International Journal of Information Security and Privacy
Volume 18 • Issue 1

RSA and Elliptic Curve Encryption System: A Systematic Literature Review

Musa Ugbedeojo, Landmark University, Nigeria
Marion O. Adebiyi, Landmark University, Nigeria
https://orcid.org/0000-0001-7713-956X
Oluwasegun Julius Aroba, Durban University of Technology, South Africa*
https://orcid.org/0000-0002-3693-7255
Ayodele Ariyo Adebiyi, Landmark University, Nigeria

ABSTRACT

Almost every living species has a motive to communicate electronically with one another and preserve data for immediate or future use. These data are becoming too large to be maintained on personal storage devices. Technological innovation has cleared the path for vast, remote storage known as the cloud. This innovation is being provided as a service to people and organizations due to the high cost of investment and the high-tech skills needed for its maintenance. Despite the many benefits of cloud computing, data privacy, integrity, and access control are issues that require immediate attention. Many studies have been conducted in order to find solutions to these challenges. In this review, the authors look at the numerous methods that have been proposed to address these security challenges. The research revealed that elliptic curve cryptography and the advance encryption system (AES) were the techniques that were most frequently used to address security issues in the digital world.

KEYWORDS

Cloud Computing, Cryptography, Cryptosystem, Elliptic, Encryption Algorithm

INTRODUCTION

Technology advancements have increased the volume of data stored by individuals and businesses. Due to the bulk, this data type could no longer be stored on microcomputers. Organizations and individuals have kept their high-volume data on a third-party cloud with ample storage capacity. While this problem has been solved for organizations and individuals, there is still the issue of data security, integrity, and access restrictions. Sebastian (2022) reported that data breaches costs the United States between $3.86 Million and $4.24 Million. The majority of these treats came from remote work. Researchers have devised several cryptographic algorithms for data security, integrity verification, and access control concerns. As technology improves daily, early cryptographic techniques appear unsuitable for modern-day advances, as various attacks (Alqahtan & Sheldon, 2022) on

DOI: 10.4018/IJISP.340728
*Corresponding Author

critical cryptographic systems have been reported. Cloud security challenges have been identified and categorized into security standards, network category, access control, cloud infrastructure, and data category (Khalil et al., 2014).

The rest of this review paper is organized as follows: We first review relevant cryptographic approaches. We then present our review methodology, outline our results and discussions, and conclude with crucial areas for additional work.

Cryptography

Cryptographic techniques have shown to be a lifesaver regarding data integrity and security. Shruthy and Maheswar (2022) defined cryptography as "the art of writing or solving codes." Cryptography conceals or changes original material into a form only the intended recipient can comprehend. Securing digital communication has proven complex, as eavesdroppers frequently hijack network traffic for nefarious purposes or as part of research. When two parties communicate via the network, a secure communication technique ensures that the conversation is secure. Cryptographic techniques safeguard the process by converting data into an unreadable form by eavesdroppers, making communication secure. Imam et al. (2021) defined encryption as "the process of transforming data into an unreadable format, and decryption is the act of converting the unreadable form back to a readable form." Many cryptographic techniques have been developed to ensure that communication between parties is secured. According to Imam et al., 2021, for any encryption technique to be secured, it must possess three important security features: confidentiality, authentication, and data integrity.

Tuteja and Shrivastava (2014) stated that based on the encryption key, two types of encryption techniques are distinguished: asymmetric (public) and symmetric (private). Symmetric encryption approaches encrypt data with a single encryption key before delivering it over the network to the intended recipient. The receiver uses the same key to decrypt the message. Although this type of encryption approach is fast, its security cannot be guaranteed because there is no secure way of sending the encryption key. The first of this type of encryption is called Data Encryption Standard (Hatzivasilis et al., 2018). Over the years, other data encryption techniques, such as 3DES, AES, RC6, RC4, Blowfish, and IDEA have been developed (Abd-Elminaam et al., 2010) to modify the flaws observed in those techniques.

The issue of exchanging keys for encryption and decryption was addressed by public key (asymmetric key) encryption. The challenge of secret key exchange without being stolen before it reaches the parties involved in communication was alleviated using an asymmetric encryption technique. Asymmetric encryption has separate encryption and decryption keys in contrast to symmetric encryption. Both the encryption and decryption systems use a set of keys. The public key is the first, while the private key is the second. When a communication is encrypted with one of the pair's keys, it can only be deciphered with the other key (Rountree, 2011). Asymmetric key algorithms are, in a strict sense, slower than symmetric key algorithms. This slow speed is partly evident because symmetric algorithms are inherently more complex, requiring more advanced techniques. Popular public key encryption algorithm examples include RSA, Diffie–Hellman key exchange, ElGamal, Digital Signature Algorithm, and Elliptic-curve.

RSA Encryption Algorithm

The Diffie-Hellman public key was the first publicly released public key algorithm, and it only enabled key exchange protocol between known participants (at least at first). ElGamal expanded it to include a full encryption and signature public key technique for ECC cryptography (Braga & de Morais, 2014). Soon after Diffie-Hellman was released, the RSA cryptosystem (Rivest Shamir Adleman) was introduced to the public (Abdullah et al., 2018). RSA algorithm provides two keys for cryptographic purposes: one for encryption called public key, published for interested parties in secure communication, and the second for decryption. Unlike the public key, the private key is kept private and used for decryption. The RSA algorithm security is founded on two separate mathematical

complexities: the RSA problem, which states that given the public key, deriving the private key cannot be computed in polynomial time, making it a computationally infeasible operation as well, and factorization of big numbers, which is computationally impossible when the numbers involved are too large (Tropea et al., 2022).

Since its first appearance, various modifications have been made to the original algorithm based on producing varying public key values (Intila et al., 2019). As a result of this enhancement, the security in this review was enhanced, with only a slight increase in encryption time and no change in decryption time (Abouelkheir & El-Sherbiny, 2022). Additionally, a study proposed by Pir (2016) outperforms the original RSA regarding security and speed by using four numbers to solve the integer n's factorization problem. Saikia (2017) presented an improved version of the original RSA algorithm; the data encryption used a dynamic key, which improved the speed of the encryption algorithm. Athukoral et al. (2022) introduced an improved RSA algorithm based on continued fractions. They improved the encryption using a similar method to padding and refined the key generation using continuous fractions. Additionally, they showed that the suggested approach is secured against the meet-in-the-middle attack, in contrast to the traditional RSA method.

Elliptic Curve Cryptography

The elliptic curve encryption algorithm is an example of public key cryptography. RSA has been used and modified since Lenstra presented the elliptic curve algorithm (Koblitz et al., 2011). This coincidental use of elliptic curves influenced Koblitz and Miller, who independently proposed using the group of points on an elliptic curve defined over a finite field in discrete log cryptosystems in 1985. (Koblitz et al., 2011). The elliptic curve algorithm has been found to have an edge over the RSA method despite some literature believing that RSA and Elliptic curve techniques have the same level of security (Yang, 2022; Rana et al., 2022; Salam & Hossen, 2021). The best-known technique for solving the ECDLP requires full exponential time, whereas RSA's IFP requires only subexponential time, the main benefit of ECC over RSA. ECC uses fewer parameters than RSA while preserving the same level of security. For instance, to get 112 bits of security using the RSA technique, a key size of 2048 bits is needed, whereas ECC calls for a key size of 224–255 bits (Mahto et al., 2016). Additionally, manufacturers of devices with limited processing and storage are drawn to it because of the compact key size (Yang, 2022). The discrete logarithm problem of an elliptic curve serves as the foundation for the security of elliptic curve encryption (Afreen & Mehrotra, 2011). Over the years, the Elliptic curve has evolved and has found many application areas. There are various variants of Elliptic curve cryptography today, each directed towards a specific purpose.

Modern Day Cryptography

Although RSA and Elliptic curve approaches have been around for decades, they remain surprisingly relevant given the fear that introducing quantum computers may end cryptography. Bernstein (2009) believed that people would conclude that cryptography is dead, as quantum computers may destroy several cryptographic algorithms such as ECDSA, RSA, and DSA. Several studies have been undertaken with quantum computers to ensure cryptography can exist in this new era. Dang et al. (2019) developed an algorithm that can withstand any attack from a quantum computer. The authors presented an implementation of a post-quantum cryptographic algorithm using three lattice-based key encapsulation mechanisms (KEMs).

Motivation

Many studies have been conducted over the years on public cryptography; between 2000 and 2023, a period of about 23 years, we found only one systematic review of the RSA Algorithm conducted by Imam et al. (2021). Also, a few systematic reviews on Elliptic Curve Cryptography were conducted. We could not find any systematic review on the hybridization of RSA and Elliptic Curve Algorithms. This prevents us from knowing the current state of research in this field and means we cannot provide

any information about it. Given this, conducting a comprehensive review of both RSA and Elliptic Curve cryptosystems is pertinent to understanding the current state of research on these two popular asymmetric cryptographic techniques.

Contribution

This systematic review has contributed to the scientific community's understanding of the current state of research in cryptography and the development of modern cryptographic techniques, especially the one coming from the amalgamation of two or more existing schemes.

RELATED WORK

In the section, related works are examined critically.

Systematic Review on RSA and Elliptic Curve Cryptography

Many reviews on various cryptographic algorithms have been conducted. While searching the database, we could only find one systematic review based on the RSA algorithm and one systematic study of Elliptic Curve cryptography. These reviews are not enough to guide a new researcher; hence, this study was initiated. Imam et al. (2021) conducted the only systematic review on RSA. The authors analyzed 90 research papers based on thorough searches of various studies and related works. The researchers classified papers into categories and compared RSA methods using parameters like encryption schemes, key features, key generation, decryption schemes, and encryption schemes.

Francia et al. (2022) reviewed the application of the elliptic curve in lightweight electronics to identify the significant application, application selection standards, and the optimal elliptic curve for lightweight devices. They stated that the Koblitz curve over prime fields is suitable for IoT devices, while processing time is a typical selection criterion, and IoT is the most widely used application of elliptic curve cryptography.

Verr et al. (2020) conducted a systematic review of Elliptic Curve Point Multiplication implementations on both FPGA and Application-Specific Integrated Circuit (ASIC) platforms (ASIC). Their research highlighted the diverse methodologies and tools for embedding ECPM into hardware systems, providing insights into the array of options for hardware designers. Most studies reviewed favored using projective coordinates alongside a polynomial basis for implementations. They also touch on socio-economic impact, noting how regulatory efforts by African governments against the dissemination of cryptographic techniques led to significant business disruptions and loss, exacerbating the challenges of the COVID-19 pandemic. However, the consensus is that projective coordinates and polynomial bases are suited for hardware adaptions of ECPM, while an efficient strategy for executing field or point multiplications is elusive. Their findings suggest that selecting algorithms, techniques, and IC technologies depends on the specific project objectives, so solution architects must consider requirements during decision-making.

