International Conference on Interdisciplinary Research in Science, Management, Engineering and Humanities (ICIRSMEH - 2025)
26th October, 2025, Bhubaneshwar, Odisha, India.

CERTIFICATE NO : ICIRSMEH /2025/C1025722

Comparative Cryptographic Performance Study for Secure Mobile Transaction Systems

Amit Sahu
Research Scholar, Department of Computer Science, Mansarovar Global University, Sehore, M.P., India.

ABSTRACT

The requirement for safe, effective, and lightweight payment methods that can function in contexts with limited resources has been heightened by the fast expansion of mobile commerce. Using a structured transaction framework and robust cryptographic methods, this article introduces a Secured Mobile Payment System (SMPS) that guarantees privacy, authenticity, integrity, and non-repudiation. Important parties including the consumer, retailer, financial institution, and mobile service provider are involved in the three main phases of the suggested system: authentication, client identification, and payment processing. Key generation, encryption, and decryption inside the payment workflow are handled by the Elliptic Curve Integrated Encryption Scheme (ECIES), which enhances security and computational efficiency. Utilizing the FlexiProvider and Bouncy Castle cryptography APIs, the system is deployed in a Java-based environment. By contrasting ECIES and RSA across a range of key sizes, we can see how well they perform in terms of computational cost, encryption and decryption latency, and overall performance. The experimental findings show that ECIES is much better than RSA for safe mobile payment applications because to its quicker key generation, shorter decryption time, and greater scalability. The results show that the suggested SMPS successfully addresses the needs of contemporary mobile payment systems with high efficiency and solid security assurances.

Keywords: *Mobile Payment System, Cryptography, Elliptic Curve, Encryption, Decryption*.

I. INTRODUCTION

The evolution of new networking technology is influencing the desire for current personal communications. Data security is of the utmost importance in wireless communication, especially for sensitive financial transactions conducted online. The goals of implementing and using online banking services and transactions are to provide consumers with convenience, quick service, increased efficiency, happy customers, round-the-clock operations, and cost savings. Many methods are used to make sure that the data being transferred is secure. The percentage of people who want the ability to handle their bank accounts from any location at any time is steadily rising, and the internet is an integral and basic component of our everyday lives. Internet banking is now an integral part of the strategy of all financial institutions and many other types of companies as a result of the tremendous rise of online transactions. It goes without saying that sensitive information pertaining to banks, their customers, and the transactions involving their funds must be kept safe.

The primary concern of banks regarding internet banking is the security of the central computer system that processes so many transactions. Because of the lack of protection, catastrophic damage might happen. Therefore, protecting client funds and personal information has become a top priority for financial institutions. Therefore, the system for online banking should include safeguards to prevent false or misleading claims, ensure that only authorized users can access a user's account, and prevent the bank or other unauthorized parties from altering or stealing any information viewed or provided. Data encryption and decryption techniques of cryptography are a significant tool for protecting sensitive information. When dealing with more complicated and enormous amounts of data, network security becomes more critical.

Cryptography is the practice of encoding data such that it cannot be deciphered by anybody who does not have the proper authorization to access it. Data privacy, data integrity, authorization, and authentication are all components of information security that are studied in relation to mathematical methods and concepts. Cryptology describes the technology that is utilized for this purpose. The process of converting plaintext or an image into an incomprehensible form known as cipher text or cipher picture happens when the user specifies the format of the input data. To us, this is known as encryption. It is up to the user to supply the exact cryptographic technique to encrypt the data. Decryption is the process of recovering the original data or message in a reversible way.

Many parties are usually involved in a mobile payment system, including consumers, businesses, banks, payment processors, and mobile network providers. Because financial transactions typically take place across public and potentially vulnerable communication channels, strong cryptographic procedures are required to guarantee the privacy, authenticity, availability, non-repudiation, and integrity of the data. Although traditional cryptographic methods work well in connected and resource-rich contexts, they may be rather taxing on mobile devices' limited processor power, memory capacity, battery life, and bandwidth, resulting in significant computational and energy overheads. As a result, mobile payment systems are increasingly seeking cryptographic solutions that are both efficient and safe, yet lightweight, so as not to negatively impact performance or the user experience.

