Optimization of Security Identification in Power Grid Data through Advanced Encryption Standard Algorithm

Biaoqi Li*, Min Xu, Yuan Zhou, Haibin Liu and Renlong Zhang

Yunnan Power Grid Co., Ltd, Kunming Enersun Technology Co., Ltd. Kunming 650000, Yunnan, China
E-mail: 18208891009@163.com
**Corresponding Author*

Received 27 September 2023; Accepted 08 November 2023;
Publication 13 February 2024

Abstract

With the increasing reliance on digital technologies in power grid systems, ensuring the security and confidentiality of data has become paramount. This study focuses on optimizing security identification processes in power grid data using the Advanced Encryption Standard (AES) algorithm. The research explores the application of AES to enhance data protection and improve the accuracy and efficiency of security identification techniques. By implementing AES encryption, the study aims to fortify the security measures within the power grid infrastructure, safeguard sensitive information, and mitigate potential threats. The findings provide insights into the benefits of AES-based security optimization, contributing to the advancement of data security in power grid operations.

Keywords: Power grid, security identification, advanced encryption standard (AES).

Journal of Cyber Security and Mobility, Vol. 13_2, 239–264.
doi: 10.13052/jcsm2245-1439.1323

1 Introduction

The modern power grid has undergone a significant transformation, becoming increasingly reliant on digital technologies and data-driven systems to enhance efficiency, reliability, and sustainability. While these technological advancements have undoubtedly revolutionized the energy sector, they have also exposed the power grid to new and evolving security challenges. Protecting the integrity, confidentiality, and availability of critical data within the power grid is imperative to ensure uninterrupted electricity supply, prevent unauthorized access, and safeguard against potential threats.

In this context, this study delves into the pivotal realm of data security within power grid systems, with a specific focus on optimizing security identification processes. The Advanced Encryption Standard (AES) algorithm, renowned for its robust cryptographic properties, emerges as a key element in this endeavor. By harnessing the power of AES encryption, we aim to fortify the security measures within the power grid infrastructure and enhance the protection of sensitive data.

The significance of this research lies in its potential to advance the field of power grid data security by offering a novel approach to security identification optimization. As digitalization continues to shape the energy sector, our findings hold the promise of bolstering the resilience of power grid systems and mitigating potential threats.

This paper explores the theoretical foundations, practical applications, and potential benefits of implementing AES encryption to optimize security identification within power grid data. Through a comprehensive examination of the topic, we seek to contribute to the ongoing efforts to secure the critical infrastructure upon which modern society depends.

2 Related Works

The reviewed literature comprises a diverse range of research efforts related to the Advanced Encryption Standard (AES) and its applications. Sarita Sanap and Vijayshree More proposed an ultra-high throughput and efficient implementation of the Advanced Encryption Standard (AES) on field programmable gate arrays [1]. Alslman Yasmeen et al. introduced a hybrid encryption scheme for medical imaging by combining AutoEncoder and AES [2]. Sabreen Ali Hussein et al. evaluated image encryption algorithms, including the Fibonacci Q-matrix in hyperchaotic, Secure Internet of Things (SIT), and AES techniques [3]. Li ZhenQiang et al. presented a novel quantum circuit implementation of AES, optimizing it in terms of qubit count and T-depth [4]. Wang Zeguo, Wei Shijie, Long Gui Lu, and Hanzo Lajos introduced a variational quantum attack algorithm (VQAA) targeting AES-like symmetric cryptography [5]. Renugadevi N. et al. survey methods to enhance Advanced Encryption Standard hardware accelerators on Field Programmable Gate Arrays [6]. Lee JongHyeok and Kim Jiyoon present a novel shuffling countermeasure for AES against profiled attacks in mobile multimedia services [7]. Nahom Gebeyehu Zinabu and Samuel Asferaw propose an Enhanced Efficiency of Advanced Encryption Standard (EE-AES) algorithm [8]. Nahom Gebeyehu Zinabu and Samuel Asferaw introduce an Enhanced Security of Advanced Encryption Standard algorithm [9]. Liu Guangzhe et al. propose an image encryption scheme based on a discrete-time alternating quantum walk and AES [10]. Raju Deril, Eleswarapu Lalitha, Pranav Muppidi Sai, and Sinha Rupesh Kumar propose a multi-level image security scheme combining elliptic curves, magic matrix, and AES [11]. Niraj Kumar, Vishnu Mohan Mishra, and Adesh Kumar address smart grid security with an S-box AES implementation [12]. Nabilah Abughazalah, Majid Khan, Noor Munir, Ammar S. Alanazi, and Iqtadar Hussain present a generalized AES in a Galois field with any characteristic p. This innovative approach adjusts all AES steps for the new enhancement, offering increased keyspace, robustness, and additional confusion abilities [13]. T. Manoj Kumar and P. Karthigaikumar propose an efficient pipelined architecture for AES key expansion, reducing propagation delay and increasing throughput [14]. Lasseni Coulibaly, Fethi Ouallouche, and Vitalice Oduol introduce a joint cryptography and channel-coding method based on LDPC codes and AES for 5G systems [15]. Padmavathi R. Anusha and Dhanalakshmi K. S. propose an efficient AES encryption and decryption architecture called AESIM for memory security [16]. Hafsa Amal, Fradi Marwa, Sghaier Anissa, Malek Jihene, and Machhout Mohsen introduce IAES, an improved AES algorithm suitable for real-time video security. IAES eliminates shift-row and sub-byte transformations, replacing them with a mix-row operation, reducing runtime and enhancing randomness [17]. Ahmad Nabihah and Hasan S.M. Rezaul present a compact ASIC implementation of AES crypto-hardware accelerator [18]. Cañadas Agustín Moreno, Gaviria Isaías David Marín, and Vega Juan David Camacho explore the relationships between the Chicken

McNugget problem, mutations of Brauer configuration algebras, and the AES [19]. Assafli, Hayder T., Hashim, Ivan A., and Naser, Ahmed A. analyze AES acceleration using GPUs [20].