Table 1. Summary of Systematic Review on RSA and ECC Encryption Algorithm

SN	Author	Year	Ref	Area	Type	Publisher
1	Imam, R., Areeb, Q. M., Alturki, A., & Anwer, F	2021	2	RSA	Journal	IEEE Access
2	Simon Francia, A., Solis-Lastra, J., & Papa Quiroz, E. A.	2021	0	ECC	Conference	Multidisciplinary International Congress on Science and Technology
3	Verr Lucca, A., Mariano Sborz, G. A., Leithardt, V. R. Q., Beko, M., Albenes Zeferino, C., & Parreira, W. D.	2020	24	ECC	Journal	Journal i of i Sensor i and i Actuator i Networks

RSA Algorithm

Rivest (1984) conducted the first review of the RSA algorithm and discussed several factors to consider while using special-purpose VLSI devices to build the RSA cryptosystem. A brief review of six RSA chips was also conducted; in his remarks, the author stated that when the RSA algorithm was first invented, there was an implementation issue; due to the technology at the time, implementing the RSA algorithm was extremely expensive, and it cost $3000 to build a TTL implementation that could handle 300 bits in length. He went on to say that at the time, the 660 bits tits implementation was well-handled on a chip. According to the author, 3-micron and higher technologies for RSA implementation may be available in the future. Mohamad et al. (2021) surveyed the RSA algorithm's trend. The authors used the RSA technique to categorize the peer-reviewed research, which included cloud computing, embedded devices, wireless sensor networks, public networks, the Internet of Things, and proxy signatures. The researchers also examined the RSA scheme's trends and performance parameters, including speed efficiency, computational complexity, security, and space.

Mumtaz and Ping (2019) reviewed 40 years of attacks on the RSA algorithm and calls for concrete examination following the underlying algebraic structure and protective measures against potential threats. The paper examines weaknesses in the relax model's use of flimsy public/private keys, the integer factorization problem, and specific low-parameter selection attacks. Such faults cannot significantly compromise the security of the RSA cryptosystem, but they can be used to investigate potential weaknesses for a deeper understanding of the underlying mathematics and erroneous parameter selection. The authors provided a concise overview of prior findings and a thorough discussion of specific attacks. A thorough analysis of all known RSA cryptosystem assaults reveals that a properly designed algorithm is impenetrable and has withstood numerous cryptanalytic attempts for the past forty years.

Al-Kaab and Belhaouar (2019) examined a variety of recommendations on how to strengthen and secure the RSA algorithm in a different review. According to the assessment, some of the methods employed in the plan include merging the RSA algorithm with the Diffie-Hellman or ElGamal algorithms, altering RSA to include three to four prime numbers, offline key storage, a dual encryption technique, and others.

Vyas and Dangra (2017) conducted a detailed study of encryption and decryption technologies, focusing on RSA improvements and summarizing less than ten variants. The writers did their review without using any research methodology and considered only a small number of papers. A summary of different simultaneous RSA technique implementations, including both software and hardware implementations, was provided by Saxena and Kapoor (2015). Parallel programming aims to use multi-core computers to execute instructions more quickly and efficiently to boost productivity and effectiveness. The authors aimed to provide future researchers with knowledge of the various parallel RSA algorithms and approaches already developed. To attain excellence and throughput in RSA and public key encryption, they investigated several concurrent RSA implementation methodologies recommended by different specialists worldwide. This study focuses exclusively on the parallel implementation feature of RSA systems.

Muhammad et al. (2014) reviewed the RSA cryptanalytic attack and discussed the concerns and obstacles associated with the RSA attack. The authors contended that the majority of the attacks are inevitable. They said the RSA method is still secure and can be trusted if correct system implementation is considered. The authors classified the attacks into three categories: attacks based on factorization techniques, attacks on the RSA function, and attacks based on extracting implementation-level features.

Asagba and Nwachukwu (2014) undertook an evaluation focused on the RSA algorithm within the scope of public key cryptography. They addressed various security issues, obstacles, and cryptographic attacks associated with RSA. The aim was to conduct an in-depth analysis of conventional RSA cryptosystems while considering several RSA variants. However, a complete literature review was not conducted.

Table 2. Summary of Reviewed Literature on the RSA Encryption Algorithm

SN	Author	Year	Ref	Review	Type	Publisher/Publication
1	Mohamad,i M.i S.i A.,i Din,i R.,i &i Ahmad,i J.i I.i	2021	2	Unsystematic	Journal	Bulletin of Electrical Engineering and Informatics
2	Mumtaz, M., & Ping, L. (2019)	2019	22	Unsystematic	Journal	Journal of Discrete Mathematical Sciences and Cryptography
3	Al-Kaabi, S. S., & Belhaouari, S. B.		2	Unsystematic	Journal	International Journal of Network Security & Its Applications
4	Vyas, C., & Dangra, J.	2017	2	Unsystematic	Journal	International Journal of Technology Research and Management.
5	Saxena, S., & Kapoor	2015	18	Unsystematic	Journal	Arxiv
6	Muhammad, S. J., Chiroma, H., & Mahmud, M.	2014	18	Unsystematic	Journal	Journal of Theoretical and Applied Information Technology
7	Asagba, P. O., & Nwachukwu, E. O. (.	2014	3	Unsystematic	Journal	West African Journal of Industrial and Academic Research
8	Rivest, R. L.	1984	54	Unsystematic	Conference	Springer

Elliptic Curve Algorithm

Takieldeen and Khalifa (2021) reviewed lightweight cryptography using elliptic curve cryptography for IoT lightweight authentication. They compared the proposals within the study to identify factors for designing a lightweight ECC scheme.

A survey of the development of Short Weierstrass elliptic curves since their emergence in cryptography was undertaken by Abhishek et al. (2021). The authors highlighted the evolutionary selection criteria of cryptographically secure elliptic curves by examining numerous attacks on elliptic curve encryption and their defenses. In their analysis, Al Saad et al. (2020) classified the Elliptic Curve into the following four groups: Basic ECC Algorithm Protocols, Algorithm Methods, ECC Applications, and Different ECC Implementations. The study also provides several graphical illustrations of cryptographic operations on EC that span infinite and finite fields. Elliptic Curve cryptography is a lightweight encryption that works well for a small number of applications, according to a survey conducted by Lara-Nino et al. (2018). Elliptic Curve cryptography is lightweight encryption that works well for a small number of applications, according to a survey conducted by Lara-Nino et al. (2018). The critical elements examined in ECC models for lightweight implementations are thoroughly assessed in representative studies. Finally, the authors defined elliptic curve lightweight cryptography's idea and standards for the first time.

Similarly, Halak et al. (2016) summarized the most cutting-edge ECC hardware implementations, particularly regarding their design objectives. A quick study is made of the hardware/software strategy's applicability concerning the security issues faced by low-end embedded devices in the Internet of Things, highlighting that ECC is susceptible to quantum assaults and offers a fix.

Hazm et al. (2015) reviewed ECP architectures, considering the design aspect of ECP and the hardware platforms used to implement them, such as field selection and algorithm for scalar multiplication. They statistically analyzed a sizable body of published material based on these characteristics. The data analysis led to several conclusions, including that binary fields are more straightforward to implement in hardware than prime fields and that polynomial structure dominates other base representations. Furthermore, given the dominance of the Lopez-Dahab Projective Coordinate, the Montgomery Scalar Multiplier was more common than the Lopez-Dahab, Binary, and NAF methods.

Thomas et al. (2014) studied various techniques for performing scalar multiplication on prime and binary fields. They claim that the Montgomery Ladder-based ECSMA saves 50% space and 45% time, driven by the Karatsuba multiplier's sub-quadratic complexity and optimized field primitives.

Gajbhiye et al. (2012) reviewed Elliptic Curve cryptography security, focusing on the performance attributes of the elliptic curve. They suggested that the Koblitz offers superior security features among the various curves and demonstrated how Koblitz curves can efficiently compute ord (p) on any curve P, facilitating an efficient derivation process. Elliptic Curve Cryptography improves the performance of the Secure Socket Layer protocol and can protect against side-channel attacks on Open SSL's implementation of the Elliptic Curve (Thomas & Sheeja, 2017).

Purpose of Hybridization Technique

Many studies have been carried out toward securing data, while some are directed toward securing infrastructure. Among the reviewed papers, a few of them are listed below:

Panda and Chattopadhyay (2017) demonstrated Hybrid RSA (HRSA). The new system does not integrate different algorithms but improves on existing ones. The new approach uses M, a combination of four prime numbers, to generate "public key" (P) and "private key" (Q). Factorization of the variable M becomes increasingly challenging. Furthermore, the computation of P and Q entails computing some additional intermediate elements, which increases the complexity of the computation. The suggested approach provides a more secure route for the encryption and decryption operations and is more effective than conventional RSA and ERSA procedures, based on the evaluation of "key generation time," "encryption speed," and "decryption speed."

Mahalle and Shahade (2014) describe a new encryption algorithm that utilizes the RSA and AES encryption algorithms to protect data on the cloud. The new method was created to improve secure data upload to the cloud, protect the integrity of uploaded data, and ensure proper usage and distribution of public, private, and secret keys. The new system accomplished this by employing three distinct keys for encryption and decryption. One of the keys is the public key, and the other is the secret key. The benefit of this scheme is that keys are produced based on system time, avoiding guesswork by intruders, thereby increasing the security of the new scheme and eliminating the possibility of a repeat or redundant key.

Table 3. Summary of Reviewed Papers on Elliptic Curve Cryptography

SN	Author	Year	Ref	Review	Type	Publisher/Publication
1	Takieldeen, A. E., & Khalifa, F.	2021	0	Unsystematic	Journal	Journal of Intelligent Systems and Internet of Things
2	Abhishek, K., & Raj, E. G. D. P.	2021	0	Unsystematic	Journal	Cybernetics and Information Technologies
3	Al Saadi, M., Muscat, O., & Kumar, B.	2020	0	Unsystematic	Journal	Journal of Future Generation Communication and Networking,
4	Lara-Nino, Carlos Andres, Arturo Diaz-Perez, and Miguel Morales-Sandoval.	2018	62	Unsystematic	Journal	IEEE Access
5	Halak, B., Waizi, S. S., & Islam, A.	2016	9	Unsystematic	Journal	Cryptology ePrint Archive
6	Hazmi, I. H., Zhou, F., Gebali, F., & Al-Somani, T. F.	2015	26	Unsystematic	Conference	IEEE
7	Thomas, C., Sheela, G., & Krishnan, S.	2014	26	Unsystematic	Journal	Int. J. Comput. Sci. Inform. Technol
8	Gajbhiye, S., Karmakar, S., Sharma, M., Sharma, S., & Kowar, M. K.	2012	10	Unsystematic	Journal	International Journal of Computer Science and Information Technologies.
9	Thomas M. Cim & Sheeja S.	2017	0	Unsystematic	Journal	International Journal of Control Theory and Applications.

Moghaddam et al. (2013) presented a hybrid asymmetric-key encryption scheme based on RSA Small-e and Efficient RSA in response to the security concerns in cloud computing environments. In contrast to the original RSA, the new technique increased the exponents to three and employed a two-step encryption process to strengthen the algorithm's security. Given the security level and effectiveness of HE-RSA, the simulation results show that the overall computation time in HE-RSA decreased by almost 50% compared to the original RSA.

In its most recent versions, Bluetooth security is compromised of 128-bit AES encryption. Albahar et al. (2018) developed a triple technique based on RSA, AES, and TwoFish to enhance Bluetooth security (Bluetooth 4.0 - 5.0). Older Bluetooth 1.0A to 3.0 + HS devices encrypt data using the E0 stream cipher, which numerous studies have shown inadequate for modern high-security requirements. The message was first encrypted with AES using a 128-bit key, and then it was encrypted once more using Twofish using the same 128-bit key. To protect the initial 128-bit key during over-the-air transfer, it was finally encrypted using RSA with a 1024-bit key. At the receiving end is the decryption process. The novel approach improved Bluetooth encryption security by removing all known weaknesses, making packet forwarding between Bluetooth devices secure, as the authors showed using experimental figures.