There is a lot of interest in Elliptic Curve Cryptography (ECC) since it is a new public-key cryptography paradigm that promises to solve the efficiency and security problems with mobile payment systems. When compared to more conventional public-key algorithms like RSA and DSA, ECC uses far lower key sizes while providing the same level of security, thanks to its foundation in the algebraic structure of elliptic curves over finite fields. To illustrate the point, a 256-bit ECC key is as secure as a 3072-bit RSA key. With its drastically reduced key size, ECC is ideal for mobile and embedded systems because it reduces computational complexity, memory requirements, processing time for cryptographic operations, and energy consumption.

Mobile payment systems that use ECC have better security because they can use digital signatures, efficient key exchange, and encryption methods that are resistant to modern cryptographic assaults. Elliptic Curve Diffie-Hellman (ECDH) and other ECC-based key agreement protocols allow communicative entities to securely establish session keys without disclosing secret keys over the

communication channel. Elliptic Curve Digital Signature Algorithm (ECDSA) and similar ECC-based digital signature systems offer robust authentication and non-repudiation, guaranteeing that transaction requests come from authorized users and remain unaltered throughout transmission. Secure mobile payment methods rely on these cryptographic primitives, which are essential for protecting customers' personal and financial data.

The efficiency and scalability of mobile payment systems are enhanced by ECC, which also offers excellent security assurances. Payment platforms need to be able to process a high volume of transactions in real time with no delays since transaction volumes are increasing at an exponential rate. To keep users happy and trust the system, ECC reduces computing cost, which means transactions may be processed faster and the system is more responsive. Additionally, ECC-based systems are better suited for mobile networks with unpredictable connection and low data rates since they use less bandwidth during authentication and key exchange.

For new forms of mobile payment including Near Field Communication (NFC), QR code-based purchases, mobile wallets, and peer-to-peer payment apps, ECC is more important than ever. For these systems to function, fast cryptographic procedures are essential for real-time transaction validation and frictionless user engagement. With ECC, mobile devices, retailers, and banks can communicate securely end-to-end, which improves the payment ecosystem's dependability and decreases the likelihood of fraud. To top it all off, ECC works with all the latest security protocols and standards, so it can be used with mobile financial services with ease. This includes TLS, SE, and TEE, which are all contemporary security standards.

While ECC has many benefits, there are a few obstacles to overcome when incorporating it into mobile payment systems. These include making sure parameters are securely selected, avoiding implementation weaknesses, and protecting against side-channel attacks. The security of systems that rely on ECC might be jeopardized due to incorrect curve selection or poor implementation. Thus, to provide strong protection, it is crucial to adhere to recognized cryptographic standards, conduct formal security verification, and build protocols rigorously. To overcome these obstacles without sacrificing speed or usability, researchers have been concentrating on developing mobile payment protocols based on ECC.

II. REVIEW OF LITERATURE

Ntayagabiri, Jean et al., (2024) Given that most IoT devices have limited resources, the fast growth of the IoT poses serious security concerns. In light of these issues, elliptic curve cryptography (ECC) has been proposed as a potential solution. ECC is great for devices with limited memory and processing capacity since it provides high levels of security with lower key lengths. The focal point of this research is a comparison of three popular cryptographic algorithms that rely on ECC: ECDSA, ECIES, and ECDH. In order to determine which algorithms are best for protecting IoT settings, the study thoroughly evaluates their performance using criteria including execution time, overall efficiency, and key generation speed. In situations where key exchanges are frequent, the results

show that ECDH is the best choice because to its fast public key generation. An effective choice for digital signatures and authentication, ECDSA has the quickest overall execution time. On the other hand, ECIES is great for situations that require additional confidentiality due to its extensive encryption capabilities, albeit it is slower. This comparison research emphasizes the significance of matching algorithm selection with particular needs of IoT applications, taking into account aspects such as operational complexity, resource restrictions, performance, and security. These results demonstrate that methods based on ECC are well-suited to tackle the specific problems with IoT security.