Efficiency in AES Implementation: Several papers focus on optimizing AES implementations for different purposes, such as hardware acceleration, quantum circuits, and memory security. These contributions demonstrate the ongoing interest in improving the efficiency and performance of AES in various contexts. AES in Security: AES remains a fundamental component in security applications. Some studies investigate AES within the broader context of securing sensitive data, including medical imaging, image encryption, and smart grids. These works aim to enhance the security of data through innovative AES-based approaches or by integrating AES with other cryptographic techniques. Quantum Computing: Quantum computing's impact on AES is a notable theme. Researchers are exploring quantum circuit implementations, quantum attacks, and countermeasures against quantum threats to AES, reflecting the need to adapt encryption methods to evolving technologies. Novel Approaches: Some papers introduce novel approaches to enhance AES or address specific challenges. These approaches include variations of AES, integration with chaotic maps, and exploring AES in specialized fields like multimedia and Galois fields. Security Challenges: Papers like address security challenges and countermeasures, considering profiled attacks, quantum threats, and unique encryption scenarios, which are crucial for staying ahead of evolving cybersecurity risks. Efficient Hardware Design: Efforts to optimize AES hardware design showcase the importance of AES in resource-constrained environments, such as field programmable gate arrays (FPGAs), memory systems, and cryptographic accelerators. In summary, these studies collectively contribute to the ongoing development, adaptation, and practical application of AES in various domains. They address issues of efficiency, security, and adaptability to emerging technologies, highlighting the continued relevance and importance of AES in contemporary cryptography and cybersecurity research.

3 AES Power Grid Data Security Identification

3.1 Data Encryption and Decryption Process

The core of the AES algorithm lies in the processes of data encryption and decryption, encompassing four primary operations: SubBytes, ShiftRows, MixColumns, and KeyExpansion.

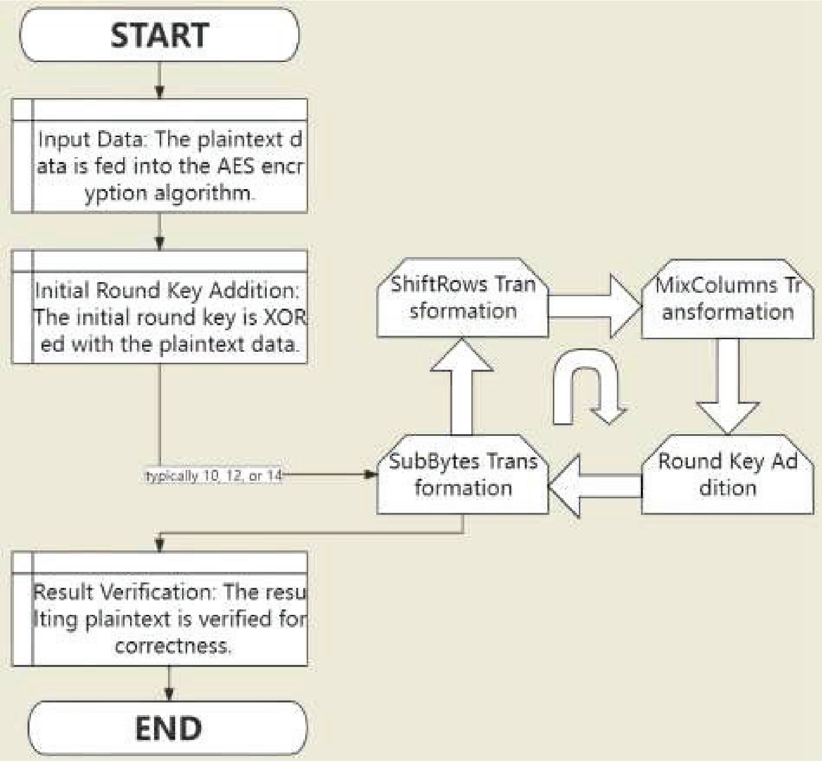
START
Input Data: The plaintext data is fed into the AES encryption algorithm.
Initial Round Key Addition: The initial round key is XORed with the plaintext data.
typically 10, 12, or 14
SubBytes Transformation
ShiftRows Transformation
MixColumns Transformation
Round Key Addition
Result Verification: The resulting plaintext is verified for correctness.
END

Figure 1 Data encryption process.

SubBytes Transformation:

The SubBytes transformation in AES is a byte substitution step that utilizes an S-box for byte substitution. The formula is expressed as:

$\mathrm{S(x, y) = A(x, y)^{-1} + b(x, y)(mod\ m)}$ $\mathrm{A(x, y)}$ represents the affine transformation matrix.
$\mathrm{b(x, y)}$ is a constant vector.
m denotes the field size.

ShiftRows Transformation:

The ShiftRows transformation entails cyclically shifting the rows of the state matrix, mathematically represented as:

$$\mathrm{State[i][j] = State[i][j+i]}$$
$$\mathrm{(for\ 0 <= i < 4)}$$

$\mathrm{State[i][j]}$: This represents an element within the state matrix, which is a two-dimensional array used to store intermediate data during the AES encryption process. It denotes the element located at row i and column j of the state matrix.

i: The variable i ranges from 0 to 3, inclusive. It corresponds to the four rows of the state matrix. Each row undergoes a distinct cyclic shift operation.

j: The variable j signifies the column index within a specific row of the state matrix. The expression j + i implies that each element within a row is shifted to the right by an offset determined by its row index. This offset varies for each row, creating a unique permutation for every row.

MixColumns Transformation:

The MixColumns transformation performs matrix multiplication with a fixed polynomial matrix:

$$\mathrm{State[i] = c(x) * State[i]}$$
$$\mathrm{(for\ 0 <= i < 4)}$$

$\mathrm{c(x)}$ is the polynomial matrix.

KeyExpansion extends the original key into a set of round keys used for encryption and decryption in different rounds. It can be expressed mathematically as:

$$\mathrm{RoundKey[i] = KeyExpansion}$$
$$\mathrm{(RoundKey[i-1],\ i)}$$
$$\mathrm{(for\ 0 <= i < Nr)}$$

$\mathrm{RoundKey[i]}$ represents the round key for round i.
$\mathrm{KeyExpansion}$ is the key expansion function.
Nr is the total number of rounds.

