IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 24, 2021, accepted November 11, 2021, date of publication November 18, 2021,
date of current version November 30, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3129224

Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status

RAZA IMAM[1], QAZI MOHAMMAD AREEB[1], ABDULRAHMAN ALTURKI[2], AND FAISAL ANWER[1]

[1]Department of Computer Science, Aligarh Muslim University, Aligarh 202002, India
[2]Electrical Engineering Department, College of Engineering, Qassim University, Buraydah 51452, Saudi Arabia

Corresponding author: Faisal Anwer (faisalanwer.cs@amu.ac.in)

ABSTRACT The interconnected digital world is generating enormous data that must be secured from unauthorized access. Advancement in technologies and new innovative methods applied by attackers play an instrumental role in breaching data security. Public key Cryptography provides a set of cryptographic algorithms in achieving data security through confidentiality, integrity and authentication. Among all cryptographic algorithms in general and public key cryptography in particular, RSA is one of the most widely used and applied algorithms. Since its inception, it is commonly being adopted in securing data across different domains such as cloud, image and others. Despite its importance and wide applications, no such systematic and extensive survey exists in the literature. A systematic and thorough study of RSA based cryptography is presented in this work covering several domains. All the available works in this direction are divided into 11 different categories, viz, Hybrid, Parallel, Cloud, Image, Multiple-Keys, Chinese-Remainder-Theorem-based, Digital-Signatures, K-Nearest-Theorem-based, Batch, Wireless, and Core-Modifications. This study methodically explores RSA-based cryptosystems, either modifications in core RSA or applications of enhanced RSA across different domains, systematically categorizing in various categories and eventually providing findings and indications. The current study compares RSA methods based on parameters such as key generation, encryption schemes, decryption schemes, key features and enhancements, and also finds the leading areas where modified RSA has been applied in the recent past. As a result, this study will guide researchers and practitioners in understanding the past and present status of RSA cryptography along with the possibility of its applications in other domains.

INDEX TERMS Asymmetric key cryptography, cryptography, data security, public key cryptography, RSA cryptography, RSA cryptosystem.

I. INTRODUCTION

Information Technology is the backbone of today's society in terms of day to day activities and is being utilized in almost every aspect of life. The exponential growth of the modern-day technological world is equally leading to the production of millions of data on a continuous basis. With such elevation, the need to keep data secure and private is increasing even more by individuals as well as organizations. Security has always been a most significant concern for the computing world in terms of transmitting information and data across the internet. Whether through the Internet, smart gadgets, or any form of transmission, the reports about data thefts and breaches seem to be growing more and more. As a result, researchers and cryptographers are continuously working towards the innovation of various new cryptographic models along with numerous improvements of existing cryptographic algorithms in order to implement in real-world applications to improve user privacy, data security, authentication, or any other such features [1].

The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru.

A. CRYPTOGRAPHY

The definition of cryptography states that it is a technique by which a message, whether in the form of texts, images or other

formats, can be disguised in such a manner that only the transacting parties, that is, sender and receiver, can interpret the actual information, and also without any intervention of any third party or adversary. The process of converting plain data into an unreadable or encrypted version is basically referred to as encryption, whereas the process done the other way around is referred to as decryption. Three of the important security requirements for any encryption-decryption protocol is typically based on these features: Confidentiality of the data, Maintenance of the Data Integrity, and Authentication of the transacting parties, meanwhile if any cryptographic protocol is not able to follow these requirements as mentioned above, it can't be said to be a reliable source for data transmission [2]. Majorly, on the basis of the number ''keys'' engagement, cryptographic protocols are classified into two broad categories, symmetric key cryptography, and public or asymmetric key cryptography. The difference between the two is that symmetric key algorithms constitute a single key, while public key cryptographic algorithms include a pair of keys during the transmission or encryption-decryption process. AES, DES, Triple DES, Blowfish are some popular examples of symmetric key algorithms, while RSA, ElGamal, and Elliptic Curve Cryptographic algorithms are extensively used public key cryptographic algorithms [3].