Vincent, Olufunke et al., (2020) There have been several security vulnerabilities in the mobile payment system. Mobile payment transactions often lead to users' privacy being violated. Using elliptic curve cryptography over a binary field in conjunction with International Mobile Equipment Identity, this work offers a more secure method for mobile payment systems. All text input is mapped to elliptic curve points using ASCII values by the system, which employs a payment gateway for registration. The gateway encrypts the payment details so that only the merchant's decryption key can decipher them. Key size, security strength, computing power, memory capacity, encryption and decryption time, and mobile phone battery life were some of the metrics used to assess the suggested technique. The outcome validates the scheme's provision of privacy, secrecy, and integrity. For environments with limited resources, such as mobile payment systems, the results demonstrate that the suggested technique is both computationally cheap and time-efficient.

Abdullah, Kawther & Hussien, Nada. (2018) Several methods for improving the Elliptic Curve Cryptography (ECC) algorithm's performance were suggested in this study. Attackers can leverage ECC's public parameters to solve the Discrete Logarithm Problem (DLP), leaving ECC vulnerable. So, to prevent all known attacks, these public parameters should be carefully chosen. A novel generating function is introduced in this research to generate the domain parameters for the elliptic curve. The suggested function employs a safe approach to evade all known attacks that aim to solve the Elliptic Curve Discrete Logarithm Problem (ECDLP). In addition, a safe way to create two subgroups may be achieved by using an efficient method that selects two basis points from the curve. Because it is not based on a hidden flaw that may be used to recover the user's private key, the aforementioned method aims to give the user more trust. Securely exchanging session keys between communication parties is accomplished via the Elliptic Curve Diffie Hellman (ECDH) method. In addition, the message undergoes a preprocessing procedure to improve its diffusion property, which in turn makes it more resistant to cryptanalysis attacks. In the end, to make the digital audio transmission even more resistant to attacks, a dual encryption/decryption process is used, which employs separate session keys at each step of encryption. With no additional time required for encryption, the results demonstrate that the dual elliptic curve system has a good impact on both speed and secrecy.

Ray, Sangram et al., (2016) Nowadays, the banking industry places a premium on mobile technology and its many uses. The advent of convenient banking solutions accessible through mobile phones has made this a reality. Many financial institutions currently provide customers with mobile banking

options; however, these services aren't very useful due to a lack of widespread adoption, reliance on third-party security measures, a lack of functionality beyond basic account inquiries and money transfers, and general inefficiency. Here we introduce m-BAT, a novel client-server application for mobile banking that makes use of elliptic curve cryptography (ECC). This architecture allows users to establish a connection to a bank server using a small client utility that is installed on their mobile device. In addition to addressing the aforementioned issues with current mobile-banking schemes, the proposed m-BAT provides a practical and affordable solution for mobile phones. Furthermore, the plan incorporates a safe method of depositing and withdrawing cash through adjacent kiosks. We examine and find that the suggested approach is well-defended against a variety of relevant security assaults. For this kind of security, ECC-compliant parameters requiring less bit-size are enough. Lastly, the suggested approach outperforms other mobile banking systems in terms of performance efficiency and security aspects.

Patel, Payal et al., (2016) One of the most exciting new frontiers in information technology is mobile cloud computing. Important concerns in MCC include security and privacy. The framework must be designed to provide security while keeping computational overhead to a minimal. We create a plan to encrypt mobile data stored in the cloud, combining Elliptic Curve Cryptography with the Blowfish technique to guarantee privacy and authenticity. Using random numbers makes it more difficult for an attacker to decipher the data during transmission, making it more secure. To further enhance performance, we additionally randomly assign a certain number of rounds to the Blowfish game. Our method has been developed and tested on several platforms, including desktop computers, mobile phones, android emulators, and aakash tablets.

Hnaif, Adnan & Alia, Mohammad. (2015) One convenient substitute for traditional payment methods like cash, checks, or credit is mobile money, often known as mobile payment. We provide a novel, secure mobile payment approach in this article. There are three main steps to this procedure. The first is the authentication process, which includes checking the credentials of the clients who have applied. The second step is the market server's member recognition procedure, which verifies the customer's membership. The last step is the payment procedure, which involves sending the customer's information over an unsecured network to the market server after it has been encrypted using the public-key encryption cryptosystem (RSA). Since the consumer can pay from their own mobile phone with no additional hassle or expense, this mobile payment technique is really more efficient than conventional payment options. Ensuring the security of the suggested solution is the RSA public-key encryption technology. But picking the right key size is critical for avoiding brute force attacks.