The corresponding decryption process is:

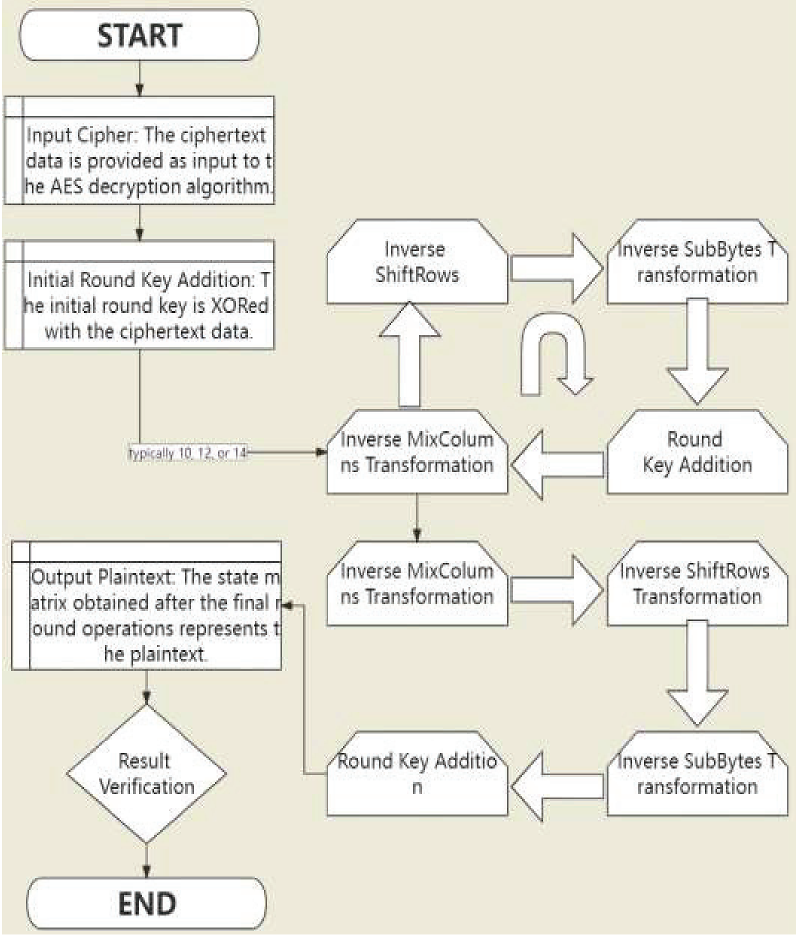
START
Input Cipher: The ciphertext data is provided as input to t he AES decryption algorithm.
Initial Round Key Addition: T he initial round key is XORed with the ciphertext data.
typically 10, 12, or 14
Inverse ShiftRows
Inverse SubBytes T ransformation
Round Key Addition
Inverse MixColum ns Transformation
Inverse MixColum ns Transformation
Inverse ShiftRows Transformation
Inverse SubBytes T ransformation
Round Key Additio n
Output Plaintext: The state m atrix obtained after the final r ound operations represents t he plaintext.
Result Verification
END

Figure 2 Data decryption process.

3.2 Power Grid Data Security Identification Process

The application of the (AES to power grid data security identification involves a systematic process to ensure the confidentiality and integrity of critical information.

Data encryption serves as the first line of defense in safeguarding power grid data. During this phase, the raw power grid data is subjected to AES encryption, a meticulously designed process rooted in mathematical operations. These mathematical transformations, characterized by the SubBytes, ShiftRows, and MixColumns operations, work in synergy with round keys generated during the KeyExpansion process to create a ciphertext that is highly resistant to attacks. The mathematical representation of this encryption process is encapsulated in the formula:

$$\begin{aligned}&\mathrm{CipherText} = \mathrm{AES}_{\mathrm{Encrypt}}\\&(\mathrm{PlainText},\ \mathrm{Key})\end{aligned}$$

$\mathrm{CipherText}$ represents the encrypted data.
$\mathrm{AES}_{\mathrm{Encrypt}}$is the AES encryption function.
$\mathrm{PlainText}$ is the original data.
Key is the encryption key.

The encrypted data can be transmitted through an insecure communication channel without concerns of data leakage.

Upon receiving the data, authorized recipients can decrypt it using the same key and AES algorithm. The decryption process is the reverse of encryption and involves steps such as inverse SubBytes, inverse ShiftRows, inverse MixColumns, and more. The mathematical representation is:

$$\begin{aligned}&\mathrm{DecryptedData} = \mathrm{AES}_{\mathrm{Decrypt}}\\&(\mathrm{CipherText},\ \mathrm{Key})\end{aligned}$$

$\mathrm{DecryptedData}$ represents the original data after decryption.
$\mathrm{AES}_{\mathrm{Decrypt}}$ is the AES decryption function.
$\mathrm{CipherText}$ is the encrypted data.
Key is the decryption key.

AES provides robust data security through complex mathematical operations and key expansion, ensuring the confidentiality of power grid data. Only authorized recipients possessing the correct key can decrypt the data.

By applying AES to power grid data security identification, the confidentiality of power grid data during transmission and storage can be guaranteed. AES's mathematical foundation and security features make it an ideal choice for protecting power grid data.

4 Performance Verification and Analysis

In this section, we delve into the performance verification and analysis of the proposed optimization of security identification in power grid data using the

Advanced Encryption Standard (AES) algorithm. The objective is to assess the effectiveness and efficiency of AES-based security enhancement within the power grid domain. Our analysis encompasses various aspects, including computational complexity, encryption/decryption speed, and overall system security.

This article discusses the performance testing conducted to evaluate the latency of various encryption and decryption operations under different key lengths (bit key size). The tests involve three different sets of data, including a large-scale data set, a medium-scale data set, and a small-scale data set.