B. RSA PUBLIC KEY CRYPTOGRAPHY

Among all the popular cryptographic algorithms, one of the oldest and the most extensively used algorithm is the RSA public key cryptographic algorithm or RSA (Rivest, Shamir, Adleman) cryptosystem, which is named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman, who first published the white paper of RSA in 1977. The most recent applications of standard RSA are incorporated in key exchanges, digital signatures [4], web browsers, chat applications, emails, VPNs and any other types of communication where data transmission between two parties is required. The security of RSA relies fundamentally on the practical difficulty of factoring the product of two large prime numbers, the ''factoring problem''. Breaking RSA encryption is known as the RSA problem. RSA is a relatively slow algorithm in comparison to other popular cryptosystems. Because of this, it is not commonly used to directly encrypt user data. More often, RSA is used to transmit shared keys for symmetric key cryptography, which are then used for bulk encryption-decryption.

Over the years, the RSA algorithm has been extensively being used in different areas to secure the data and information transmission, whether that area is cloud servers, key exchanges, or internet protocols or any area where secure transmission is required between two parties. In recent days, many researchers are also working on making RSA more useful in IoT devices, smart gadgets, and lightweight devices [5], [6]. The reason for such an enormous usage of RSA is its security that can't be breached easily by normal day PCs and systems, but in spite of that, several records have been reported recently about breaking RSA ciphers with shorter key sizes, which eventually offers the researchers and cryptographers to come up with a more enhanced version of RSA. Whether it is any symmetric cryptosystem or public cryptosystem, RSA is one the most considerable algorithm among all, and numerous research works are going on a continuous basis on its enhancement in terms of its security and performance to make the RSA more complex and reliable along with increasing its encryption and decryption speed.

C. MOTIVATION

Despite being the utilization of RSA in a number of areas, a proper Systematic Literature Survey (SLR) is not present in the recent academic literature that could showcase the past, recent and current trend of contributions in RSA enhancement as it is known among the research peers that before the beginning of any research contribution, a researcher always looks for a systematic literature review in order to assess the area where the future research could be focused on. Hence the need for a systematic survey that collects all the enhancements in the RSA scheme till the present day is required. Therefore, this literature survey collects and presents all the RSA based methods, including enhanced versions and applications across different domains, to employ clear procedures for identifying what can be confidently asserted on the basis of these studies. The main objective of the systematic survey is not just to provide an aggregation of existing contributions or literature but also to provide a direction in which further research contribution can be made [7]. They are designed to find as much research as feasible on a given research issue. With the goal of providing a wide range of outcomes that are trustworthy, methods should be not only clear but also systematic.

D. CONTRIBUTIONS

This SLR on the RSA based schemes summarizes and organizes recent literature results in a way that integrates and adds understanding to the work in the RSA field. This systematic survey emphasizes the classification of the existing literature to develop a perspective on the certain dominant RSA areas and domains and assess the research trends following the standard SLR methodology. The paper performs a systematic survey of the current research work done in an RSA field and provides a critical assessment of the past and current work that has been done by stating the strengths and weaknesses of the existing literature. Therefore, the contribution of this review is an exploration of RSA Schemes proposed using various modified approaches and applications across different domains with identification of constraints and limitations encountered. We have highlighted various related works and literature reviews, especially in the relevant fields of RSA and general cryptography in Section II. We documented our research methodology in Section III, while Section IV deals with presenting the under-studied literature in a systematic and elaborative manner, considering every domain and sub-domains. Section V discusses the results and future

directions, while the paper is concluded in Section VI. Also, abbreviations are shown in Table 18 (Appendix A).

II. RELATED WORKS

A number of surveys based on various cryptographic approaches, including RSA algorithms, have been published in recent years. However, there is not a single study that aims to study all of the RSA enhancements in a systematic and comprehensive manner. Most of the studies that we are covering in this section are unsystematic surveys, and we have also included some literature in this section that focuses on the review of various other asymmetric key cryptographic and lightweight cryptographic algorithms.

In the year 2021, Mohamad *et al.* [8] discuss a review of the RSA scheme of asymmetric cryptography techniques. Based on the efforts of researchers over the last decade, it attempts to present the domains of RSA scheme use, such as public network, wireless sensor network, image encryption, cloud computing, proxy signature, Internet of Things, and embedded device. Apart from that, based on the number of studies conducted, the article examined the trends and performance parameters of the RSA scheme, including security, speed, efficiency, computational complexity, and space. Finally, this study discusses the proposed scheme's techniques and advantages. This survey is very unsystematic and covers very few RSA schemes. No proper research methodology has been used in this study.