Chen, Xiao & Zou, Shi. (2014) Mobile terminal and network capacity limits prevent the direct implementation of the existing Secure Electronic Transaction (SET) protocol into mobile payment. There are potential security issues with the current mobile payment system since it frequently employs a symmetric encryption technique. This presentation introduced a new secure mobile payment protocol built on ECC, which improves the security of client information while ensuring

information flows from merchants to customers. In addition to guaranteeing that the ratio of the length of the ECC key to that of the RSA key is larger than 5:1, theoretical study reveals that ECC may satisfy the requirements of a quick key generation time while breaking the code. Current mobile terminal and network capabilities may handle the new protocol, which ensures a safe and effective mobile payment process, because there are fewer signatures required for certificate verification, asymmetric and symmetric encryption, and so on, compared to the SET protocol.

Vincent, Olufunke et al., (2010) Many people are wary of making purchases online because of the crimes that have been linked to online shopping, particularly with payment methods. In this respect, sensitive applications, such as online commerce, rely on the secure socket layer (SSL) protocol to conduct transactions securely. One of the biggest complaints from online buyers is the poor server response time caused by using SSL technology. Here, we provide an Elliptic Curve Cryptosystem (ECC)–based system for safe credit and debit card transactions. We started by taking a look at the ECC algorithm on prime fields GF(p). Then, we put our suggested solution into action with a real-life credit/debit card transaction and compared its performance to that of the RSA cryptosystem. Based on our findings, ECC outperforms the comparable RSA system in terms of memory use and response time to transaction requests. Since swift actions are required in a constraint open environment, such as a payment system, this makes public key cryptography a better fit.

III. PROPOSED SYSTEM

Each of the three main procedures in the proposed Secured Mobile Payment System (SMPS)—the Authentication Process, the Client Recognition Process, and the Payment Process—is essential to the system's ability to guarantee safe and fast transactions. Customer, retailer, bank, and mobile operator are some of the key players in the system.

Authentication (Getting Service) Process

In the proposed system, the authentication procedure is the first step. The bank and cell operator play a key part in this step. The customer has to be registered before they can utilize this service.

First, the customer must arrange to meet with a bank staff to request the service. The employee will verify with the client that they have supplied the cell phone number that will be used for payment. If the number is not already on file, the employee will ask for it. Step 2: The bank has to communicate with the cell operator to authorize this service by providing them the customer's details. Once this service has been approved, the mobile operator will immediately notify the customer through a notification message that the registration was successful. step 3. Final stage in the registration process is for the bank to provide the customer with their PIN. In the fifth stage, the bank will compute an ECIES public key (Bpu1) and a private key (Bpv1), and in the sixth step, the bank will transmit the public keys (Bpk1) to the market server. The market will then provide the bank the public key Mpu1 after generating the calculated ECIES key Mpr1 in step 7. The consumer may now use the mobile payment service to purchase in the market.

International Conference on Interdisciplinary Research in Science, Management, Engineering and Humanities (ICIRSMEH - 2025)
26th October, 2025, Bhubaneshwar, Odisha, India.

Client Recognition Process

First, the client should access the market to shop. Then, in steps 2 and 3, the market server should verify if the consumer is registered or not. If this is the case, step 4 involves sending a notification message to confirm that the mobile payment service is available. If this is not addressed, the client will go unnoticed (step 5).

Payment Process

The payment procedure is the last step of the suggested system. The two distinct steps of the payment process are the payment itself and the confirmation of payment.

Payment Phase

When a customer chooses to pay with their cell phone, the transaction begins. To begin, the customer can pay using a variety of methods, including cash, credit card, or mobile phone. Now is the time for the customer to give the business their cell phone number if they want to pay with a mobile payment. Step 2 involves verifying the customer's membership via the market server, and the next processes will be executed in a secure manner. The following procedures will be followed in the event that the customer is a member. Client details, such as payment amount and mobile phone number, and market details, such as market ID and password, should be communicated by the market server to the bank. The bank should verify the availability of the funds at the same time.