For large-scale datasets, we tested 1 million randomly generated keys, using randomly generated data and random keys to simulate real-world usage. For the medium-size dataset, we tested 100,000 randomly generated keys, which is much smaller than the large-scale dataset, but still requires the use of relatively high-performance computing and storage resources. For small-scale data sets, we tested 10,000 randomly generated keys, a relatively small set of tests designed to simulate systems running on smaller computers and storage resources.

The test environment is as follows.

CPU: Intel Xeon E5-2690 v4, 18 cores, 36 threads.
Memory: 128GB DDR4 ECC memory.
Storage: 1TB SSD and 2TB SATA.
Network: 1000Mbps Ethernet card.
Operating system: Ubuntu 18.04 LTS.
Database: MySQL 5.7.
Encryption and decryption library: OpenSSL 1.1.1.
Programming language: Python 3.6.

In addition, we used a load machine to simulate concurrent user access to test system performance metrics such as response time, throughput, number of concurrent users, and so on. The load machine can be configured according to the test requirements to simulate user access in different scenarios.

We focus on the performance of the following four encryption operations:

SubBytes Transformation Complexity: This is a step in the Advanced Encryption Standard (AES) that involves byte substitution. We measured the time required to perform the SubBytes transformation at different key lengths, in milliseconds (ms).

ShiftRows Transformation Complexity: ShiftRows is another step in AES, involving row shifting. We recorded the time taken to perform the ShiftRows transformation at different key lengths, in milliseconds.

MixColumns Transformation Complexity: MixColumns is a part of AES that involves column mixing. We conducted tests on the time required to execute the MixColumns transformation at different key lengths, in milliseconds.

KeyExpansion Complexity: KeyExpansion is a critical step in AES encryption, dealing with key expansion. We measured the time taken to perform KeyExpansion at different key lengths, in milliseconds.

These tests enable us to understand the performance characteristics of these encryption and decryption operations under various key lengths and data set sizes. This information is valuable for optimizing encryption algorithms to enhance both security and system performance.

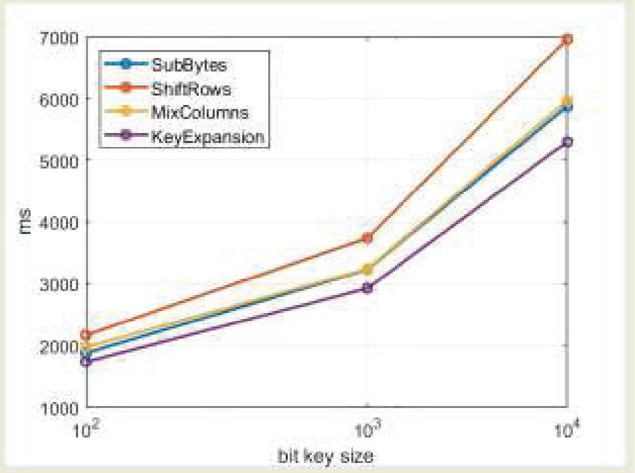

Figure 3 Large-scale data set.

The figure reflects data characteristics, trends, and potential causes for the Large-scale data set across different bit key sizes (128, 192, and 256) for various transformation complexities:

The SubBytes transformation complexity increases as the bit key size grows. There is a clear upward trend in SubBytes complexity with larger key sizes. This increase is expected because a larger key size requires more computational effort to perform the SubBytes transformation, which involves byte substitution.

Similar to SubBytes, the ShiftRows transformation complexity also shows an upward trend with increasing bit key size. There is a consistent increase in ShiftRows complexity as the key size increases. The ShiftRows operation involves row shifting, and larger key sizes likely lead to more intricate row manipulation, resulting in higher complexity.

Similar to the other transformations, MixColumns complexity increases with larger key sizes. There is a consistent upward trend in MixColumns complexity. MixColumns involves column mixing, and larger key sizes likely lead to more complex mixing patterns, requiring additional computational effort.

The KeyExpansion complexity also increases as the bit key size increases. There is a clear upward trend in KeyExpansion complexity. KeyExpansion is a fundamental step in AES encryption, and larger key sizes result in more extensive key expansion, leading to higher computational complexity.

In summary, the data indicates that as the bit key size increases, the computational complexity of SubBytes, ShiftRows, MixColumns, and KeyExpansion transformations also increases. This trend is expected because larger key sizes necessitate more computational effort to perform these encryption operations, enhancing security but also potentially impacting system performance.

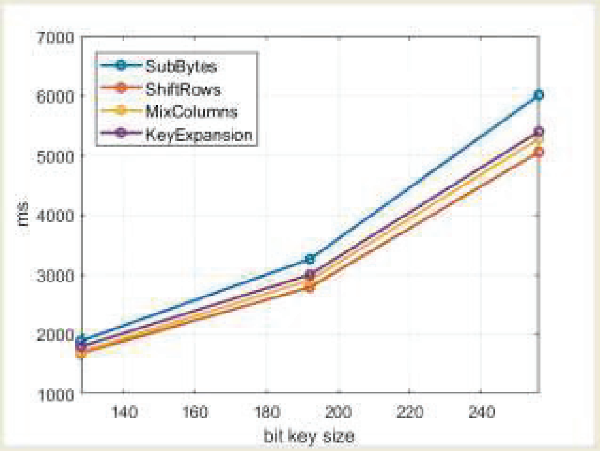

Figure 4 Medium-scale size data set.

The figure illustrates data characteristics, trends, and potential factors for the Medium-scale size data set across different bit key sizes (128, 192, and 256) for various transformation complexities:

SubBytes transformation complexity generally increases with larger bit key sizes. There is an upward trend in SubBytes complexity as the key size grows. The increase in SubBytes complexity is due to the larger key sizes, which require more computational effort for byte substitution during the transformation.

ShiftRows transformation complexity also shows an upward trend with increasing bit key size. There is a consistent increase in ShiftRows complexity as the key size increases. Larger key sizes lead to more intricate row-shifting operations within the transformation, resulting in higher computational complexity.

MixColumns complexity increases with larger bit key sizes. There is a clear upward trend in MixColumns complexity. Larger key sizes require more complex column-mixing operations during the MixColumns transformation, necessitating additional computational effort.

