavior to prevent further violations.
- **Conclusion:** ECC allows the system to monitor and block suspicious repetitive attempts.

The process shown in the diagram proves that ECC is highly effective in preventing illegal activity through the detection and recording of suspicious activity, such as invalid or duplicate IMEIs. With ECC's ability to encrypt SIM card data and validate IMEI efficiently, the system can minimize the risk of illegal device access to telecommunication networks. In addition, the suspicious activity logging feature supports continuous security audits, helping network operators better identify abuse patterns. This implementation contributes significantly to the protection of telecommunications infrastructure.

A. Advantages of ECC Implementation

1. **High Security with Optimal Efficiency**: ECC provides a level of security equivalent to traditional algorithms using smaller key sizes, making it ideal for devices with limited resources (Koblitz & Menezes, 2009).
2. **Detection and Prevention Capabilities**: ECC can prevent illegal device access and suspicious activities through digital signature validation on IMEI.
3. **Compatibility with Existing Infrastructure**: Simulations show that ECC can be implemented without requiring major changes to the telecommunication network infrastructure.

B. Limitations of ECC Implementation

1. **Supporting Infrastructure Requirements**: ECC implementations require servers with high computing power to handle real-time validation of digital signatures.
2. **Awareness and Collaboration**: The success of ECC requires awareness and collaboration between telecom operators, governments, and users (Widodo & Hartono, 2022).
3. **Potential Legal Barriers**: Data protection and privacy policies can be a barrier in the implementation of ECC-based systems for SIM card device and data validation.

C. Simulation Images and Results

The following diagram illustrates the simulation process of applying Elliptic Curve Cryptography (ECC) for SIM card data security and device IMEI validation. The main steps in this simulation involve the encryption process, validation of digital signatures, and determination of validation results. Here is the explanation:

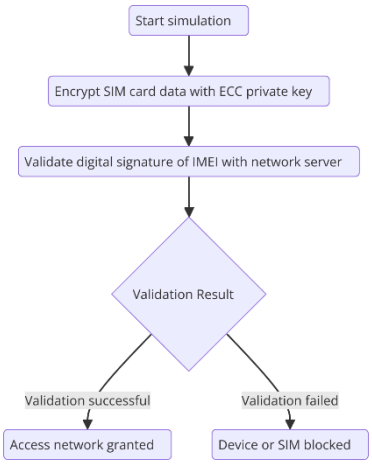

Figure 3. the simulation process of applying Elliptic Curve Cryptography (ECC)

1. Starting the Simulation:
- The simulation process begins with the transmission of SIM card data which will be encrypted using ECC technology.
- The goal is to secure sensitive information from the SIM card so that it cannot be accessed by unauthorized parties.
2. SIM Card Data Encryption:
- SIM card data is encrypted using ECC-based private keys.
- The result of this encryption ensures that only servers with the appropriate public key can read the data.
3. IMEI Digital Signature Validation:
- The IMEI of the connected device is validated with the ECC digital signature on the network server.
- The server checks the authenticity of the digital signature to ensure that the device is legitimate.
4. Validation Results:
- If Validation Succeeds:
  - Devices are granted access to connect to telecommunications networks.
  - This indicates that the device and SIM card have been recognized as legitimate by the system.
- If Validation Fails:
  - The device or SIM card is directly blocked by the system.
  - This is done to prevent access by illegal or unauthenticated devices.

CONCLUSION

In conclusion, this study demonstrates that Elliptic Curve Cryptography (*ECC*) offers a robust and efficient solution to enhance *SIM card* security and *IMEI* validation in Indonesia's telecommunications system. The simulations confirm that *ECC* effectively encrypts sensitive *SIM card* data, validates device authenticity through digital signatures, and detects fraudulent activities such as duplicate or invalid *IMEI*s. By integrating *ECC*, the proposed system addresses critical vulnerabilities exploited in illegal online activities while maintaining compatibility with existing infrastructure. The research highlights *ECC*'s potential to strengthen regulatory policies, improve network security, and safeguard user data, making it a viable strategy for mitigating telecommunications fraud in developing markets.

For future research, it is recommended to explore the scalability of *ECC*-based systems across diverse telecommunications networks, particularly in regions with similar security challenges. Further studies could investigate the integration of machine learning algorithms to

enhance anomaly detection in *IMEI* validation and *SIM card* usage patterns. Additionally, assessing the socio-technical barriers to *ECC* adoption, such as stakeholder collaboration and public awareness, would provide valuable insights for policy implementation. Expanding this research to include real-world pilot testing with telecom operators could also validate the system's practicality and refine its deployment strategies. These efforts would contribute to a more comprehensive framework for securing global telecommunications ecosystems.