Thus, the ECIES method is used to encrypt both the customer and market data, with the help of the bank's public keys (Bpu1), to create ciphertext. Afterwards, the bank will get all of this data. In step 4, the bank uses its private key (Bpr1) to decode the data after receiving the encrypted text, which is known as ciphertext. After the first two scenarios are successfully implemented, the bank will test for a legitimate amount and verify that the merchant ID and password are valid.

Once the testing procedure is complete, the bank will communicate the result to the mobile operator. Following this, in steps 7 and 8, the customer is required to reply with their PIN in order for the mobile provider to validate the payment, provided that the amount is legitimate in step 6. The transfer of funds from the mobile provider to the bank is illustrated in step 9.

Payment Confirmation Phase

The payment confirmation phase follows the payment phase in the payment process.

The first step in this phase is for the bank to notify the merchant's server that the payment was processed properly (step 1). Using the public key of the merchant server (Mpu1), the ECIES algorithm encrypts this information. Step 2 involves the market server receiving the encrypted report and decrypting it using the ECIES algorithm using the market private-key (Mpr1). After an operation is successful, the bank will notify the mobile provider (step 3). Lastly, in step 4, the customer is notified of the operation's success by the mobile provider.

International Conference on Interdisciplinary Research in Science, Management, Engineering and Humanities (ICIRSMEH - 2025)
26th October, 2025, Bhubaneshwar, Odisha, India.

The program was developed on an Intel Core i7-based Windows 7 environment with the help of the flexiprovider and bouncycastle APIs, as well as the NetBeans IDE. When it comes to JCA/JCE, Flexiprovider is a formidable toolbox. Key creation, encryption, and decryption are all part of the implementation.

IV. RESULTS AND DISCUSSION

Table 1: RSA and ECIES Keys Generation

Algorithms	80 bit	112 bit	128 bit
RSA	420.50	3890.75	17650.30
ECIES	22.10	24.80	25.40

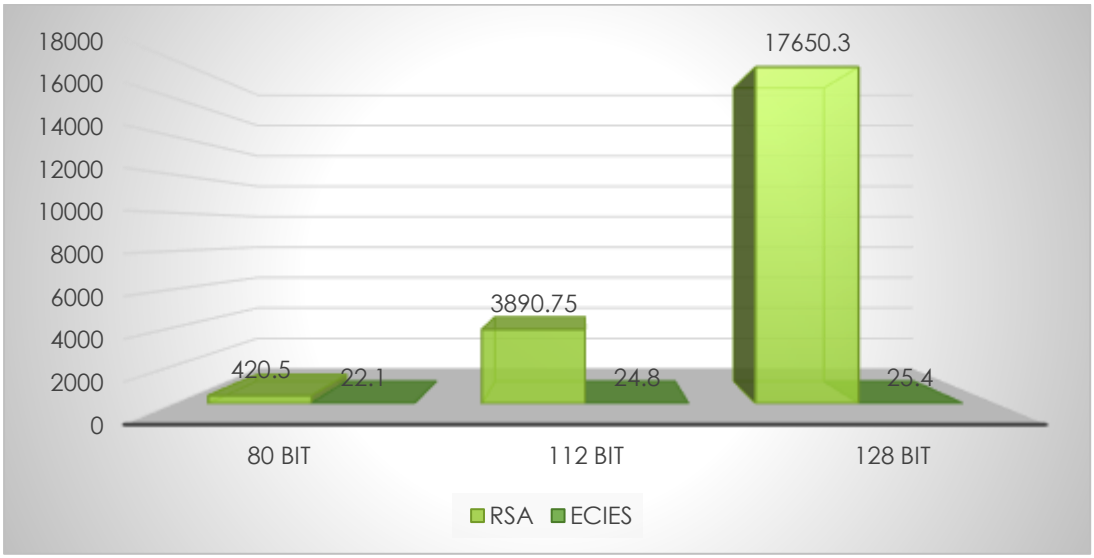

Figure 1: RSA and ECIES Keys Generation

Table 1 shows how long it takes to make keys with the RSA and ECIES algorithms at three distinct security levels: 80-bit, 112-bit, and 128-bit. The findings demonstrate that the time it takes to make an RSA key goes up a lot as the key size goes up.