Abdalwahid et al. (2019) introduced a hybrid technique utilizing two well-known public key cryptography algorithms to encrypt data stored in HDFS (RSA and Paillier), encrypting data before being posted to HDFS. The proposed system has higher computational cost and lower latency than the RSA cryptosystem alone.

Rege et al. (2013) proposed a hybrid encryption system based on RSA and AES to enhance Bluetooth communication security for data transmission. The suggested approach used the RSA algorithm to encrypt the AES key due to its advantages in key management and the AES algorithm for data transmission due to its superior efficiency in block encryption compared to the E0 encryption algorithm. Thus, Bluetooth data transmission is more secure due to the dual protection that uses the AES and RSA algorithms, providing a straightforward and practical way to encrypt transmitted data.

A lightweight and effective Secure Hybrid RSA (SHRSA) messaging technique with a four-layered authentication stack was introduced by Bhattacharjya et al. (2019). With this method, RSA's asymptotic prolonged decryption performance, computational modular exponentiation cost, and partial key exposure vulnerability issues were all attempted to be resolved. Thanks to its own four mechanisms, this system has done away with the need for any password, external digital certificates, or a third party for authentication. The approach also uses 1-3 percent less memory and 2-4 percent less CPU than primary RSA while resolving many scientific problems associated with RSA. Compared to the primary RSA and CRT RSA, its average decryption time has grown by 8.858 and 2.248 times, respectively. The decryption throughput of SHRSA is 8.5345 times faster than primary RSA and 2.1174 times faster than CRT-RSA compared to RSA and CRT-RSA, which all have throughputs of roughly 6 KB/Sec.

Santoso (2021) devised a hybrid form of RSA and the hill cipher. The author illustrated how hybrid hill cipher cryptography, which uses RSA with 512-bit and 3x3 matrix keys to secure data transmission and prevent unauthorized parties from reading delivered messages, can address security issues. Similarly, Kadam and Khairnar (2015) proposed a method using hybrid encryption, which can be used as end-to-end encryption or in addition to current SSL, to increase data security. Data transfer security between two clients increases when a web service is used as an intermediary. The content block is encrypted using the suggested method, and only the client—not the web server—can decrypt it.

A novel biometric security protocol based on a hybrid encryption unique approach offers an efficient and effective mechanism for the secrecy and authentication of biometric security systems using RSA and a fundamental symmetric key method (Nasir & Kuppuswamy, 2013). Among several methods and characteristics for coping with variations in biometric attributes, a proposed combination of biometric traits addresses common problems with a biometric scheme for authentication.

METHODOLOGY

Imam et al. (2021) assert that a well-designed survey thoroughly analyzes all previous research on the topic or area of interest. A methodical review of the literature provides insight into a complete examination of current literature relevant to various issue formulations (Murt et al., 2021). An extensive search was undertaken to conduct a study on some of the most important and widely used websites and scientific databases, notably Google Scholar, IEEEXplore, ScienceDirect, Ijoti, Academic, Githumb, Researchgate, SpringerLink, Citeseerx, Arxiv, F1000Research, Wiley Online Library, and Microsoft Academy.

Research Questions

The following research questions were developed to gather data from the literature:

RQ1 What is the motive behind the hybridization technique in cryptology?
RQ2 What is the yearly coverage of research in hybridization in cryptography?
RQ3 What are the minimum techniques that have ever been combined for hybridization purposes?
RQ4 Which of the cryptographic techniques gets more attention?

Search Database

The following databases were searched to get a comprehensive list of studies conducted on RSA and Elliptic curve algorithms, in addition to two search engines (google scholar and Microsoft Academic):

1. Researchgate.net
2. IEEExplore
3. SpringerLink (mostly monetized)
4. Citeseerx
5. Sciencedirect (sometimes monetized)
6. arxiv
7. F1000Research
8. Wiley Online Library (Monitized)

Search Criteria

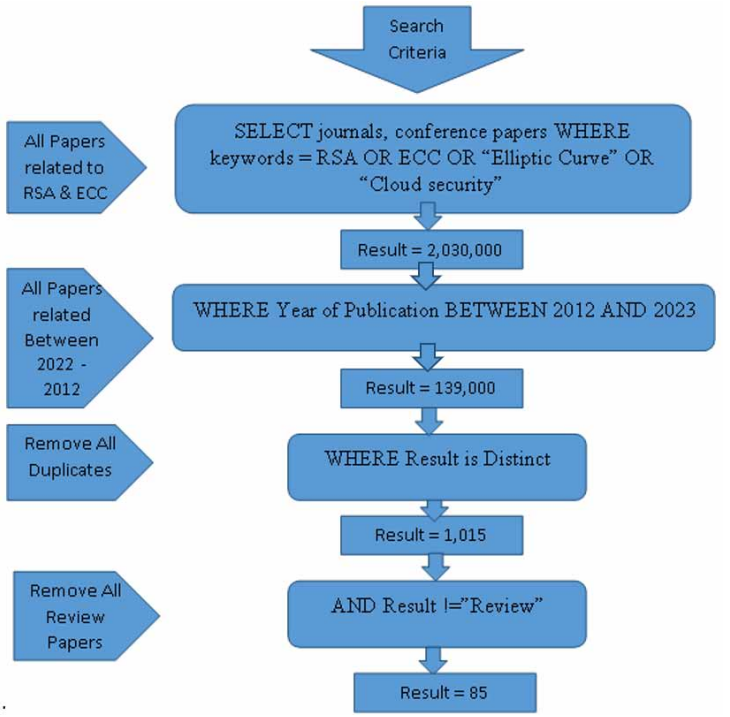
Several search criteria were formulated and combined to get the relevant papers for this review. These criteria are illustrated in Figure 1.

Inclusion Criteria

We searched for all papers related to RSA, ECC, Elliptic Curve, and cloud security. All these keywords are contained a single command called criterial1, which produced 2,030,000 papers.

```
Criteria 1
SELECT journals, conference papers WHERE keywords = RSA OR ECC OR
"Elliptic Curve" OR "Cloud security" WHERE Year of Publication
BETWEEN 2012 AND 2023 {
                Result+=result;
        }
        Return result;
```

Figure 1. Search Criteria



Exclusion Criteria

Another criteria was formulated to reduce this number by removing older papers since we are looking at research conducted within the last ten years (criteria2). This reduced the result to 139,000. Similarly, criteria3 removed duplicates since these papers came from different database and search engines, reducing our total to 1015 papers. Finally, criteria4 extracted only review papers giving us 85 papers.

```
Criteria 2
SELECT FROM result WHERE content = "Abstract"{
        Result+=result;
}
Return result;
Criteria 3
SELECT DISTINCT FROM result {
        Result+=result;
}
Criteria 4
SELECT FROM result WHERE content != "Review" {
        Result+=result;
}
Return result;
```

RESULTS AND DISCUSSION

The 80 papers in Table 4 were the shortlisted papers that met the criteria and were reviewed.

Table 4. List of Papers Reviewed

SN	AUTHOR(S)	YEAR	PUBLISHER	TYPE	APPLICATION	METHODOLOOGY
1	Taha, A. A., Elminaam, D. S. A., & Hosny, K. M.	2018	Far East Journal of Electronics and Communications	Journal	Cloud Computing	3DES, AES, DES, RSA, Krisha
2	Subramanian, K., John, F. L., & John, F. L.	2018	International Journal of Advanced and Applied Sciences	Journal	Cloud Computing	3DES, RSA
3	Panda, P. K., & Chattopadhyay, S.	2017	ICACCS	Conference	Text encryption	4 Prime Numbers
4	Malik, A., & Jain, V. K.	2016	Int. J. Intel. Eng. Syst	Journal	Cloud computing	ABC, RSA
5	Mateescu, G., & Vladescu, M.	2013	Federated Conference on Computer Science and Information Systems	Conference	Cloud computing	AES MD5, RSA
6	Akomolafe, O. P., & Abodunrin, M. O.	2017	Journal of Computer Network and Information Security	Journal	Cloud Computing	AES, Blake2b, Schnorr
7	El_Deen, A. E. T.	2013	International Journal of Scientific & Engineering Research	Journal	Text encryption	AES, Blowfish
8	AbdElminaam, D. S. (2018).	2018	Journal of Electronics and Information Engineering	Journal	Cloud Computing	AES, Blowfish
9	Siregar, R.	2018	In Journal of Physics: Conference Series	Journal	Medical Record	AES, Blowfish
10	Le, D. N., Seth, B., & Dalal, S.	2018	Journal of Cyber Security and Mobility		Cloud Computing	AES, Blowfish, Diffie–Hellman, RSA
11	Jabbar, A., & Lilhore, P. U.	2017	International Journal Online of Science	Journal	Cloud computing	AES, Blowfish, EC-RSA, SHA256
12	Kvyetnyy, R. N., Romanyuk, O. N., Titarchuk, E. O., Gromaszek, K., & Mussabekov, N.	2016	In Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments	Conference	Cloud computing	AES, Deffi-Hellman
13	Gutub, A. A. A., & Khan, F. A. A.	2012	International conference on advanced computer science applications and technologies	Journal	Text Encryption	AES, DES, RSA
14	Bhatele, K., Sinhal, A., & Pathak, M.	2012	IEEE International Conference on Advanced Communication Control and Computing Technologies	Journal	Network	AES, Dual RSA MD5
15	Iyer, S. C., Sedamkar, R. R., & Gupta, S.	2016	Procedia Computer Science	Conference	Network	AES, ECC
16	Rezai, A., Keshavarzi, P., & Moravej, Z.	2016	Security and communication networks	Journal	Network	AES, ECC
17	Rajput, U., Abbas, F., Eun, H., & Oh, H.	2017	IEEE Access	Journal	VANET	AES, ECC
18	Al-Attab, B. S., & Fadewar, H. S.	2018	Sinhgad Institute of Management & Computer Application.	Journal	Cloud computing	AES, ECC
19	Prakash, S., & Rajput, A.	2018	Ambient Communications and Computer Systems	Journal	Wireless Sensor	AES, ECC
20	Orobosade, A., Aderonke, T., Boniface, A., & Gabriel, A. J.	2020	Communications	Journal	Cloud computing	AES, ECC