Al-Kaabi and Belhaouari [10] used several ideas on different approaches used to strengthen the RSA algorithm and improve its security in their survey work of 2019. Few RSA variants that this paper studied include variants like combining the RSA method with the Diffie-Hellman or ElGamal algorithms, modifying RSA to include three or four prime numbers, offline storing of generated keys, a secured RSA process where the message can be encrypted using dual encryption keys, and few more such variants. They have discussed a total of 10 such RSA variants. The publication also explains the methods involved in solving the Number Field Sieve (NFS), which is used to factor very large integers. It also includes a discussion of the consequences for moduli larger than RSA-768. This study focuses only on a few variants of RSA and not an extensive and critical survey.

In his work, Santoso *et al.* [11] in 2018 seeks to perform a systematic literature review on the creation of cryptographic algorithms and their use in order to compare them based on numerous factors such as encryption strength, speed of operation, cost, and so on. As a result, state of the art may be determined in terms of the benefits and drawbacks of various cryptographic algorithms, which are in use now. The authors of this study synthesis some literature connected to the research topic and found a total of 12 cryptography papers, but only seven are relevant to the research domain. Cryptographic key algorithms (Blow Fish, DES, AES) are compared, as well as asymmetric keys (RSA, DSA, Diffie-Hellman). Key types, key length, encryption strength, tunability, speed of operation, implementation, and power consumption are among the parameters that are compared. Their study covers very few articles having a limited scope.

In 2017, Vyas and Dangra [12] published another review study of modern data encryption and decryption technologies while focusing on RSA enhancements. They included less than ten such RSA variants, and a brief discussion of all such approaches was provided in this paper. The authors performed their review without using any proper research methodology and considered very few articles for their review.

Saxena and Kapoor [13] presented a survey of different parallel implementations of the RSA algorithm in 2015, which included a wide range of hardware and software implementations. Parallel programming is a new area of research that aims to improve performance and efficiency by utilizing multi-core processors to execute instructions more quickly and efficiently. The authors aimed to raise awareness among upcoming researchers about numerous parallel RSA implementation strategies that have already been developed. They investigated a number of concurrent techniques to implementing RSA provided by many researchers around the world in order to attain high performance and throughput in the field of RSA and public key cryptography. This survey focuses on only one aspect of RSA schemes, i.e., parallel implementation.

In 2014, Asagba and Nwachukwu [14] presented a review of public-key cryptography, focusing on the RSA method. They talked about some of RSA's security concerns, obstacles, and several cryptographic attacks. The author aimed to provide a comprehensive assessment of the standard RSA cryptosystems while discussing some RSA variants. However, they missed a comprehensive literature survey.

Dhanda *et al.* [15] in 2020 presented an in-depth and up-to-date systematic survey of lightweight cryptographic schemes. The study compares 54 LWC algorithms in their respective classes, including 21 lightweight block ciphers, 19 lightweight stream ciphers, nine lightweight hash functions, and five variations of elliptic curve cryptographic (ECC) algorithms. The ciphers were compared in terms of chip size, energy and power consumption, hardware and software efficiency, throughput, latency, and figure of merit (FoM). Based on the findings, they concluded that AES and ECC are the best lightweight cryptographic primitives to use. In the subject of lightweight cryptography, some open research topics have also been highlighted in this systematic study. A comprehensive review has been done in this study without following a structured methodology.

In 2018, Lara-Nino *et al.* [16] did a survey on elliptic curve lightweight cryptography and defined the characteristics that make an ECC-based system lightweight and suitable for use in limited applications. The key factors examined in ECC designs for lightweight realizations are systematically reviewed as well. As a result, the paper establishes the concept and specifications for elliptic curve lightweight cryptography for the first time. This type of study is missing

TABLE 1. Brief Summary of some published Cryptography related surveys.