For example, it takes 420.50 ms to make an 80-bit key and 17,650.30 ms to make a 128-bit key. This fast rise shows how hard it is to produce huge RSA keys. On the other hand, ECIES key generation times are low and stable across all security levels, going up only a bit, from 22.10 ms to 25.40 ms.

Table 2: RSA and ECIES Encryption and Decryption Process

Algorithm	Key Size	Encryption Time (ms)	Decryption Time (ms)
ECIES	160 bit	5.50	8.90
	224 bit	13.80	17.85
	256 bit	18.40	24.10
RSA	1024 bit	2.75	11.20
	2048 bit	4.45	63.80
	3072 bit	5.35	198.90

International Conference on Interdisciplinary Research in Science, Management, Engineering and Humanities (ICIRSMEH - 2025)
26th October, 2025, Bhubaneshwar, Odisha, India.

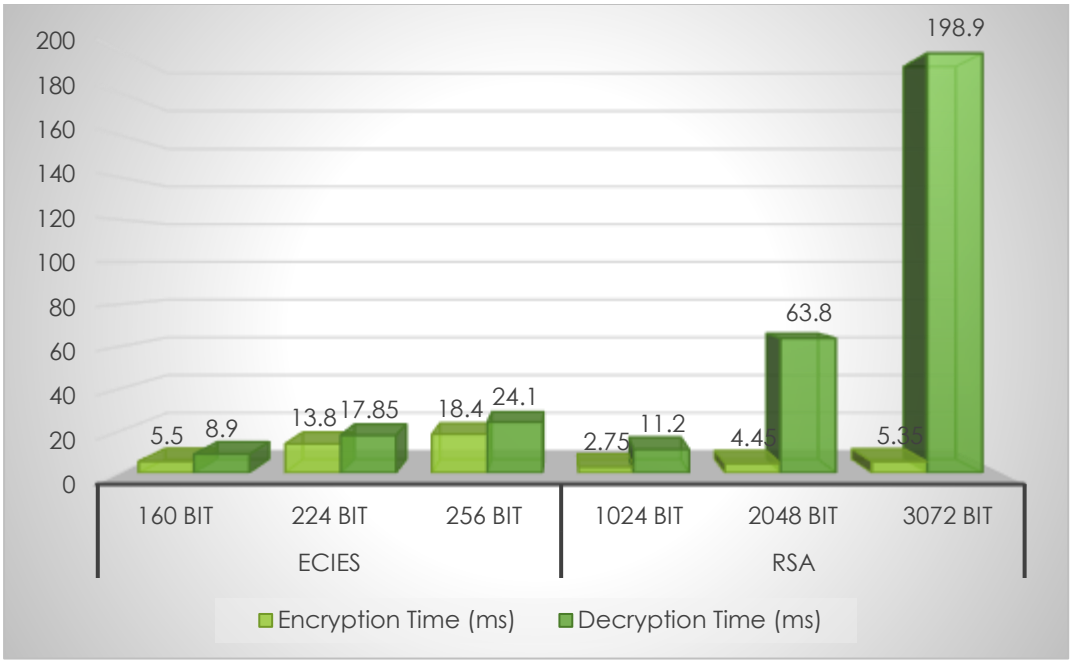

Figure 2: RSA and ECIES Encryption and Decryption Process

Data encryption and decryption performance for different key sizes is displayed in Table 2 for both ECIES and RSA methods. The encryption and decryption times in ECIES gradually rise as the key size grows from 160 to 256 bits. Take the increase in encryption time from 5.50 ms to 18.40 ms and decryption time from 8.90 ms to 24.10 ms as an example. Evidence of ECIES's scalability and efficiency is its consistent and predictable growth.

However, even with bigger keys, RSA still manages to have relatively short encryption lifetimes. The decryption time, however, rapidly increases with key length, rising from 11.20 ms for a 1024-bit key to 198.90 ms with a 3072-bit key. This large increase demonstrates how much more demanding RSA decryption techniques are on computers.

Table 3: Comparative Performance Evaluation of RSA and ECIES Algorithms with Different Key Size

Algorithm	Key Size	Performance Value
RSA	2048-bit	7420.85
	3072-bit	35210.40
ECIES	244-bit	82.60
	256-bit	95.10

International Conference on Interdisciplinary Research in Science, Management, Engineering and Humanities (ICIRSMEH - 2025)
26th October, 2025, Bhubaneshwar, Odisha, India.