continued on following page

Table 4. Continued

SN	AUTHOR(S)	YEAR	PUBLISHER	TYPE	APPLICATION	METHODOLOOGY
21	Hafsa, A., Sghaier, A., Zeghid, M., Malek, J., & Machhout, M.	2020	International Journal of Information and Computer Security	Journal	Network	AES, ECC
22	Kumar, H.	2021	Turkish Journal of Computer and Mathematics Education	Journal	IoT	AES, ECC
23	Hafsa, A., Gafsi, M., Malek, J., & Machhout, M.	2021	Cryptography-Recent Advances and Future Developments. IntechOpen.	Conference	Text encryption	AES, ECC
24	Rehman, S., Talat Bajwa, N., Shah, M. A., Aseeri, A. O., & Anjum, A.	2021	Electronics	Journal	Cloud Computing	AES, ECC
25	Chen, Y., Liu, H., Wang, B., Sonompil, B., Ping, Y., & Zhang, Z.	2021	Journal of Cloud Computing	Journal	Cloud computing	AES, ECC
26	Hosam, O., & Ahmad, M. H.	2019	Int. J. Comput. Sci. Eng	Journal	Cloud computing	AES, ECC, LSB
27	Mostafaa, H., Eisaa, S. M., Issaa, H. H., & Shaker, N. H.	2021	Materials Science and Engineering	Journal	IoT	AES, ECDH
28	Parenreng, J. M., & Wahid, A.	2022	Internet of Things and Artificial Intelligence Journal	Journal	E-mail	AES, El-Gamal
29	Harba, E. S. I.	2017	Engineering, Technology & Applied Science Research	Journal	Text encryption	AES, HMAC, RSA
30	Nasir, M. S., & Kuppuswamy, P.	2013	Innovative Research in Computer and Communication Engineering	Journal	Biometric	AES, RSA
31	Rege, K., Goenka, N., Bhutada, P., & Mane, S.	2013	International Journal of Computer Applications	Journal	Bluetooth	AES, RSA
32	Mahalle, V. S., & Shahade, A. K.	2014	IEEE	Conference Paper	Cloud computing	AES, RSA
33	Kuswaha, S., Waghmare, S., & Choudhary, P.	2015	International Journal on Recent and Innovation Trends in Computing and Communication	Journal	Network	AES, RSA
34	AbdElnapi, N. M., Omara, F. A., & Omran, N. F.	2016	International Journal of Computer Science and Information Security	Journal	Cloud Computing	AES, RSA
35	Brousmiche, K. L., Durand, A., Heno, T., Poulain, C., Dalmieres, A., & Hamida, E. B.	2018	International Conference on Internet of Thing IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data	Conference	Blockchain	AES, RSA
36	Biswas, C., Gupta, U. D., & Haque, M. M.	2019	International Conference on Electrical, Computer and Communication Engineering	Journal	Text Encryption	AES, RSA
37	Issad, M., Anane, N., Bellemou, A. M., & Boudraa, B.	2020	Data Communication. Malaysian Journal of Computing and Applied Mathematics	Journal	Network	AES, RSA
38	Mantoro, T., & Zakariya, A.	2012	TELKOMNIKA Indonesian Journal of Electrical Engineering	Journal	E-mail	AES, RSA, SHA

continued on following page

Table 4. Continued

SN	AUTHOR(S)	YEAR	PUBLISHER	TYPE	APPLICATION	METHODOLOOGY
39	Kadam, K. G., & Khairnar, V	2015	International Journal of Technical Research and Applications	Journal	Web Services	AES, RSA, SHA256
	Albahar, M. A., Olawumi, O., Haataja, K., & Toivanen, P.	2018	Journal of Information Security	Journal	Bluetooth	AES, RSA, TwoFish
40	Mateescu, G., & Vladescu, M.	2013	Federated Conference on Computer Science and Information Systems	Conference	Web Service	AES, SOAP/XML, SHA1
41	Patel, P., Patel, R., & Patel, N.	2016	Procedia Computer Science	Conference	Mobile Phone	Blowfish, ECC
42	Chinnasamy, P., Padmavathi, S., Swathy, R., & Rakesh, S.	2021	Inventive Communication and Computational Technologies	Journal	Cloud Computing	Blowfish, ECC
43	Kaur, J., & Garg, D. S.	2015	Journal of Engineering Research and General Science,	Journal	Cloud Computing	Blowfish, RSA
44	Thillaiarasu, N., Chenthur Pandian, S.,Naveeni Balaji G.,Benithai Shierly,R. M., Divya,A.,& Divya Prabha,G.	2018	International conference on intelligent data communication technologies and internet of things	Conference	Cloud Computing	Blowfish, RSA, SHA3
45	Safiraa, M. O., & Mogi, I. K. A.	2020	Jurnal Elektronik Ilmu Komputer Udayana	Journal	IoT	Cipher, RSA, Vigenere
46	Sharma, S., & Chopra, V.	2017	International Journal of Security and Its Applications	Journal	Text encryption	DES, ECC
47	Hoobi, M. M.	2020	Journal of Southwest Jiaotong University	Journal	Text Encryption	DES, ECC
48	Panse, T., & Kapoor, V.	2012	International Journal of Computer Applications	Journal	Bluetooth	DES, MD5, RSA
49	Rani, S., & Gangal, A.	2012	International journal of computer science and information technologies	Journal	Cloud computing	DES, MD5, RSA
50	Prakash, S., & Purohit, M.	2013	International Journal of Information Communication and Computing Technology	Journal	Text encryption	DES, RSA
51	Adedej Kazeem, B., & Akinlolu, P. (2014).	2014	International Journal of Scientific & Engineering Research	Journal	Network	DES, RSA
52	Kapoor, V., & Yadav, R.	2016	International Journal of Computer Applications	Journal	Network	DES, RSA, SHA1
53	Bodkhe, M. R., & Jethani, V.	2015	International Journal of Engineering, Science and Mathematics	Journal	Text Encryption	Diffie-Hellman, IRSA
54	Agrawal, A., & Patankar, G.	2016	International Research Journal of Engineering and Technology	Journal	Network	Diffie-Hellman, RC5, RSA, SHA1
55	Deshmukh, S., & Patil, R.	2014	Int. J. Comput. Sci. Inf. Technol	Journal	Text Encryption	Diffie-Hellman, RSA
56	Moghaddam,F.F.,Varnosfaderan, S. D., Ghavam,I., & Mobed, S.	2013	IEEE Student Conference on Research and Development	Conference	Cloud computing	Diffie-Hellmani RSA small-e
57	Barman, P., & Saha, B.	2015	International Research Journal of Computer Science	Journal	Network	DNA, ECC
58	Rizk, R., & Alkady, Y.	2015	Journal of Electrical Systems and Information Technology	Journal	Wireless Network Sensor	ECC, Dual RSA, MD5

continued on following page

Table 4. Continued

SN	AUTHOR(S)	YEAR	PUBLISHER	TYPE	APPLICATION	METHODOLOOGY
59	Almaiah, M. A., Dawahdeh, Z., Almomani, O., Alsaaidah, A., Al-Khasawneh, A., & Khawatreh, S.	2020	Int. J. Electr. Comput. Eng.	Journal	Text encryption	ECC, Hill Cipher
60	Rajavarman, R.	2021	Turkish Journal of Computer and Mathematics Education	Journal	Cloud Computing	ECC, Honey
61	Takieldeen, A., Abd Elkhalik, S. H., Samra, A. S., Mohamed, M. A., & Khalifa, F.	2021	Information	Journal	Multimedia	ECC, Ong Schnorr, Shamir
62	Elkamchouch, H. M.,Takieldeen, A. E., & Shawky, M. A.	2018	International Conference on Electrical and Electronic Engineering	Journal	Network	ECC, Ong, Schnorr, OSS
63	Eltaib, H. A., AbdelRassoul, R., & Zaghloul, M. S.	2020	Journal of Physics: Conference Series	Journal	Network	ECC, Ong, Schnorr, Shamir Digital Signature Scheme
64	Tripathy, A., Pradhan, S. K., Tripathy, A. R., & Nayak, A. K.	2021	Int. J. Innovative Technol. Exploring Eng.		wireless sensor network	ECC, RC4
65	Tripathy, A., Tripathy, A. R., Rath, S., Jena, O. P., & Swagatika, S.	2021	Intelligent and Cloud Computing	Conference	Cloud Computing	ECC, RC4
66	Tayel, M., Dawood, G., & Shawky, H.	2018	International conference on advances in computing, communications and informatics	Conference	IoT	ECC, Serpent
67	Siva, S. P., & Kirubanand, V. B.	2019	International Journal of Electrical and Computer Engineering	Journal	Cloud Computing	ECC, TwoFish
68	Arora, S. & Pooja	2015	International Journal of Computer Applications	Journal	Text encryption	El-Gamal, RSA
69	Rehman, E., Asad, M., & Sher, M.	2015	VFAST Transactions on Software Engineering	Journal	Wireless Sensor	HECC, Synchription
70	Santoso, Y. S.	2021	Journal Matematika Dan Ilmu Pengetahuan Alami LLDikti Wilayah	Journal	Messaging	Hill Cipher RSA
71	Shehzad, D., Khan, Z., Dag, H., & Bozkus, Z.	2016	International Journal of Computer Science and Information Security	Journal	Cloud computing	Image key, RSA
72	Bhattacharjya, A., Zhong, X., & Li, X.	2019	IEEE Access,	Journal	Virtual Private Network	Layered RSA
73	Zhang, F., Chen, Y., Meng, W., & Wu, Q.	2019	International Journal of Database Management Systems	Journal	Cloud Computing	P-AES, RSA
74	Abdalwahid, S. M. J., Yousif, R. Z., & Kareem, S. W.	2019	Applied Computer Science	Journal	Hadoop	Paillier, RSA
75	Xavier, A. P., & Kesavan, R. (2022).	2022	IETE Journal of Research	Journal	Big data	PSO/CS, ECC
76	Kaur, S., Bharadwaj, P., & Mankotia, S.	2017	International Journal of Computer Network and Information Security	Journal	Text Encryption	RSA and DES
77	Jamaludin, J., & Romindo, R.	2020	International Journal of Information System & Technology	Journal	Text Encryption	RSA, Vigenere Cipher
78	Rahmadani, R., & Mawengkang, H.	2018	Journal of Physics: Conference Series	Journal	Text Encryption	RSA–CRT optimization, VMPC

continued on following page

Table 4. Continued

SN	AUTHOR(S)	YEAR	PUBLISHER	TYPE	APPLICATION	METHODOLOOGY
79	Moghaddam, F. F., Alrashdan, M. T., & Karimi, O.	2013	Journal of advances in Computer Network	Journal	Cloud computing	Small-e, RSA
80	Sihombing, G. L. A.	2017	InfoTekJar:i Jurnali Nasionali Informatikai dani Teknologii Jaringan	Journal	Text Encryption	Stream Cipher, RSA
81	Alanzy, M., Alomrani, R., Alqarni, B., & Almutairi, S.	2023	Applied Sciences	Journal	Cloud Computing	AES and Blowfish
82	Kuppuswamy, P., Al, S. Q. Y. A. K., John, R., Haseebuddin, M., & Meeran, A. A. S.	2023	Bulletin of Electrical Engineering and Informatics	Journal	Communication and Financial Transactions	RSA and SSK
83	Somaiya, R., Gonsai, A., & Tanna, R.	2023	International Journal of electrical and computer engineering systems	Journal	Multimedia File Encryption	Modified AES and ECC
84	Zhao, J.	2023	IEEE	Conference	Communication	DES and RSA
85	Hameed, M. I., & Hoomod, H. K.	2023	AIP Publishing.	Conference Proceeding	Cloud Computing	chaotic system and mCrypton-salsa20 algorithms

Population of Hybridization of various encryption techniques by Year

Researchers worldwide continue to undertake daily studies to ensure cloud servers are carefully secured using various encryption techniques. Figure 2 depicts the distribution of various hybrid techniques carried out year-by-year between 2012 and 2022. We can observe that the highest research was conducted in 2018, followed by 2021, showing that various hybridizations approaches remain new, and researchers are still working diligently to ensure appropriate encryption techniques are used and developed to protect server data.

Hybridization Technique

Hybridization technique is a method of combining more than one techniques to develop a new technique. In this review, out of the 85 papers reviewed, 23 studies combined more than two techniques, two combined variants of the same technique, while 59 studies combined two cryptographic techniques to form a new technique. The majority of the hybridization techniques were carried out by combining symmetric and asymmetric techniques.