KeyExpansion complexity rises as the bit key size increases. There is a noticeable upward trend in KeyExpansion complexity. KeyExpansion is a fundamental step in AES encryption, and larger key sizes result in a more extensive key expansion process, leading to higher computational complexity.

In summary, the data demonstrates that increasing the bit key size generally leads to higher computational complexity for SubBytes, ShiftRows, MixColumns, and KeyExpansion transformations. This trend is driven by the need for more computational effort to perform these encryption operations with larger key sizes, which enhances security but may impact system performance.

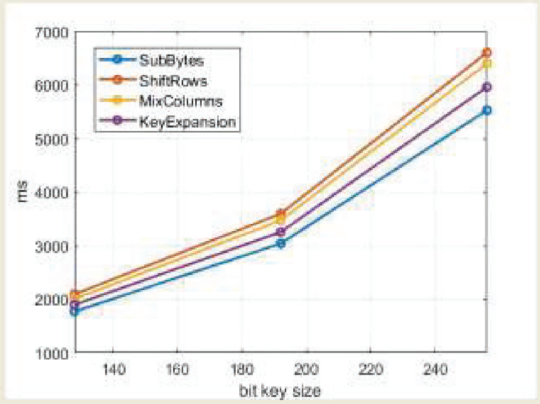

Figure 5 Small-scale data set.

The figure illustrates data characteristics, trends, and potential factors for the Small-scale data set across different bit key sizes (128, 192, and 256) for various transformation complexities:

SubBytes transformation complexity tends to increase as the bit key size grows. There is an upward trend in SubBytes complexity as the key size increases. The rise in SubBytes complexity can be attributed to the larger key sizes, which require more computational effort for byte substitution during the transformation.

ShiftRows transformation complexity also exhibits an upward trend with increasing bit key size. There is a consistent increase in ShiftRows complexity as the key size becomes larger. Larger key sizes result in more intricate row-shifting operations within the transformation, leading to higher computational complexity.

MixColumns complexity increases with larger bit key sizes. There is a clear upward trend in MixColumns complexity. The increase in MixColumns complexity is due to larger key sizes requiring more complex column-mixing operations during the transformation, necessitating additional computational effort.

KeyExpansion complexity rises as the bit key size increases. There is a noticeable upward trend in KeyExpansion complexity. KeyExpansion is a fundamental step in AES encryption, and larger key sizes result in a more extensive key expansion process, leading to higher computational complexity.

In summary, the data reveals that increasing the bit key size generally results in higher computational complexity for SubBytes, ShiftRows, MixColumns, and KeyExpansion transformations. This trend is driven by the need for more computational effort to perform these encryption operations with larger key sizes, which enhances security but may impact system performance.

4.1 Encryption/Decryption Speed Evaluation

Throughput Measurement: To gauge the practical performance of AES-based security identification in power grid data, we measure the encryption and decryption throughput. We examine the latency introduced by AES encryption and decryption processes. Latency represents the delay incurred during data transformation, and it is crucial in real-time applications within the power grid sector.

The testing encompasses three recognition capability groups: Strong recognition ability, Standard recognition capability, and Weak recognition.

The focus is on measuring the time taken for encryption and decryption throughput, with time units recorded in milliseconds (ms).

The specific testing methodology and procedures involved are elaborated in the article, which includes:

Recognition Capability Groups: Dividing the test cases into three groups based on recognition ability—Strong, Standard, and Weak. These groups represent various scenarios with varying security requirements.

Bit Key Sizes: Testing is performed using different bit key sizes to evaluate the impact of key length on encryption and decryption efficiency. Common key sizes such as 128, 192, and 256 bits are typically considered.

Throughput Measurements: Measuring the time taken for encryption and decryption operations for each recognition capability group and key size. Throughput is assessed in terms of how many milliseconds are required to perform these operations.

By conducting performance tests using this methodology, the article aims to provide insights into the time efficiency of encryption and decryption across various recognition capability scenarios and key sizes. This analysis aids in understanding the trade-offs between security and processing speed, which can be crucial for selecting appropriate encryption configurations in different applications.

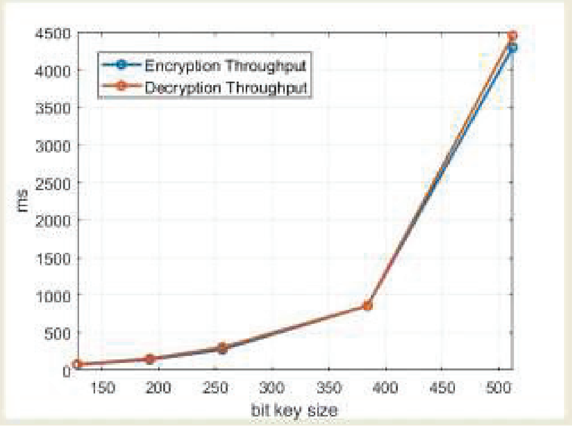

Figure 6 Strong recognition ability.

Encryption throughput increases significantly as the bit key size grows. There is a clear and consistent upward trend in encryption throughput with larger bit key sizes. The increase in encryption throughput is mainly due to the larger bit key sizes, which provide stronger security but also require more computational effort for encryption. As key size increases, the encryption process becomes more complex, resulting in higher throughput times.

Similar to encryption, decryption throughput also exhibits a substantial increase as the bit key size increases. There is a noticeable and consistent upward trend in decryption throughput with larger key sizes. The increase in decryption throughput is primarily attributed to the larger bit key sizes, which demand more computational effort for decryption. Larger keys entail more complex decryption processes, leading to higher throughput times.

In summary, the data reveals a strong positive correlation between bit key size and both encryption and decryption throughput for Strong recognition ability. As the key size increases, the encryption and decryption processes become more computationally intensive, resulting in longer throughput times. This trade-off between security (achieved through larger key sizes) and processing speed should be carefully considered when selecting encryption configurations for scenarios requiring strong recognition ability.