Year	Work	Refs	Survey Coverage	Survey Type	Total Refs
2021	Mohamad et al.	[8]	RSA / Algorithms & Strengths	Unsystematic & Short	45
2019	Al-Kaabi and Belhaouari	[10]	RSA / Encryption-Decryption	Uncomprehensive & Unsystematic	18
2018	Santoso et al.	[11]	Symmetric & Public Key Cryptography	Systematic & Uncomprehensive	7
2017	Vyas and Dangra	[12]	RSA / Encryption-Decryption	Blunt, Short & Uncomprehensive	12
2015	Saxena and Kapoor	[13]	Parallel RSA Implementations	Unsystematic & Comprehensive	15
2014	Asagba and Nwachukwu	[14]	RSA / Security	Uncomprehensive & Unsystematic	33
2020	Dhanda et al.	[15]	IoT / Lightweight Ciphers	Comprehensive & Unsystematic	108
2018	Lara-Nino et al.	[16]	Elliptic Curve Cryptography	Systematic & Well-Defined	110
2017	Buchanan et al.	[17]	Lightweight Cryptography	Comprehensive & Unsystematic	33

in the literature for RSA public key cryptography, a worthy competitor of ECC.

In 2017, Buchanan *et al.* [17] described several of the techniques that are defined as substitutes for traditional cryptography in the IoT (Internet of Things) arena, as well as certain trends in lightweight algorithm design. The study further provides a review of state-of-the-art ultra-lightweight and IoT encryption that can be employed over resource-constrained smart devices like intelligent sensors and several wireless systems like RFID [18].

The analysis of the above included surveys on RSA schemes and their related fields suggests that a systematic and extensive study on RSA public key cryptography is missing. All studies focus on a very limited domain and largely just on variants of RSA schemes. In this study, we have made a systematic and critical survey on RSA schemes, their different variants and applications across different domains. This study will prove to be very useful for researchers and practitioners in the field of cryptography and especially on RSA public key cryptography. A summary of all the related literature reviews is also shown in Table 1, along with their coverage and, survey type and total references they have covered in their work.

III. RESEARCH METHODOLOGY

A well-structured survey involves the study and thorough interpretation of all the available research on the interest subject or field. According to Kitchenham and Charters [19], there are several steady reasons that need to be considered while doing a methodological survey, like summing up the existing works and findings of a specific subject and also suggesting further improvisation by distinguishing any shortcomings or gaps. Furthermore, instead of any unsystematic method, a systematic approach reflects the overall research purpose and their expected quality by classifying underlying topics based on certain categories and parameters. This section analyzes out the methodological approach of our survey.

A. RESEARCH QUESTIONS

- RQ 1. What's the overall objective of the author for enhancing or modifying the RSA model?
- RQ 2. What are all the several RSA modifications that have been made in the standard RSA algorithm till today?
- RQ 3. What's the yearly based research coverage in the RSA domain since the start of the research and developments in RSA algorithms?
- RQ 4. How do the proposed RSA schemes resolve the existing limitations and issues of current information or network security?
- RQ 4. Which domain has got more attention as far as RSA schemes are concerned?

As per Kitchenham, the question structure comprises of three aspects: Population, Interventions, and Outcomes. The Population in this survey is the focus of our research that includes all under-studied RSA models or rather algorithms that are further enhanced or modified versions of the actual standard RSA algorithm. The Interventions, in our case pertaining to this specific survey, are the actions like modified or enhanced, and several other terms that showcase the type of treatments with RSA. The Outcomes are the final conclusion that decides if the enhanced RSA algorithms have shown any significant advantage.

B. SEARCH STRATEGY GENERATION

We have searched various RSA schemes on the basis of the following stages:

1) RECOGNIZING DESCRIPTIVE TERMS AND RELATED SUBSTITUTES

The influence of terminology variations is reduced to the minimum to have a result narrowed down to our specific demand pertaining to our survey. We have also selected the keywords of all related studies and selectively included them in our search strategy.

2) JOINING TERMS AND THEIR SUBSTITUTES USING OR BOOLEAN

To achieve efficiency in our search results, we have used OR Boolean to join the terms and their substitute words or synonyms. This broadens up our results in every previously researched domain and presents the results covering all the areas wherever the RSA has been previously researched on.

3) JOINING TERMS USING AND BOOLEAN

To achieve straightforward and topic-specific results, we have employed the AND Boolean to join words and their

categorical terms. This narrows down our results as per the particular demand of our review.