Cryptographic Techniques by Population

Figure 4 depicts the distribution of different encryption algorithms that have been merged to build a new methodology. According to the graph, Advance Encryption Standard (AES) and Elliptic Curve

Figure 2. Distribution of Hybrid Encryption Techniques by Year

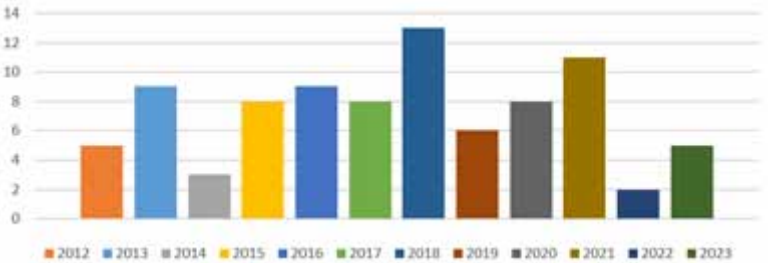
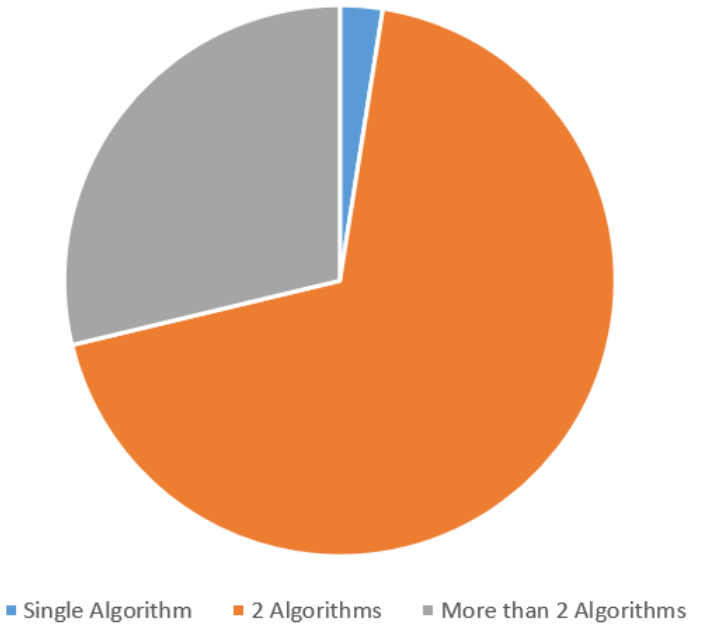


Figure 3. Hybrid Techniques Distribution by Number of Algorithms



Cryptography (ECC) have been researched and combined to create new hybrid encryption techniques; the combination is most common, followed closely by Rivest Shamir Adleman (RSA) combined with Advance Encryption Standard (AES) (AES).

Furthermore, the Advance Encryption Standard and Blowfish algorithms (El Deen, 2013; AbdElminaam, 2018; Siregar, 2018) have been investigated and merged to create a new cryptographic technique. Similarly, the academic community has focused on the Data Encryption Standard and the RSA algorithms (Prakash & Purohit, 2013; Adedeji & Akinlolu, 2014). Likewise, Blowfish and Elliptic Curve Cryptography (ECC) were researched and merged (Patel et al., 2016; Chinnasamy et al., 2021), while DES, MD5, and RSA (Panse & Kapoor, 2012; Rani & Gangal, 2012) were studied and integrated in several publications. Several researchers have coupled RC4 and ECC (Tripathy et al., 2021; Tripathy et al. 2021), and DES and ECC (Sharma & Chopra, 2017; Hoobi, 2020), to create hybrid encryption schemes.

Most Commonly Used Technique for Hybridization

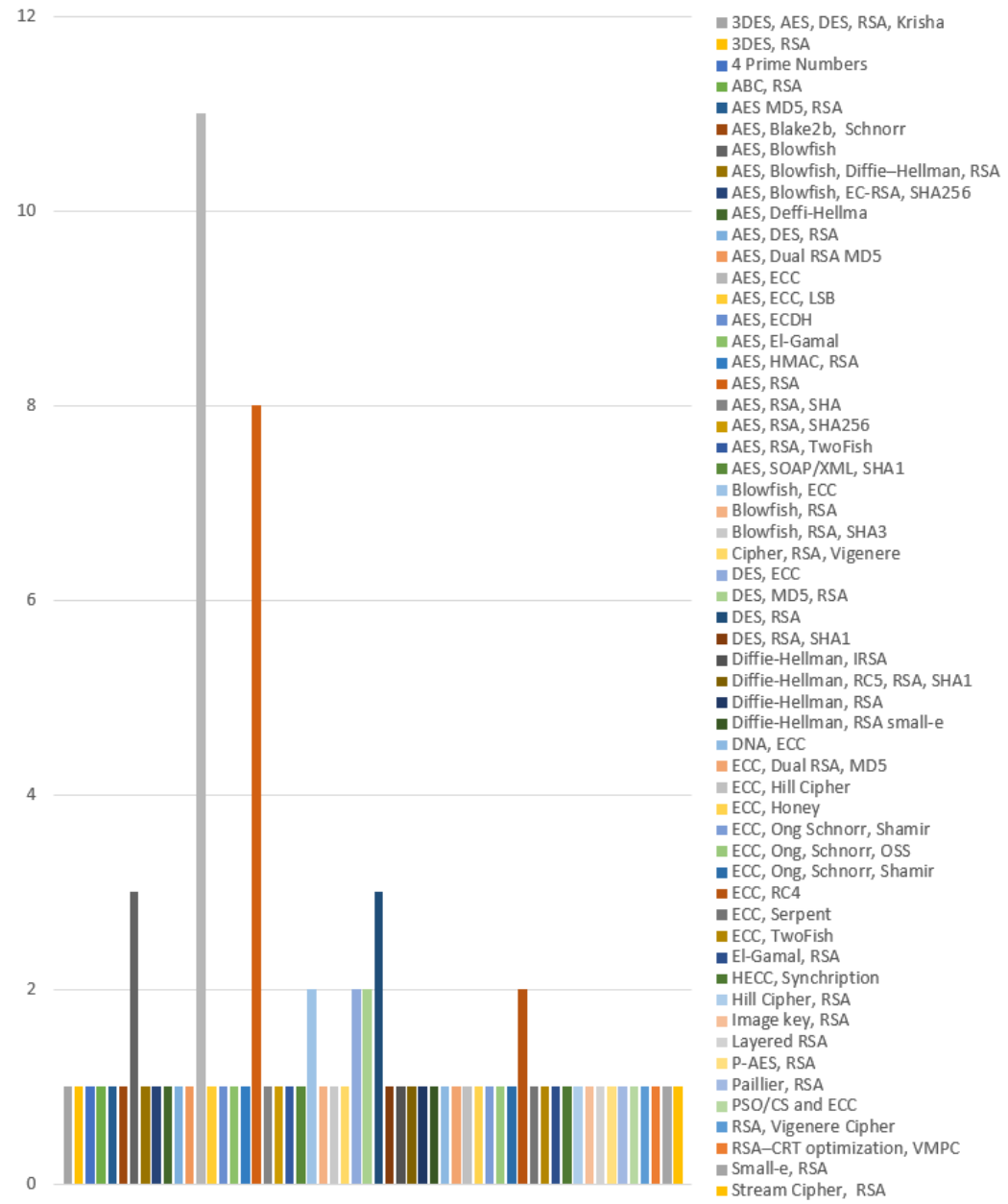
Here, we mentioned only three algorithms with the highest appearances within the 81 papers reviewed. As indicated in Table 3 and Figures 4 and 5, the Advanced Encryption Standard (AES) is the most commonly used algorithm for hybridization. AES is a symmetric algorithm, mostly combined with asymmetric algorithm(s). Elliptic Curve Cryptography is the second most used algorithm for hybridization (Figures 4 and 5 and Table 3). Finally, another example of public cryptography, RSA, is third-ranked and is frequently combined with asymmetric encryption (Figures 4 and 5 and Table 3).

Application Areas

All studies on hybrid encryption are directed toward a particular direction or are designed to solve a particular problem. In this section, we have analyzed these studies based on the area of application.

Various application areas have been identified, such as Big Data, Biometric, Blockchain, Bluetooth, Cloud Computing, Email, Hadoop, IoT, Medical Record, Messaging, Mobile Phone,

Figure 4. Hybrid Techniques Distribution by Various Encryption Techniques



Multimedia, Network, Text Encryption, and VANET. Cloud computing has the highest number (27 studies), closely followed by Text Encryption (18 studies). While the list of study areas that have been the least researched include Big Data, Biometric, Blockchain, Hadoop, Medical Records, Messaging, Mobile Phones, Multimedia, VANET, Virtual Private Networks, and Wireless Sensor Networks. From this, we can deduce that various research has been undertaken to ensure the security of files stored on the cloud and the infrastructure has been undertaken. However, as frequent and various attacks are recorded on cloud servers, this is insufficient (Somani et al., 2017; Abusaimeh, 2020; Gill et al., 2019).

Figure 5. Distribution of Hybrid Techniques by Popularity

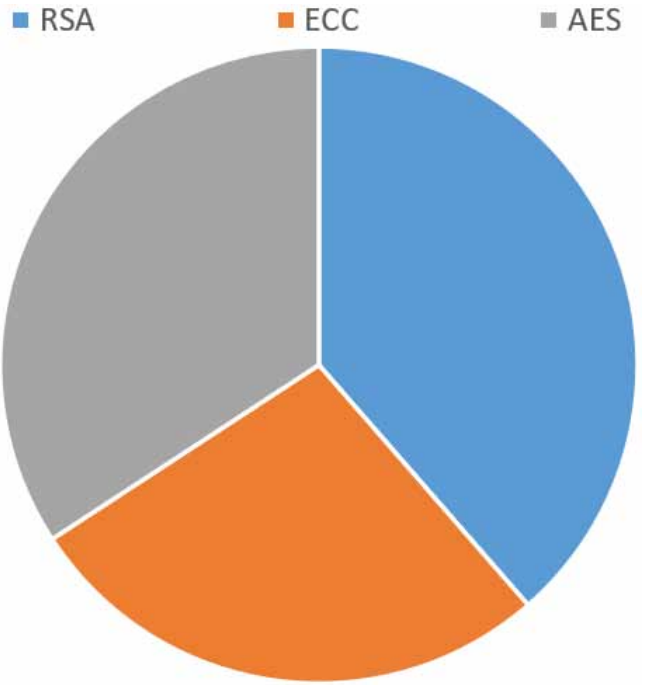
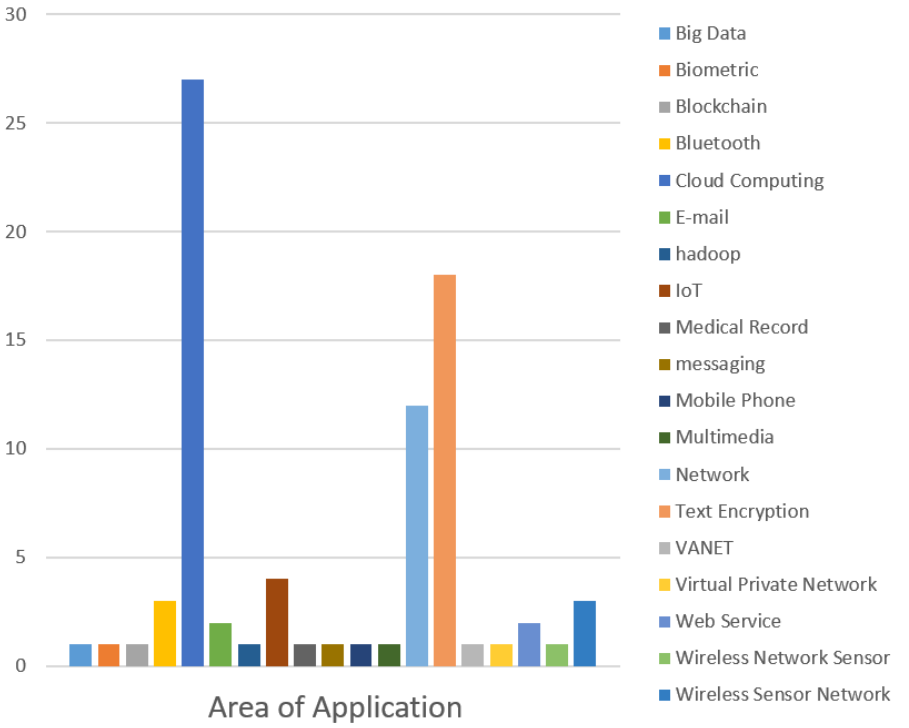


Figure 6. Research Distribution by Area of Application



CONCLUSION

The most well-known method for protecting digital data is cryptography. This has been used to protect the privacy, authenticity, and integrity of data transmitted through networks. While different cryptographic techniques have already been applied, many have been ineffectual due to advancements in computer technology and hacking strategies, prompting the academic community to launch several projects to enhance the security of data communicated across networks. Such research can require developing a new technique or combining several others.