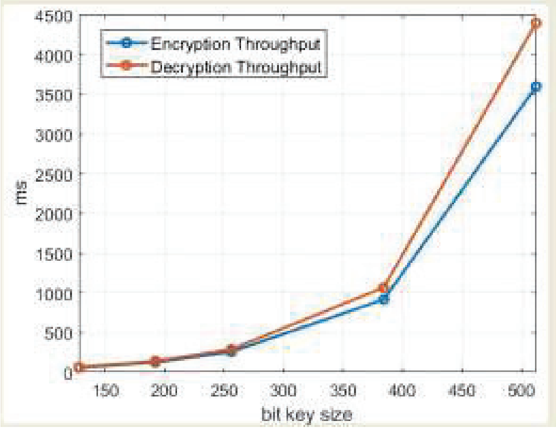

Figure 7 Standard recognition capability.

Encryption throughput increases as the bit key size grows, but the increase is not as steep as in the Strong recognition ability group. There is an upward trend in encryption throughput with larger bit key sizes. The increase in encryption throughput is still primarily due to the larger bit key sizes, which provide enhanced security. However, the encryption process for Standard recognition requires fewer computational resources compared to Strong recognition, resulting in a less steep increase in throughput times compared to the Strong recognition group.

Similar to encryption, decryption throughput increases as the bit key size increases, but again, the increase is not as pronounced as in the Strong recognition ability group. There is an upward trend in decryption throughput with larger key sizes. The increase in decryption throughput is mainly driven by the larger bit key sizes, which enhance security but require more computational effort. The decryption process for Standard recognition is less computationally intensive than for Strong recognition, leading to a milder increase in throughput times.

In summary, for Standard recognition capability, the data reflects a positive correlation between bit key size and both encryption and decryption throughput. However, the increase in throughput is less pronounced compared to the Strong recognition ability group, indicating a more moderate trade-off between security and processing speed. This suggests that Standard recognition configurations strike a balance between security and performance.

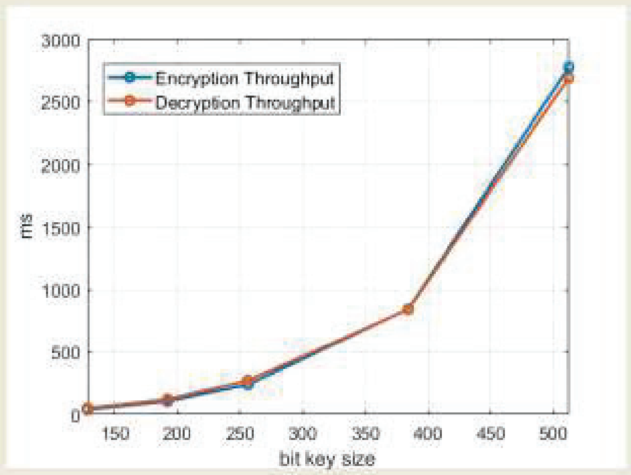

Figure 8 Weak recognition.

Encryption throughput increases as the bit key size grows, but the increase is the least pronounced among the three recognition groups (Strong, Standard, and Weak). There is an upward trend in encryption throughput with larger bit key sizes. The increase in encryption throughput is still primarily due to the larger bit key sizes, which offer some level of enhanced security. However, for Weak recognition, the encryption process requires fewer computational resources compared to the other recognition groups, resulting in the smallest increase in throughput times.

Similar to encryption, decryption throughput increases as the bit key size increases, with a relatively mild increase. There is an upward trend in decryption throughput with larger key sizes. The increase in decryption throughput is mainly attributed to the larger bit key sizes, which offer some level of enhanced security. However, the decryption process for Weak recognition requires fewer computational resources compared to Strong and Standard recognition, resulting in a more moderate increase in throughput times.

In summary, for Weak recognition, the data indicates a positive correlation between bit key size and both encryption and decryption throughput. However, the increase in throughput is the least pronounced among the three recognition groups, suggesting that configurations for Weak recognition prioritize performance over security. This trade-off is evident as the encryption and decryption processes for Weak recognition are less computationally intensive compared to the other recognition groups.

4.2 System Security Assessment

This set of performance tests is designed to assess the performance of different Architecture types (Single-Tier Architecture, Microservices Architecture, Three-Tier Architecture) against key security performance indicators.

Risk of Unauthorized Access:

Test objective: To evaluate the security performance of different architectures against unauthorized user access.

Test methods: Simulate unauthorized user attempts to access the system or data, record successful and failed attempts, and any potential vulnerabilities. This can include methods such as penetration testing, access control audits, etc. If U is the set of all possible users, A is the set of attackers, N is the number of all legitimate users, T is the number of all attackers, and X is a random variable indicating whether a user is authorized (1 indicating authorization, 0 indicating non-authorization), then we can define a binary random variable (X, Y) to represent the attempt of authorization and non-authorization. The probability of successful authorization is $P(X=1|Y=0)$, and the probability of successful non-authorization is $P(X=0|Y=1)$.

The risk of unauthorized access decreases slightly as the bit key size increases. There is a slight downward trend in the risk of unauthorized access with larger key sizes. Larger key sizes provide stronger protection against unauthorized access, resulting in a lower risk of unauthorized access. This is a positive security trend.

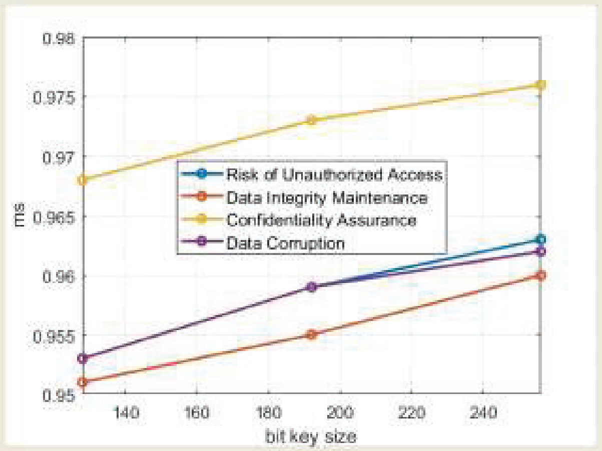

Figure 9 Single-tier architecture.