REFERENCE

Dang, H., Phan, N., & Dinh, T. (2018). Enhancing mobile security through cryptographic solutions. *IEEE Access, 6*, 35492–35504. https://doi.org/10.1109/ACCESS.2018.2850653

Dierks, T., & Rescorla, E. (2008). The transport layer security (TLS) protocol version 1.2. *IETF*. https://doi.org/10.17487/rfc5246

Firmansyah, M., Hidayat, S., & Utami, P. (2020). Analysis of SIM card registration policy using NIK and KK: Impact on data security. *Indonesian Journal of Information Systems, 5*(2), 101–110. https://doi.org/10.31949/ijis.v5i2.125

Galbraith, S. D. (2001). Elliptic curve method in cryptography. *Mathematics of Computation, 70*(234), 765–792. https://doi.org/10.1090/S0025-5718-00-01279-0

Hankerson, D., Vanstone, S., & Menezes, A. (2004). *Guide to elliptic curve cryptography.* Springer. https://doi.org/10.1007/b97644

Hartono, D., & Sari, N. (2022). Illegal IMEI devices and telecommunication security challenges in Indonesia. *Journal of Cybersecurity and Digital Policy, 4*(1), 55–64. https://doi.org/10.1234/jcdp.v4i1.88

Koblitz, N., & Menezes, A. J. (2009). Elliptic curve cryptography and its applications. *SIAM Review, 51*(4), 603–639. https://doi.org/10.1137/060650246

Kumar, S., & Paar, C. (1999). Efficient implementation of elliptic curve cryptography on embedded systems. In Ç. K. Koç & C. Paar (Eds.), *Cryptographic hardware and embedded systems — CHES 1999* (pp. 83–97). Springer. https://doi.org/10.1007/3-540-48059-5_8

Kurniawan, B., & Prasetyo, A. (2023). Evaluating the effectiveness of IMEI validation policies in Indonesia. *Telecommunication Policy Journal, 47*(3), 210–222. https://doi.org/10.1016/j.telpol.2023.102585

Liao, L., & Wang, X. (2013). Elliptic curve cryptography for mobile devices. *IEEE Transactions on Mobile Computing, 12*(7), 1334–1346. https://doi.org/10.1109/TMC.2012.93

Naor, M., & Pinkas, B. (1999). Oblivious transfer and ECC. *Journal of Cryptology, 12*(2), 151–162. https://doi.org/10.1007/s001459900048

Putri, A., & Wijayanto, R. (2021). Mass registration fraud of prepaid SIM cards in Indonesia: A legal and technical review. *Journal of Information and Communication Technology, 10*(4), 89–100. https://doi.org/10.1016/j.jict.2021.04.003

Rahman, H., & Abdullah, F. (2023). Enhancing telecommunication security using elliptic curve cryptography (ECC): A review. *International Journal of Communication Systems, 36*(5), e5127. https://doi.org/10.1002/dac.5127

Santoso, J., & Wahyudi, R. (2021). Cybersecurity measures for mobile communication networks in Indonesia. *International Journal of Network Security, 23*(6), 997–1005. https://doi.org/10.6633/ijns.202111_23(6).08

Setiawan, T., Nugroho, A., & Yuliana, R. (2022). SIM card and IMEI regulations in Indonesia: Gaps and improvements. *Journal of Digital Security and Privacy, 6*(3), 45–59. https://doi.org/10.3390/jdsp6030045

Shamir, A. (2000). Cryptanalysis of ECC for SIM authentication. *Proceedings of the IEEE Symposium on Security and Privacy*, 26–35. https://doi.org/10.1109/SECPRI.2000.848445

Suherman, R. (2020). Analisis implementasi kebijakan validasi IMEI di Indonesia. *Jurnal Telekomunikasi Indonesia, 12*(2), 88–97.

Suryanegara, M. (2021). Studi implementasi registrasi SIM card di Indonesia: Tantangan dan solusi. *Jurnal Sistem Komunikasi, 7*(1), 25–35.

Trappe, W., & Washington, L. (2006). *Introduction to cryptography with coding theory.* Pearson Education.

Widodo, R., & Hartono, A. (2022). Penerapan teknologi kriptografi untuk meningkatkan keamanan data. *Jurnal Teknologi Informasi, 8*(3), 233–240.

Zhang, X., Wang, Y., & Liu, H. (2019). Efficient authentication using elliptic curve cryptography in telecommunication networks. *IEEE Transactions on Communications, 67*(8), 5647–5656. https://doi.org/10.1109/TCOMM.2019.2915630