The RSA and ECC algorithms have been extensively researched and used to secure data and information transfer in many scenarios, including key exchanges, cloud servers, networking protocols, and any other situation needing secure communication between two parties.

According to the findings of this study, the most hybridization occurred between symmetric and asymmetric cryptography. This motivated us to research the hybridization of two public asymmetric cryptography techniques, RSA and ECC. Furthermore, we discovered that, despite increased interest in cloud computing, there is still a need for additional research in this area.

The result shows that the Advanced Encryption Standard (AES) has the highest number of hybridizations, followed by Elliptic Curve Cryptography, while the RSA algorithm came third. This result shows that Asymmetric algorithms (such as RSA and ECC) are more often hybridized with another asymmetric algorithm than a symmetric one.

ABBREVIATIONS

ECDH Elliptic Curve Diffie-Hellman
RC 4 Rivest Cipher 4
PSO Particle Swarm Optimization
CS Cuckoo Search
ECC Elliptic Curve Cryptography
DES Data Encryption Standard

REFERENCES

Abd Elminaam, D. S., Abdual-Kader, H. M., & Hadhoud, M. M. (2010). Evaluating the performance of symmetric encryption algorithms. *International Journal of Network Security*, *10*(3), 216–222.

Abdalwahid, S. M. J., Yousif, R. Z., & Kareem, S. W. (2019). Enhancing approach using hybrid pailler and RSA for information security in bigdata. *Applied Computer Science, 15*(4).

AbdElminaam, D. S. (2018). Improving the security of cloud computing by building new hybrid cryptography algorithms. *International Journal of Electronics and Information Engineering*, *8*(1), 40–48.

AbdElnapi, N. M., Omara, F. A., & Omran, N. F. (2016). A hybrid hashing security algorithm for data storage on cloud computing. *International Journal of Computer Science and Information Security*, *14*(4).

Abdullah, K. M., Houssein, E. H., & Zayed, H. H. (2018). New security protocol using hybrid cryptography algorithm for WSN. *2018 1st International Conference on Computer Applications & Information Security (ICCAIS),* 1-6.

Abhishek, K., & Raj, E. G. D. P. (2021). Evaluation of computational approaches of short Weierstrass elliptic curves for cryptography. *Cybernetics and Information Technologies*, *21*(4), 105–118. doi:10.2478/cait-2021-0045

Abouelkheir, E., & El-Sherbiny, S. (2022). *Enhancement of speech encryption/decryption process using RSA algorithm variants*. Academic Press.

Abusaimeh, H. (2020). Security Attacks in Cloud Computing and Corresponding Defending Mechanisims. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(3), 4141–4148. doi:10.30534/ijatcse/2020/243932020

Adedeji Kazeem, B., & Akinlolu, P. (2014). A new hybrid data encryption and decryption technique to enhance data security in communication networks: Algorithm development. *International Journal of Scientific and Engineering Research*, *5*(10).

Afreen, R., & Mehrotra, S. C. (2011). *A review on elliptic curve cryptography for embedded systems.* arXiv.

Agrawal, A., & Patankar, G. (2016). Design of hybrid cryptography algorithm for secure communication. *International Research Journal of Engineering and Technology*, *3*(01), 2395–0056.

Akomolafe, O. P., & Abodunrin, M. O. (2017). A hybrid cryptographic model for data storage in mobile cloud computing. *International Journal of Computer Network and Information Security*, *9*(6), 53. doi:10.5815/ijcnis.2017.06.06

Al-Attab, B., & Fadewar, H. S. (2018). Hybrid data encryption technique for data security in cloud computing. Sinhgad Institute of Management & Computer Application.

Al-Kaabi, S. S., & Belhaouari, S. B. (2019). Methods toward enhancing RSA algorithm: A survey. *International Journal of Network Security & its Applications*, 11.

Al Saadi, M., Muscat, O., & Kumar, B. (2020). A review on elliptic curve cryptography. *International Journal of Future Generation Communication and Networking*, *13*(3), 1597–1601.

Alanzy, M., Alomrani, R., Alqarni, B., & Almutairi, S. (2023). Image steganography using LSB and hybrid encryption algorithms. *Applied Sciences (Basel, Switzerland)*, *13*(21), 11771. doi:10.3390/app132111771

Albahar, M. A., Olawumi, O., Haataja, K., & Toivanen, P. (2018). *Novel hybrid encryption algorithm based on AES, RSA, and TwoFish for bluetooth encryption*. Academic Press.

Almaiah, M. A., Dawahdeh, Z., Almomani, O., Alsaaidah, A., Al-Khasawneh, A., & Khawatreh, S. (2020). A new hybrid text encryption approach over mobile ad hoc network. *Iranian Journal of Electrical and Computer Engineering*, *10*(6), 6461–6471. doi:10.11591/ijece.v10i6.pp6461-6471

Alqahtani, A., & Sheldon, F. T. (2022). A survey of crypto ransomware attack detection methodologies: An evolving outlook. *Sensors (Basel)*, *22*(5), 1837. doi:10.3390/s22051837 PMID:35270983

Anwana, E. O., & Aroba, O. J. (2022). African women entrepreneurs and COVID-19: Towards achieving the African Union Agenda 2063. *Hervormde Teologiese Studies*, *78*(2). Advance online publication. doi:10.4102/hts.v78i2.7987

Arora, S. & Pooja. (2015). Enhancing cryptographic security using novel approach based on enhanced-RSA and Elamal: Analysis and comparison. *International Journal of Computer Applications*, *975*, 8887.

Asagba, P. O., & Nwachukwu, E. O. (2014). A review of RSA cryptosystems and cryptographic protocols. *West African Journal of Industrial and Academic Research*, *10*(1), 3–16.

Athukorala, P., Chathurangi, M., & Ranasinghe, R. (2022). A variant of RSA using continued fractions. *Journal of Discrete Mathematical Sciences and Cryptography*, *25*(1), 127–134. doi:10.1080/09720529.2021.1968574

Barman, P., & Saha, B. (2015). An efficient hybrid elliptic curve cryptography system with DNA encoding. *International Research Journal of Computer Science, 2*(5).

Bernstein, D. J. (2009). Introduction to Post-quantum cryptography. In D. J. Bernstein, J. Buchmann, & E. Dahmen (Eds.), *Post-quantum cryptography*. Springer. doi:10.1007/978-3-540-88702-7_1

Bhatele, K., Sinhal, A., & Pathak, M. (2012). A novel approach to the design of a new hybrid security protocol architecture. *2012 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT),* 429-433. doi:10.1109/ICACCCT.2012.6320816

Bhattacharjya, A., Zhong, X., & Li, X. (2019). A lightweight and efficient secure hybrid RSA (SHRSA) messaging scheme with four-layered authentication stack. *IEEE Access : Practical Innovations, Open Solutions*, *7*, 30487–30506. doi:10.1109/ACCESS.2019.2900300

Biswas, C., Gupta, U. D., & Haque, M. M. (2019). An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography. *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE),* 1-5. doi:10.1109/ECACE.2019.8679136

Bodkhe, M. R., & Jethani, V. (2015). Hybrid encryption algorithm based improved RSA and Diffie-Hellman. *International Journal of Engineering*. *Science and Mathematics*, *4*(1), 1.

Braga, A. M., & de Morais, E. M. (2014). Implementation issues in the construction of standard and non-standard cryptography on android devices. *SECURWARE*, *2014*, 155.

Brousmiche, K. L., Durand, A., Heno, T., Poulain, C., Dalmieres, A., & Hamida, E. B. (2018). Hybrid cryptographic protocol for secure vehicle data sharing over a consortium blockchain. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),* 1281-1286. doi:10.1109/Cybermatics_2018.2018.00223

Chen, Y., Liu, H., Wang, B., Sonompil, B., Ping, Y., & Zhang, Z. (2021). A threshold hybrid encryption method for integrity audit without trusted center. *Journal of Cloud Computing (Heidelberg, Germany)*, *10*(1), 1–14. doi:10.1186/s13677-020-00222-6

Chinnasamy, P., Padmavathi, S., Swathy, R., & Rakesh, S. (2021). Efficient data security using hybrid cryptography on cloud computing. In *Inventive Communication and Computational Technologies* (pp. 537–547). Springer. doi:10.1007/978-981-15-7345-3_46

Dang, V. B., Farahmand, F., Andrzejczak, M., & Gay, K. (2019). Implementing and benchmarking thre lattice-based post-quantum cryptography algorithms using software/hardware. *Codesign, 2019 International Conference on Field-Programmable Technology (ICFPT)*, 206-214. doi:10.1109/ICFPT47387.2019.00032

Deshmukh, S., & Patil, R. (2014). Hybrid cryptography technique using modified Diffie-Hellman and RSA. *International Journal of Computer Science and Information Technologies*, *5*(6).

El Deen, A. E. T. (2013). Design and implementation of hybrid encryption algorithm. *International Journal of Scientific & Engineering Research, 4*(12), 669-673.

Elkamchouchi, H. M., Takieldeen, A. E., & Shawky, M. A. (2018). An advanced hybrid technique for digital signature scheme. *2018 5th International Conference on Electrical and Electronic Engineering (ICEEE)*, 375-379.

Eltaib, H. A., AbdelRassoul, R., & Zaghloul, M. S. (2020). Hybrid signature scheme integrating elliptic curve cryptosystem with ong, schnorr, and shamir digital signature scheme. *Journal of Physics: Conference Series*, *1454*(1), 012006. doi:10.1088/1742-6596/1454/1/012006

Francia, A. S., Solis-Lastra, J., & Quiroz, E. A. P. (2022). Elliptic curves cryptography for lightweight devices in IoT systems. *Emerging Research in Intelligent Systems: Proceedings of the CIT 2021*.

Gajbhiye, S., Karmakar, S., Sharma, M., Sharma, S., & Kowar, M. K. (2012). Application of elliptic curve method in cryptography: A literature review. *International Journal of Computer Science and Information Technologies*, *3*(3), 4499–4503.