During our search, we have utilized the following terms to efficiently fetch out all of the required research pertaining to our survey:

- Population: RSA, Rivest Shamir Adleman, PK, public key, cryptosystem, asymmetric, model, scheme, algorithm, encryption, decryption, generation, cryptanalysis
- Interventions: enhanced, efficient, improved, improvised, modified, fast, optimized, secured, robust, designed, increased, encode, hybrid
- Outcomes: security, efficiency, performance, reliability, confidentiality, improvement, scalability, maintainability, safety, robustness, integrity, availability

We performed the search-string inspection in several academic databases and search engines and primarily focused on all available journals and conference proceedings. We have considered 1980 as our initial search year as after this only researchers began proposing the initial versions of RSA modifications, as per our findings. We have utilized the two-stage searching strategy for our findings. In the first stage, we manually inspected using several search strings and their combinations using Booleans. The databases and digital libraries we have inspected within are as follows:

- ScienceDirect
- Scopus
- ACM Digital Library
- Springer
- IEEE Xplore
- Web of Science

We have also utilized several web search engines to access the related literature across all the publishing formats and disciplines, which are mentioned as follows:

- Google Scholar
- Microsoft Academics

The first stage of our inspection includes the combinatorial searches using the search strings (see Fig. 1) made up of several strings and terms within the combination of above mentioned booleans. We have also tried out the search strings on an iterative basis in order to fine-tune our search results. This fine-tuning also enabled us to tackle the challenge of aligning our searches with completeness and consistency. The search strings are implemented distinctively on the title, abstract and corresponding keywords. The detailed inspection of the implemented search strings is shown in Appendix A.

We also manually fetched across several reputed journals as well as some veteran conferences pertaining to the domain of our research. These selected journals and conferences comprise previously held research in the field of cryptography/cryptology, RSA and its related enhancements in the relevant domains. Some of those journals are International Journal of Information Security (Springer), Journal of Information Security and Applications (Elsevier), IEEE Transactions on Dependable and Secure Computing (IEEE), Journal of Cryptology (Springer), IET Information Security (IET Digital Library) and IEEE Security and Privacy (IEEE). Whereas several conferences we have searched in are SECRYPT, International Conf. on Cryptography, Security and Privacy, CRYPIS and International Cryptology Conference.

FIGURE 1. Word cloud for RSA public key cryptography.

Further, In order to get a more significant sample of our research in the prior stage, we have done a second stage procedure. During the second stage, we have scanned all the reference lists and examined all principal research in order to find additional articles. Fig. 2 shows our two-stage approach in an illustrative manner. Initially, utilizing our search string, a total of 1145 papers from all considered databases were discovered. And finally, after implementing our search strategy, we have discovered a total of 245 papers that pertain to our relevant survey study.

C. INCLUSION AND EXCLUSION SELECTION CRITERIA

Our initial search yielded 245 out of 1145 total counts of papers. The selection procedure and ultimate choice of primary studies were managed by one of the authors. If there were any discrepancies concerning the legitimacy of a particular paper, conversation and interaction with the other authors addressed this issue. We have also illustrated our whole study selection criteria and the number of papers collected from each database in Fig. 3. As a result, it is critical that we establish detailed inclusion/exclusion criteria to ensure that only primary studies that offer evidence relevant to the research topics are chosen. This review then further omitted those papers that meet the following exclusion criteria:

- Do not directly or indirectly propose the modified or enhanced version of the standard RSA algorithm
- Relates to only the cryptanalysis of RSA algorithm
- Relates to the proposal of other efficient algorithms or methods that are integrated with RSA
- Relates to any proposal of key distribution schemes
- Relates to attacks on various server-aided RSA Protocols
- Relates to the encryption or decryption of Image or other formats without proposing any researched scheme of RSA
- Relates to the implementation of any other applications utilizing the standard or previously enhanced RSA
- Relates to any other method of generating random numbers utilizing RSA algorithms