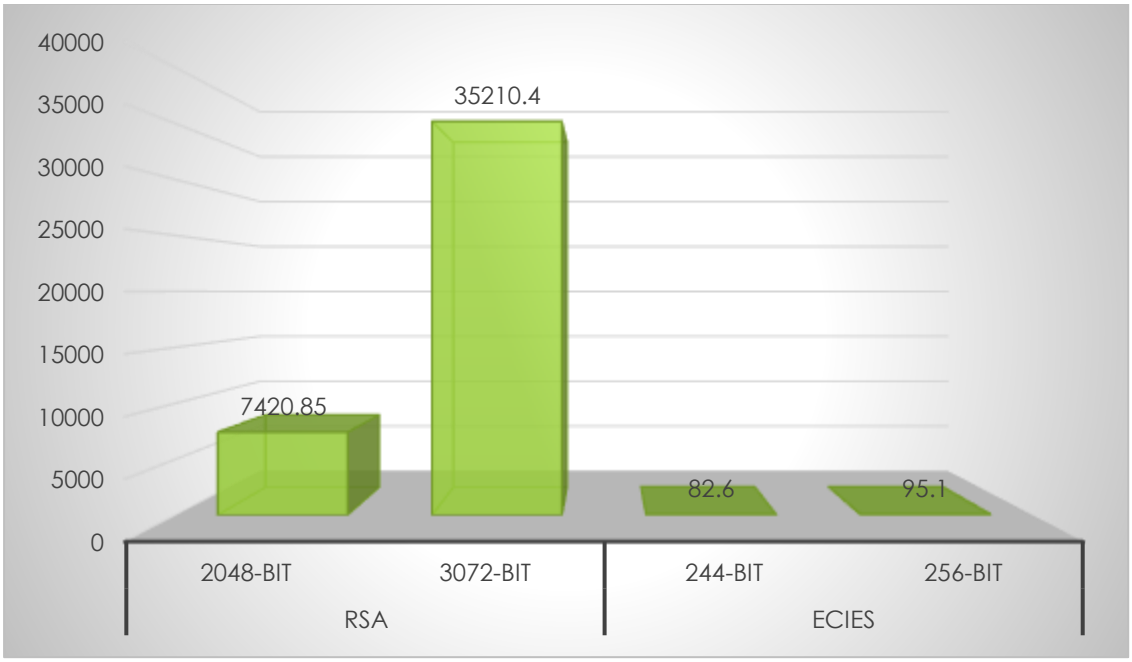

Figure 3: Comparative Performance Evaluation of RSA and ECIES Algorithms with Different Key Size

Table 3 shows the results of comparing the RSA and ECIES algorithms' performance at various key sizes. From 7420.85 at 2048 bits to 35,210.40 at 3072 bits, the data reveal that RSA's performance value grows dramatically with key size, suggesting a significant rise in computational overhead with the use of tighter security levels.

The performance numbers of ECIES, on the other hand, are substantially lower and more consistent, rising just slightly from 82.60 at 244-bit to 95.10 at 256-bit. This striking contrast illustrates how much better ECIES is than RSA in terms of efficiency and scalability, especially in settings where both processing power and reaction time are paramount.

V. CONCLUSION

This study sought to address critical performance and security issues in mobile transaction environments by developing and assessing a Secured Mobile Payment System. The proposed architecture divides the system into steps for authentication, client identification, and payment processing. This makes it possible for customers, merchants, banks, and cell carriers to talk to each other safely. Adding the Elliptic Curve Integrated Encryption Scheme considerably improves data privacy, authentication, and transaction integrity. It also helps to lower the cost of computing. When it comes to generating keys and decrypting them, RSA's computational cost goes up a lot as the key size gets bigger. The experimental study clearly reveals that ECIES is far faster than RSA. However, ECIES works well on low-powered mobile devices since it maintains operating smoothly even when the security level goes up. The results suggest that ECIES strikes a solid balance between high security and ease of use. The proposed SMPS is beneficial for real-world mobile payment systems

because it has better scalability, reduced latency, and improved security. This research contributes to the advancement of secure mobile commerce by demonstrating the efficacy of elliptic curve-based encryption inside contemporary payment infrastructures.