Gill, K. S., Saxena, S., & Sharma, A. (2019). Taxonomy of security attacks on cloud environment: A case study on telemedicine. *2019 Amity International Conference on Artificial Intelligence (AICAI)*, 454-460. doi:10.1109/AICAI.2019.8701363

Gutub, A. A. A., & Khan, F. A. A. (2012). Hybrid crypto hardware utilizing symmetric-key and public-key cryptosystems. *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT),* 116-121. doi:10.1109/ACSAT.2012.44

Hafsa, A., Gafsi, M., Malek, J., & Machhout, M. (2021). Hybrid encryption model based on advanced encryption standard and elliptic curve pseudo random. In Cryptography-Recent advances and future developments. IntechOpen. doi:10.5772/intechopen.95511

Halak, B., Waizi, S. S., & Islam, A. (2016). A survey of hardware implementations of elliptic curve cryptographic systems. *Cryptology ePrint Archive*.

Hameed, M. I., & Hoomod, H. K. (2023, March). New hybrid encryption algorithm for cloud computing security using chaotic system and mCrypton-salsa20 algorithms. *AIP Conference Proceedings*, *2591*(1), 030046. doi:10.1063/5.0119644

Harba, E. S. I. (2017). Secure data encryption through a combination of AES, RSA and HMAC. *Engineering, Technology &. Applied Scientific Research*, *7*(4), 1781–1785.

Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, C. (2018). A review of lightweight block ciphers. *Journal of Cryptographic Engineering*, *8*(2), 141–184. doi:10.1007/s13389-017-0160-y

Hazmi, I. H., Zhou, F., Gebali, F., & Al-Somani, T. F. (2015). Review of elliptic curve processor architectures. *2015 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM),* 192-200. doi:10.1109/PACRIM.2015.7334833

Hoobi, M. M. (2020). Efficient Hybrid Cryptography Algorithm. *Journal of Southwest Jiaotong University*, *55*(3), 5. doi:10.35741/issn.0258-2724.55.3.5

Imam, R., Areeb, Q. M., Alturki, A., & Anwer, F. (2021). Systematic and critical review of RSA based public key cryptographic schemes: Past and present status. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 155949–155976. doi:10.1109/ACCESS.2021.3129224

Intila, C., Gerardo, B., & Medina, R. (2019). A study of public key 'e' in RSA algorithm. *IOP Conference Series. Materials Science and Engineering*, *482*(1), 012016. doi:10.1088/1757-899X/482/1/012016

Issad, M., Anane, N., Bellemou, A. M., & Boudraa, B. (2020). Secure hybrid crypto-system AES/RSA on FPGA for data communication. *Malaysian Journal of Computing and Applied Mathematics*, *3*(1), 11–20. doi:10.37231/myjcam.2020.3.1.38

Iyer, S. C., Sedamkar, R. R., & Gupta, S. (2016). A novel idea on multimedia encryption using hybrid crypto approach. *Procedia Computer Science*, *79*, 293–298. doi:10.1016/j.procs.2016.03.038

Jabbar, A., & Lilhore, P. U. (2017). Design and implementation of hybrid EC-RSA security algorithm based on TPA for cloud storage. *International Journal Online of Science*, *3*(11), 6. doi:10.24113/ojsscience.v3i10.148

Jamaludin, J., & Romindo, R. (2020). Implementation of combination vigenere cipher and RSA in hybrid cryptosystem for text security. *International Journal of Information System & Technology*, *4*(1), 471–481.

Kadam, K. G., & Khairnar, V. (2015). Hybrid RSA-AES encryption for web services. *International Journal of Technical Research and Applications*, *31*, 51–56.

Kapoor, V., & Yadav, R. (2016). A hybrid cryptography technique for improving network security. *International Journal of Computer Applications*, *141*(11), 25–30. doi:10.5120/ijca2016909863

Kaur, J., & Garg, D. S. (2015). Security in cloud computing using hybrid of algorithms. *International Journal of Engineering Research and General Science*, *3*(5), 300–305.

Kaur, S., Bharadwaj, P., & Mankotia, S. (2017). Study of multi-level cryptography algorithm: Multi-prime RSA and DES. *International Journal of Computer Network and Information Security*, *11*(9), 22–29. doi:10.5815/ijcnis.2017.09.03

Khalil, I. M., Khreishah, A., & Azeem, M. (2014). Cloud computing security: A survey. *Computers*, *3*(1), 1–35. doi:10.3390/computers3010001

Koblitz, A. H., Koblitz, N., & Menezes, A. (2011). Elliptic curve cryptography: The serpentine course of a paradigm shift. *Journal of Number Theory*, *131*(5), 781–814. doi:10.1016/j.jnt.2009.01.006

Kumar, H. (2021). Mutual authentication and data security in IOT using hybrid mac id and elliptical curve cryptography. *Turkish Journal of Computer and Mathematics Education*, *12*(11), 501–507.

Kuppuswamy, P., Al, S. Q. Y. A. K., John, R., Haseebuddin, M., & Meeran, A. A. S. (2023). A hybrid encryption system for communication and financial transactions using RSA and a novel symmetric key algorithm. *Bulletin of Electrical Engineering and Informatics*, *12*(2), 1148–1158. doi:10.11591/eei.v12i2.4967

Kuswaha, S., Waghmare, S., & Choudhary, P. (2015). Data Transmission using AES-RSA Based Hybrid Security Algorithms. *International Journal on Recent and Innovation Trends in Computing and Communication*, *3*(4), 1964–1969. doi:10.17762/ijritcc2321-8169.150445

Kvyetnyy, R. N., Romanyuk, O. N., Titarchuk, E. O., Gromaszek, K., & Mussabekov, N. (2016). Usage of the hybrid encryption in a cloud instant messages exchange system. *Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments*, *10031*, 1355–1361.

Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2018). Elliptic curve lightweight cryptography: A survey. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 72514–72550. doi:10.1109/ACCESS.2018.2881444

Le, D. N., Seth, B., & Dalal, S. (2018). A hybrid approach of secret sharing with fragmentation and encryption in cloud environment for securing outsourced medical database: A revolutionary approach. *Journal of Cyber Security and Mobility*, *7*(4), 379–408. doi:10.13052/jcsm2245-1439.742

Mahalle, V. S., & Shahade, A. K. (2014). Enhancing the data security in cloud by implementing hybrid (RSA & AES) encryption algorithm. *2014 International Conference on Power, Automation and Communication (INPAC),* 146-149. doi:10.1109/INPAC.2014.6981152

Mahto, D., Khan, D. A., & Yadav, D. K. (2016). Security analysis of elliptic curve cryptography and RSA. *Proceedings of the World Congress on Engineering, 1*, 419-422.

Malik, A., & Jain, V. K. (2016). Effective renewal and signing method to achieve secure storage and computation using hybrid RSA-MABC algorithm. *International Journal of Intelligent Engineering Systems*, *9*(3), 11–20. doi:10.22266/ijies2016.0930.02

Mantoro, T., & Zakariya, A. (2012). Securing e-mail communication using hybrid cryptosystem on android-based mobile devices. *TELKOMNIKA Indonesian Journal of Electrical Engineering*, *10*(4), 827–834. doi:10.11591/telkomnika.v10i4.874

Mateescu, G., & Vladescu, M. (2013). A hybrid approach of system security for small and medium enterprises: Combining different cryptography techniques. *2013 Federated Conference on Computer Science and Information Systems,* 659-662.

Moghaddam, F. F., Alrashdan, M. T., & Karimi, O. (2013). A hybrid encryption algorithm based on rsa small-e and efficient-rsa for cloud computing environments. *Journal of Advances in Computer Network, 1*(3).

Moghaddam, F. F., Varnosfaderani, S. D., Ghavam, I., & Mobedi, S. (2013). A client-based user authentication and encryption algorithm for secure accessing to cloud servers based on modified Diffie-Hellman and RSA small-e. *2013 IEEE Student Conference on Research and Development,* 175-180. doi:10.1109/SCOReD.2013.7002566

Mohamad, M. S. A., Din, R., & Ahmad, J. I. (2021). Research trends review on RSA scheme of asymmetric cryptography techniques. *Bulletin of Electrical Engineering and Informatics*, *10*(1), 487–492. doi:10.11591/eei.v10i1.2493

Mostafaa, H., Eisaa, S. M., Issaa, H. H., & Shaker, N. H. (2021). Lightweight hybrid encryption system with FPGA design proposal. *IOP Conference Series. Materials Science and Engineering*, *1051*(1), 012023. doi:10.1088/1757-899X/1051/1/012023

Muhammad, S. J., Chiroma, H., & Mahmud, M. (2014). Cryptanalytic attacks on Rivest, Shamir, and Adleman (RSA) cryptosystem: Issues and challenges. *Journal of Theoretical and Applied Information Technology*, *61*(1).

Mumtaz, M., & Ping, L. (2019). Forty years of attacks on the RSA cryptosystem: A brief survey. *Journal of Discrete Mathematical Sciences and Cryptography*, *22*(1), 9–29. doi:10.1080/09720529.2018.1564201

Nasir, M. S., & Kuppuswamy, P. (2013). Implementation of biometric security using hybrid combination of RSA and simple symmetric key algorithm. *International Journal of Innovative Research in Computer and Communication Engineering*, *1*(8), 1741–1748.

Orobosade, A., Aderonke, T., Boniface, A., & Gabriel, A. J. (2020). Cloud application security using hybrid encryption. *Communications*, *7*, 25–31.

Panda, P. K., & Chattopadhyay, S. (2017). A hybrid security algorithm for RSA cryptosystem. *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS),* 1-6.

Panse, T., & Kapoor, V. (2012). An integrated scheme based on triple DES, RSA and MD5 to enhance the security in bluetooth communication. *International Journal of Computer Applications*, *50*(7), 45–50. doi:10.5120/7787-0884

Parenreng, J. M., & Wahid, A. (2022). The e-mail security system using el-gamal hybrid algorithm and AES (advanced encryption standard) algorithm. *Internet of Things and Artificial Intelligence Journal*, *1*, 1–9. doi:10.31763/iota.v2i1.510

Pir, R. M. (2016). Security improvement and speed monitoring of RSA algorithm. *International Journal of Engineering Development and Research*, *4*(1), 195–200.

Prakash, S., & Purohit, M. (2013). Applied hybrid cryptography in key-pair generation of RSA implementation. *JIMS8I-International Journal of Information Communication and Computing Technology, 1*(1), 7-12.

Prakash, S., & Rajput, A. (2018). Hybrid cryptography for secure data communication in wireless sensor networks. In *Ambient Communications and Computer Systems* (pp. 589–599). Springer.

Rahmadani, R., Mawengkang, H., & Sutarman, . (2018). Hybrid cryptosystem RSA–CRT optimization and VMPC. *Journal of Physics: Conference Series*, *978*(1), 012041. doi:10.1088/1742-6596/978/1/012041

Rajavarman, R. (2021). Hybrid security system over banking transaction maintance by a meta key. *Turkish Journal of Computer and Mathematics Education*, *12*(7), 864–868.