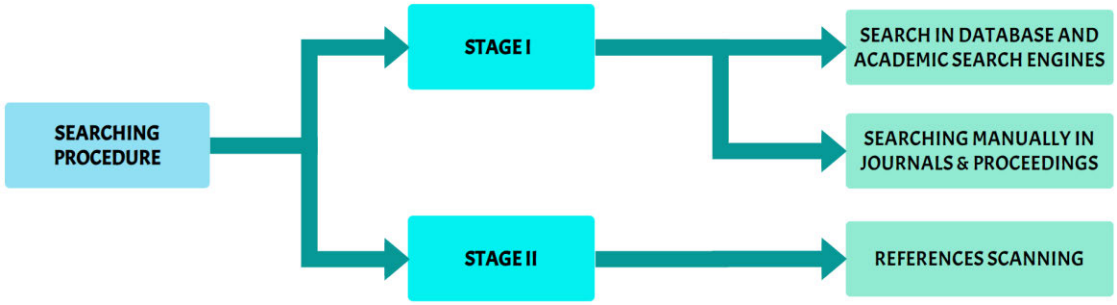


FIGURE 2. Implemented search procedure.

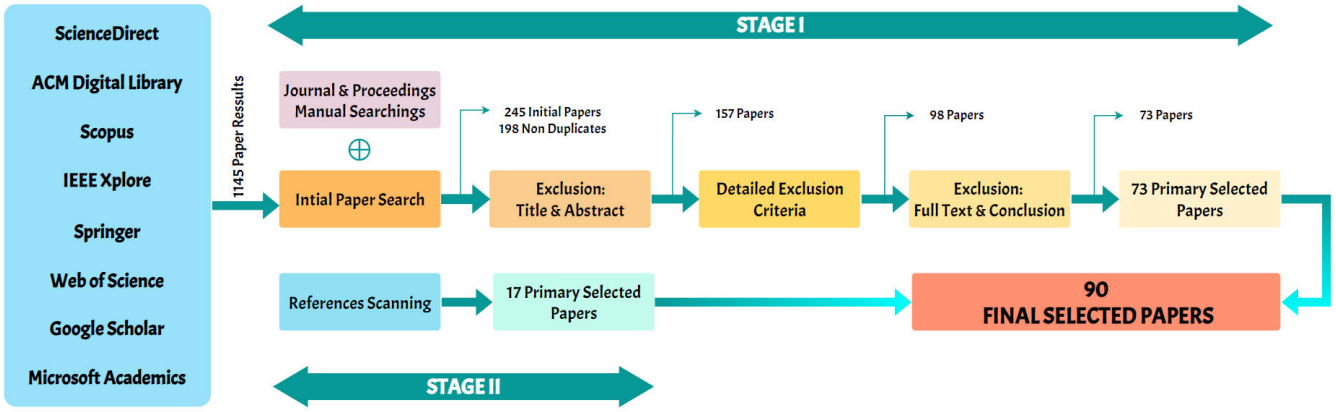


FIGURE 3. Study selection criteria.

- Relates to the cryptanalysis of the standard RSA algorithm
- Relates to just cryptanalysis, the hybrid version or any other enhanced versions of RSA algorithms
- Relates to highlighting any other research sectors utilizing RSA algorithms

We have considered only those RSA papers which are proposed in order to showcase the newly researched RSA algorithms, which is an enhanced or modified version than traditional RSA. The papers were removed from a total based mostly on title and abstract, obviously out of the scope and did not deal with the topic of our interest, and also considering our discussed exclusion criteria. Our search strings result in a total of 1145 papers, which on the basis of the first paper search and sorting in the databases, 245 papers get finalized. Next, considering comparable research published in other digital libraries, databases and search engines, a total of 47 out of 245 papers were neglected initially, as they were overlapping with our initial results. Hence after duplicate elimination, we were left with a total of 198 papers. We employed the use of a multi-step strategy for the exclusion implementation of our collected papers. Initially, one of the authors considered the title and abstract of 198 papers, and among those which were not a bit relevant to our interests and were obviously beyond the field of the study, were excluded from the list of papers. In this manner, 41 more papers were excluded, and we were left with a total of 157 papers. Moreover, two of the authors considered the exclusion criteria on an individual basis, and in the consensus of all authors, 59 more papers were considered for elimination as they were aligned with our discussed exclusion criteria mentioned above. Furthermore, we were left with a total of 98 papers and then applying the conclusion of individual papers and full-text exclusions, we finally concluded a total of 73 papers from stage 1 of our findings. Considering stage 2, i.e., scanning the references lists, we have collected a total of 17 papers taking into account the exclusion criteria and all other viewpoints. Stage 2 helped us to cover all the papers that pertain to our interest of survey with the minimal of any papers left of our survey. In this manner, utilizing the multi-step study selection procedure, we have collectively taken a total of 90 papers for our survey that pertains to the relevant enhancements of the RSA algorithm.