Data integrity maintenance improves marginally as the bit key size increases. There is a slight upward trend in data integrity maintenance with larger key sizes. Larger key sizes contribute to better data integrity maintenance, indicating that data remains less susceptible to corruption or tampering during transmission or storage.

Confidentiality assurance improves as the bit key size increases. There is a clear upward trend in confidentiality assurance with larger key sizes. Larger key sizes significantly enhance the confidentiality of data, making it more secure against unauthorized access and eavesdropping.

Prevention improves slightly as the bit key size increases. There is a minor upward trend in prevention with larger key sizes. Larger key sizes contribute to better protection against data corruption, reducing the likelihood of data becoming corrupted during transmission or storage.

In summary, for the Single-Tier Architecture, increasing the bit key size generally leads to improved security performance across all four metrics. Larger key sizes enhance security by reducing the risk of unauthorized access, improving data integrity maintenance, providing better confidentiality assurance, and preventing data corruption. This suggests that selecting larger key sizes can be an effective strategy to enhance security within a Single-Tier Architecture.

The risk of unauthorized access shows a mixed trend, with a slight increase from 128-bit to 192-bit key size and then a decrease at 256-bit. The change in the risk of unauthorized access is relatively small, but the

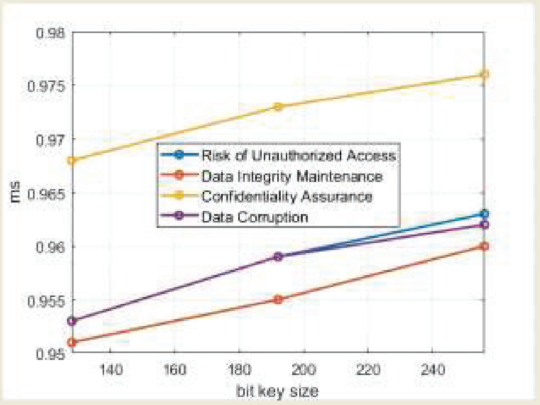

Figure 10 Microservices architecture.

architecture exhibits better performance at 256-bit key size. This suggests that a 256-bit key provides slightly better protection against unauthorized access in this architecture.

Data integrity maintenance shows a mixed trend, with a slight increase from 128-bit to 192-bit key size and a decrease at 256-bit. Similar to the risk of unauthorized access, the trend is not consistent, but the performance slightly improves with a 192-bit key size. This indicates better data integrity maintenance with a 192-bit key.

Confidentiality assurance improves as the bit key size increases. There is a consistent upward trend in confidentiality assurance with larger key sizes. Larger key sizes significantly enhance the confidentiality of data, making it more secure against unauthorized access and eavesdropping.

Prevention shows a mixed trend, with a slight increase from 128-bit to 192-bit key size and then a decrease at 256-bit. Similar to the risk of unauthorized access and data integrity maintenance, the trend is not consistent, but the architecture exhibits better prevention with a 192-bit key.

In summary, for the Microservices Architecture, the relationship between bit key size and security metrics is not as consistent as in the Single-Tier Architecture. While larger key sizes generally improve confidentiality assurance, the trends for risk of unauthorized access, data integrity maintenance, and prevention are mixed. It's important to note that the choice of key size should consider the specific security requirements and trade-offs within the Microservices Architecture.

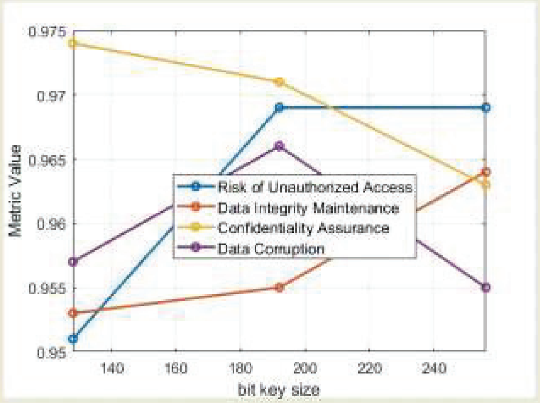

Figure 11 Three-tier architecture.

The risk of unauthorized access shows a mixed trend, with a slight increase from 128-bit to 192-bit key size and then remaining stable at 256-bit. The architecture exhibits better performance in terms of risk of unauthorized access at 192-bit key size compared to 128-bit. However, it stabilizes at 256-bit, indicating that further increases in key size may not provide significant additional protection against unauthorized access.

Data integrity maintenance shows a mixed trend, with a slight increase from 128-bit to 192-bit key size and a further increase at 256-bit. The trend suggests that data integrity maintenance slightly improves with larger key sizes. A 256-bit key offers slightly better protection against data tampering or corruption compared to 128-bit and 192-bit keys.

Confidentiality assurance exhibits a decreasing trend as the bit key size increases. Surprisingly, larger key sizes result in a decrease in confidentiality assurance within the Three-Tier Architecture. This might indicate that the architecture has specific characteristics or limitations that impact confidentiality performance at larger key sizes.

Prevention shows a mixed trend, with a slight increase from 128-bit to 192-bit key size and then a decrease at 256-bit. Similar to the risk of unauthorized access and data integrity maintenance, the trend is not consistent. The architecture exhibits better prevention with a 192-bit key.

In summary, for the Three-Tier Architecture, the relationship between bit key size and security metrics is somewhat mixed and varies compared to the other architectures. While larger key sizes offer better data integrity maintenance and, to some extent, risk of unauthorized access protection, they result in decreased confidentiality assurance. This indicates that the choice of key size should be carefully considered within the context of the specific architecture's characteristics and security requirements.

5 Conclusion

The application of AES encryption not only bolsters data protection but also leads to improved accuracy and efficiency in security identification techniques. This research has illuminated the path to fortifying security measures within power grid operations, thereby reducing vulnerability to potential threats. As we wrap up this study, it is evident that the findings have illuminated the advantages of AES-based security optimization, ultimately contributing to the advancement of data security in power grid operations. The lessons learned and insights gained from this research will undoubtedly play a pivotal role in ensuring the continued reliability and resilience of power grids in an increasingly digital and interconnected world.