Rajput, U., Abbas, F., Eun, H., & Oh, H. (2017). A hybrid approach for efficient privacy-preserving authentication in VANET. *IEEE Access : Practical Innovations, Open Solutions*, *5*, 12014–12030. doi:10.1109/ACCESS.2017.2717999

Rana, A., Chakraborty, C., Sharma, S., Dhawan, S., Pani, S. K., & Ashraf, I. (2022). Internet of medical things-based secure and energy-efficient framework for health care. *Big Data*, *10*(1), 18–33. doi:10.1089/big.2021.0202 PMID:34958234

Rani, S., & Gangal, A. (2012). Cloud security with encryption using hybrid algorithm and secured endpoints. *International Journal of Computer Science and Information Technologies*, *3*, 4302–4304.

Rege, K., Goenka, N., Bhutada, P., & Mane, S. (2013). Bluetooth communication using hybrid encryption algorithm based on AES and RSA. *International Journal of Computer Applications*, *71*(22).

Rehman, E., Asad, M., & Sher, M. (2015). ECC and symmetric based hybrid authenticated key agreement implementation and analysis for body sensor networks. *VFAST Transactions on Software Engineering*, *5*(1), 1–9.

Rehman, S., Talat Bajwa, N., Shah, M. A., Aseeri, A. O., & Anjum, A. (2021). Hybrid AES-ECC Model for the Security of Data over Cloud Storage. *Electronics (Basel)*, *10*(21), 2673. doi:10.3390/electronics10212673

Rezai, A., Keshavarzi, P., & Moravej, Z. (2016). Advance hybrid key management architecture for SCADA network security. *Security and Communication Networks*, *9*(17), 4358–4368. doi:10.1002/sec.1612

Rivest, R. L. (1984). RSA chips (past/present/future). In *Workshop on the theory and application of of cryptographic techniques*. Springer.

Rizk, R., & Alkady, Y. (2015). Two-phase hybrid cryptography algorithm for wireless sensor networks. *Journal of Electrical Systems and Information Technology*, *2*(3), 296–313. doi:10.1016/j.jesit.2015.11.005

Rountree, D. (2011). *Security for Microsoft Windows system administrators: Introduction to key information security concepts*. Elsevier.

Safiraa, M. O., & Mogi, I. K. A (2020). Design of hybrid cryptography with vigenere cipher and RSA algorithm on IOT data security. *Jurnal Elektronik Ilmu Komputer Udayana*.

Saikia, L. P. (2017). Simulation and analysis of modified RSA cryptographic algorithm using five prime numbers. *International Journal on Recent and Innovation Trends in Computing and Communication*, *5*(6), 224–228.

Salam, T., & Hossen, M. (2021). HECC (hyperelliptic curve cryptography). In Functional encryption (pp. 59-78). Springer.

Santoso, Y. S. (2021). Message security using a combination of hill cipher and RSA algorithms. *Jurnal Matematika Dan Ilmu Pengetahuan Alam LLDikti Wilayah 1, 1*(1), 20-28.

Saxena, S., & Kapoor, B. (2015). *State of the art parallel approaches for RSA public key based cryptosystem*. arXiv.

Sebastian, G. (2022). Cyber kill chain analysis of five major US data breaches: Lessons learnt and prevention plan. *International Journal of Cyber Warfare & Terrorism*, *12*(1), 1–15. doi:10.4018/IJCWT.315651

Sharma, S., & Chopra, V. (2017). Data encryption using advanced encryption standard with key generation by elliptic curve diffie-hellman. *International Journal of Security and Its Applications*, *11*(3), 17–28. doi:10.14257/ijsia.2017.11.3.02

Shehzad, D., Khan, Z., Dag, H., & Bozkus, Z. (2016). A novel hybrid encryption scheme to ensure Hadoop based cloud data security. *International Journal of Computer Science and Information Security*, *14*(4).

Shruthy, V. J., & Maheswari, V. (2022). An efficient encryption process with graceful labeling–A hybrid approach. *AIP Conference Proceedings*, *2385*(1), 130032. doi:10.1063/5.0071137

Sihombing, G. L. A. (2017). Hybrid chriptography stream cipher and RSA algorithm with digital signature as a key. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan, 1*(2), 75-83.

Siregar, R. (2018). Performance analysis of AES-Blowfish hybrid algorithm for security of patient medical record data. *Journal of Physics: Conference Series*, *1007*(1), 012018. doi:10.1088/1742-6596/1462/1/012018

Siva, S. P., & Kirubanand, V. B. (2019). Hybrid cryptography security in public cloud using TwoFish and ECC algorithm. *Iranian Journal of Electrical and Computer Engineering*, *9*(4), 2578.

Somaiya, R., Gonsai, A., & Tanna, R. (2023). Implementation and evaluation of EMAES–A hybrid encryption algorithm for sharing multimedia files with more security and speed. *International Journal of Electrical and Computer Engineering Systems*, *14*(4), 401–409. doi:10.32985/ijeces.14.4.4

Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Computer Communications*, *107*, 30–48. doi:10.1016/j.comcom.2017.03.010

Subramanian, K., John, F. L., & John, F. L. (2018). Dynamic and secure unstructured data sharing in multi-cloud storage using the hybrid crypto-system. *International Journal of Advanced and Applied Sciences*, *5*(1), 15–23. doi:10.21833/ijaas.2018.01.003

Taha, A. A., Elminaam, D. S. A., & Hosny, K. M. (2018). An improved security schema for mobile cloud computing using hybrid cryptographic algorithms. *Far East Journal of Electronics and Communications*, *18*(4), 521–546. doi:10.17654/EC018040521

Takieldeen, A., Abd Elkhalik, S. H., Samra, A. S., Mohamed, M. A., & Khalifa, F. (2021). A robust and hybrid cryptosystem for identity authentication. *Information (Basel)*, *12*(3), 104. doi:10.3390/info12030104

Takieldeen, A. E., & Khalifa, F. (2021). Authentication and encryption of IoT devices based on elliptic curves. *Survey (London, England)*.

Tayel, M., Dawood, G., & Shawky, H. (2018). A proposed serpent-elliptic hybrid cryptosystem for multimedia protection. *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI),* 387-391. doi:10.1109/ICACCI.2018.8554950

Thillaiarasu, N., Chenthur Pandian, S., Naveen Balaji, G., Benitha Shierly, R. M., Divya, A., & Divya Prabha, G. (2018). Enforcing confidentiality and authentication over public cloud using hybrid cryptosystems. In *International Conference on Intelligent Data Communication Technologies and Internet of Things* (pp. 1495-1503). Springer.

Thomas, C., Sheela, G., & Krishnan, S. (2014). A survey on various algorithms used for elliptic curve cryptography. *International Journal of Computer Science and Information Technologies*, *5*, 7296–7301.

Thomas, M., & Sheeja, S. (2017). Elliptic curve cryptography and its application in the secure socket layer/transport layer security protocol. *International Journal of Control Theory and Applications*, *10*(29).

Tripathy, A., Tripathy, A. R., Rath, S., Jena, O. P., & Swagatika, S. (2021). Rivest cipher 4 cryptography and elliptical curve cryptography techniques to secure data in cloud. In *Intelligent and cloud computing* (pp. 661–668). Springer. doi:10.1007/978-981-15-5971-6_69

Tropea, M., Spina, M. G., De Rango, F., & Gentile, A. F. (2022). Security in wireless sensor networks: A cryptography performance analysis at MAC layer. *Future Internet*, *14*(5), 145. doi:10.3390/fi14050145

Tuteja, A., & Shrivastava, A. (2014). A literature review of some modern RSA variants. *International Journal for Scientific Research & Development*, *2*(8).

Verri Lucca, A., Mariano Sborz, G. A., Leithardt, V. R. Q., Beko, M., Albenes Zeferino, C., & Parreira, W. D. (2020). A review of techniques for implementing elliptic curve point multiplication on hardware. *Journal of Sensor and Actuator Networks*, *10*(1), 3. doi:10.3390/jsan10010003

Vyas, C., & Dangra, J. (2017). A review of modern cryptography techniques with special emphasis on RSA. *International Journal of Technology Research and Management.*

Xavier, A. P., & Kesavan, R. (2022). Hybrid elliptic curve cryptographic approach for data privacy and authentication in secured map reduce layer (SMR) for optimized CPU utilization. *Journal of the Institution of Electronics and Telecommunication Engineers*, 1–14.

Yang, W. (2022). ECC, RSA, and DSA analogies in applied mathematics. In *International Conference on Statistics, Applied Mathematics, and Computing Science (CSAMCS 2021)* (Vol. 12163, pp. 699-706). SPIE. doi:10.1117/12.2628013

Zhang, F., Chen, Y., Meng, W., & Wu, Q. (2019). Hybrid encryption algorithms for medical data storage security in cloud database. *International Journal of Database Management Systems, 11*.

Zhao, J. (2023). DES-Co-RSA: A hybrid encryption algorithm based on DES and RSA. *2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA),* 846-850.

Musa Ugbedeojo received the M.Sc. degree in management information system (MIS) from Covernant University, Ota, Ogun State, Nigeria. Her research areas are data science, data analysis and project management. She is a lecturer with The Federal Polytechnic, Idah, Kogi State. She is currently a Ph.D student in the Department of Computer Science, Colledge of Pure and Applied Science, Landmark University, Omu-Aran, Kwara State. She can be contacted at email: musa.ugbedeojo@yahoo.com

Marion O. Adebiyi received a BSc. degree in computer science from University of Ilorin, Kwara State, Nigeria in 2000. Her MSc. and Ph.D degree also in computer science, bioinformatics Option from Covenant University, Ota, Nigeria in 2008 and 2014 respectively. She is an associate professor in Computer Science and Head of Department of Landmark University and Covenant University. Her research interests include bioinformatics, genomics, proteomics, and Organism's inter-pathway analysis. She has published widely in local and international reputable journals. He is a member of Nigerian Computer Society (NCS), the Computer Registration Council of Nigeria (CPN) and IEEE member.

Oluwasegun. J. Aroba, a Durban University of Technology lecturer, Department of Information Systems. Honorable Research Associate in the Department of Operations and Quality Management. He has a PhD. in Information Technology. A graduate of Information Technology University from the prestigious Coventry University United Kingdom, BSc. Computer Science and Technology (Upper-Class Division) Crawford University whose research inclination focus area are into Wireless Sensor Networks, Hyper-Heuristic, Hybrid-Heuristic, Meta-Analysis, Project Management, Data Science, Machine Learning, SAP Specialist with over decade years of experience in the higher education sector, healthcare industries, government parastatals, a consultant across the globe, a graduate member of IEEE, IITPSA South Africa, Member of IET UK. He has Chaired and Co-Chaired International and National Conferences. He is a global mentor to SMEs and European African, Sisonke NdabaX, and a seasoned guest speaker. He has a vast collaboration network across Spain, France, Morocco, the USA, the UK, South Africa, and Sweden. oluwaseguna@dut.ac.za

Ayodele Ariyo Adebiyi is a faculty and former Head of Department of Computer and Information Sciences, Covenant University, Ota Nigeria. He is currently the Dean, College of Pure and Applied Sciences at Landmark University, Omu-Aran, Nigeria, a sister University to Covenant University. He holds a B.Sc degree in Computer Science and MBA degree from University of Ilorin, Ilorin, Nigeria in 1996 and 2000 respectively. He had his M.Sc and Ph.D degree in Management Information System (MIS) from Covenant University, Nigeria in 2006 and 2012. His research interests include, application of soft computing techniques in solving real life problems, software engineering and information system research. He has successfully mentored and supervised several postgraduate students at Masters and Ph.D level. He has published widely in local and internationally reputable journals. He is a member of Nigerian Computer Society (NCS), the Computer Registration Council of Nigeria (CPN) and IEEE member.