REFERENCES

1) J. Ntayagabiri, J. Ndikumagenge, Y. Bentaleb, and H. El Makhtoum, "Comparative analysis of elliptic curve-based cryptographic approaches for Internet of Things security," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 10, no. 6, pp. 1077–1092, 2024.
2) L. Harnaningrum and K. Mahardhian, "Comparison of mobile transaction security using NFC and QR codes," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, vol. 13, no. 4, pp. 265–271, 2024.
3) U. Musa, M. A. Adebiyi, O. Aroba, and A. Adebiyi, "RSA and elliptic curve encryption system," *International Journal of Information Security and Privacy*, vol. 18, no. 1, pp. 1–27, 2024.
4) T. Mshvidobadze, "Security issues in next generation mobile payment systems," *Economic Bulletin of Dnipro University of Technology*, vol. 77, no. 1, pp. 134–139, 2022.
5) O. Vincent, T. Okediran, A. A. Adebayo, and J. Adeniran, "An identity-based elliptic curve cryptography for mobile payment security," *SN Computer Science*, vol. 1, no. 2, pp. 1–12, 2020.
6) M. Al-Zubaidie, Z. Zhang, and J. Zhang, "Efficient and secure ECDSA algorithm and its applications: A survey," *International Journal of Communication Networks and Information Security*, vol. 11, no. 1, pp. 7–35, 2019.
7) K. Abdullah and N. Hussien, "Security improvement in elliptic curve cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 5, pp. 122–131, 2018.
8) S. Ray, G. Biswas, and M. Dasgupta, "Secure multi-purpose mobile banking using elliptic curve cryptography," *Wireless Personal Communications*, vol. 90, no. 3, pp. 1–12, 2016.
9) P. Patel, R. Patel, and N. Patel, "Integrated ECC and Blowfish for smartphone security," *Procedia Computer Science*, vol. 78, no. 1, pp. 210–216, 2016.
10) A. Maryoosh, "Data security for cloud computing based on elliptic curve integrated encryption scheme (ECIES) and modified identity based cryptography (MIBC)," *International Journal of Applied Information Systems*, vol. 10, no. 6, pp. 7–13, 2016.
11) A. Hnaif and M. Alia, "Mobile payment method based on public-key cryptography," *International Journal of Computer Networks and Communications Security*, vol. 7, no. 2, pp. 81–92, 2015.
12) S. Muthuswamy, P. Ganapathi, and S. Narayanan, "Mobile device data security: A cryptographic approach by outsourcing mobile data to cloud," *Procedia Computer Science*, vol. 47, no. 4, pp. 480–485, 2015.

13) S. Chaudhry, M. Farash, S. A. Naqvi, and M. S. Ramzan, "A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography," *Electronic Commerce Research*, vol. 16, no. 1, pp. 1–15, 2015.
14) D. Sathiya, D. T. Bai, J. Martin, and S. Rabara, "An architecture for secure mobile database transaction for corporate environment," *International Journal of Applied Engineering Research*, vol. 10, no. 5. pp. 14813–14828, 2015.
15) X. Chen and S. Zou, "A secure mobile payments protocol based on ECC," *Applied Mechanics and Materials*, vol. 1, no. 2, pp. 151–154, 2014.
16) J. Thirumal, "Framework for secure mobile banking application using elliptic curve cryptography and image steganography," *International Journal of Scientific Engineering and Research*, vol. 2, no. 4, pp. 48–50, 2014.
17) J. Tellez and S. Zeadally, "Secure mobile payment systems," *IT Professional*, vol. 16, no. 3, pp. 36–43, 2014.
18) J. Tellez and S. Zeadally, "Design, implementation, and performance analysis of a secure payment protocol in a payment gateway centric model," *Computing*, vol. 96, no. 7, pp. 1–15, 2013.
19) M. Mittal, "Performance evaluation of cryptographic algorithms," *International Journal of Computer Applications*, vol. 41, no. 7, pp. 1–6, 2012.
20) O. Vincent, O. Folorunso, and A. Akinde, "Improving e-payment security using elliptic curve cryptosystem," *Electronic Commerce Research*, vol. 10, no. 1, pp. 27–41, 2010.