References

[1] Sarita Sanap,and Vijayshree More. "An Ultra-High Throughput and Efficient Implementation of Advanced Encryption Standard." International Journal of Electrical and Electronic Engineering & Telecommunications 12.1(2023). doi:10.18178/IJEETC.12.1.46-52.

[2] Alslman Yasmeen, et al. "Hybrid Encryption Scheme for Medical Imaging Using AutoEncoder and Advanced Encryption Standard." Electronics 11.23(2022). doi:10.3390/ELECTRONICS11233967.

[3] Sabreen Ali Hussein, et al. "Evaluating image encryption algorithms for the hyperchaotic system and fibonacci q-matrix, secure internet of things, and advanced encryption standard." Eastern-European Journal of Enterprise Technologies 5.2(2022). doi:10.15587/1729-4061.2022.

[4] Li ZhenQiang, et al. "Novel quantum circuit implementation of Advanced Encryption Standard with low costs." Science China Physics, Mechanics & Astronomy 65.9(2022). doi:10.1007/S11433-022-1921-Y.

[5] Wang Zeguo, et al. "Variational quantum attacks threaten advanced encryption standard based symmetric cryptography." Science China Information Sciences 65.10(2022). doi:10.1007/S11432-022-3511-5.

[6] Renugadevi N., et al. "Methods for improving the implementation of advanced encryption standard hardware accelerator on field programmable gate array-A survey." Security and Privacy 5.6(2022). doi: 10.1002/SPY2.254.

[7] Lee JongHyeok, Kim Jiyoon,and Han Dong Guk. “Novel Shuffling Countermeasure for Advanced Encryption Standard (AES) against Profiled Attack in Mobile Multimedia Services.” Wireless Communications and Mobile Computing 2022. doi:10.1155/2022/6495546.

[8] Nahom Gebeyehu Zinabu,and Samuel Asferaw. “Enhanced Efficiency of Advanced Encryption Standard (EE-AES) Algorithm.” American Journal of Engineering and Technology Management 7.3(2022). doi: 10.11648/J.AJETM.20220703.13.

[9] Nahom Gebeyehu Zinabu,and Samuel Asferaw. “Enhanced Security of Advanced Encryption Standard (ES-AES) Algorithm.” American Journal of Computer Science and Technology 5.2(2022). doi:10.11648/J.AJCST.20220502.13.

[10] Liu Guangzhe, et al. “An Image Encryption Algorithm Based on Discrete-Time Alternating Quantum Walk and Advanced Encryption Standard.” Entropy 24.5(2022). doi:10.3390/E24050608.

[11] Raju Deril, et al. “Multi-level image security using elliptic curve and magic matrix with advanced encryption standard.” Multimedia Tools and Applications 81.26(2022). doi:10.1007/S11042-022-12993-Y.

[12] Niraj Kumar, Vishnu Mohan Mishra,and Adesh Kumar. “Smart Grid Security by Embedding S-Box Advanced Encryption Standard.” Intelligent Automation & Soft Computing 34.1(2022). doi:10.32604/IASC.2022.024804.

[13] Nabilah Abughazalah, et al. “Generalization of Advanced Encryption Standard Based on Field of Any Characteristic.” Computers, Materials & Continua 73.3(2022). doi:10.32604/CMC.2022.031417.

[14] T. Manoj Kumar,and P. Karthigaikumar. “Implementation of a High-Speed and High-Throughput Advanced Encryption Standard.” Intelligent Automation & Soft Computing 31.2(2022). doi:10.32604/IASC.2022.020090.

[15] Lasseni Coulibaly, Fethi Ouallouche,and Vitalice Oduol. “Joint Cryptography and Channel-Coding Based on Low-Density Parity-Check Codes and Advanced Encryption Standard for 5G Systems.” International Journal of Electrical and Electronic Engineering & Telecommunications 10.6(2021). doi:10.18178/IJEETC.10.6.397-406.

[16] Padmavathi R. Anusha,and Dhanalakshmi K. S. “An Advanced Encryption Standard in Memory (AESIM) Efficient, High Performance S-box Based AES Encryption and Decryption Architecture on VLSI.” Wireless Personal Communications 123.4(2021). doi:10.1007/S11277-021-09278-2.

[17] Hafsa Amal, et al. "Real-time video security system using chaos – improved advanced encryption standard (IAES)." Multimedia Tools and Applications 81.2(2021). doi:10.1007/S11042-021-11668-4.

[18] Ahmad Nabihah,and Hasan S.M. Rezaul. "A new ASIC implementation of an advanced encryption standard (AES) crypto-hardware accelerator." Microelectronics Journal 117.(2021). doi:10.1016/J.MEJO.2021.105255.

[19] Cañadas Agustín Moreno, Gaviria Isaías David Marín,and Vega Juan David Camacho. "Relationships between the Chicken McNugget Problem, Mutations of Brauer Configuration Algebras and the Advanced Encryption Standard." Mathematics 9.16(2021). doi:10.3390/MATH916 1937.

[20] Assafli, Hayder T., Hashim, Ivan A.,and Naser, Ahmed A. "Advanced Encryption Standard (AES) acceleration and analysis using graphical processing unit (GPU)." Applied Nanoscience 13.2(2021). doi:10.1007/ S13204-021-01985-3.

Biographies

Biaoqi Li, (1994–) Male, Liaoning, Master degree, Senior Engineer, Service computing.

Min Xu (1988–) Male, Yunnan, Senior Engineer, Data management and Data quality.

Yuan Zhou (1989–) Male, Yunnan, Senior Engineer, Enterprise Information System.

Haibin Liu (1987–) Male, Gansu, Data Engineer, Data mining, analysis and Data asset operation.

Renlong Zhang (1997–) Male, Yunnan, Data Engineer, Data mining, analysis and Data asset operation.