D. QUALITY ASSESSMENT AND DATA EXTRACTION

Quality checklists must be included in the survey for evaluating each and every literature, and these checklists are prepared via methodical quality assessments. Data extraction helps to find if how exact information from the under-study papers can be fetched efficiently. Extensive exclusion procedures can be utilized to develop a quality data extraction and their assessments. In order to prevent any misinterpretation

of results owing to the quality of the test, we utilized the evaluation of qualitative research mainly to guide findings for data analyses and their reconciliation. Table 19 in Appendix A depicts the quality assessment criteria for each of the mentioned literature. The studies that answer ''Yes'' to our quality assessment criteria are marked with (✓), and if ''No'', they are marked with (✗). The criteria developed for the quality assessment is mentioned as follows:

A. Do the selected papers, which are comprised of proposed algorithms, have been practically implemented or not?

B. Do the selected papers involve the comparison of their proposed algorithms with others?

C. Do the methods which are partially proposed in the conference papers are subsequently extended in the Journals or not?

D. Do the proposed methods evaluate each phase of the algorithm (i.e., key generation, encryption and decryption phases)?

E. Are the objective and discussion corresponding exactly with the conclusion described by the authors?

We have done data extraction from each of the studies in order to fetch all of the required information that would help to further answer the research questions in a more efficient manner. We examined the literature in accordance with standard details on the titles, authors, year and publishing parameters to evaluate the consistency of data extraction. The data extractions were primarily examined for the primary research subject, the objective of the suggested scheme, the domain category dealt with, restrictions/limits of the particular proposed RSA algorithm, possibilities of future studies discovered and key conclusions were also examined. Furthermore, this data extraction classified all of the under-study literature by the category of the year they were researched and proposed and further considered the domain and field those enhanced algorithms cover. This data extraction also assesses whether it is only the algorithm enhancement that only improves performance and security or also enhanced to adopt other fields and domains.

E. DATA ANALYSIS

We have shown several analyses of our data assessment through various illustrations and classifications. On the basis of prior studies, we have also divided all the literature into several domains. The term ''Domain'' here implies that in which area or field a particular RSA algorithm has been focused on during its proposal. There is a total of 11 categorized domains considered in this survey. Those number of primary selected literature describing several domains of RSA enhancement are as ''Batch'', ''Chinese-Remainder-Theorem-Based'', ''Cloud'', ''Image'' ''Digital Signatures'', ''Hybrid-Versions'', ''K-Nearest-Theorem-Based'', ''Parallel'', ''Multiple-Keys-Based'', ''Wireless areas'' and finally ''Core-Modifications''. The ''Core-Modifications'' domain is further classified into Fast Variants, Integrated Schemes, Security Focused and Mathematical Modifications. The ''Core-Modifications'' domain here comprises of all those studies which are modified only on the mathematical core of algorithm itself, not on the basis of any particular area or field, or criteria it may be that they are the found ''single'' in our findings, and we can't keep that single paper in any other domains because they contain those algorithms which are solely covering up a sole area by itself, or they are more general in comparison to all considered domains. Fig. 4 represents all the research in the enhancements of RSA algorithms on the basis of the domain and yearly distributions, starting from the year 1978, in which RSA was introduced itself, up to the period of July 2021. Similarly, for a more deep and selective understanding, Table 2 provides the yearly distribution of each study on the basis of considered domains. Fig. 5 illustrates a pie-of-pie chart that describes the distribution of selected research domains that each of the papers have covered up, including the ''Core-Modifications'' section. We have also illustrated the distribution of several sub-domains that the ''Core-Modifications'' section has covered up.

IV. DISCUSSIONS OF THE FINDINGS

In this section, we provide the descriptive evaluation of the reviewed literature with respect to the researched enhancements of several RSA variants. Each of the considered domains is discussed in terms of the proposal's objective and their conclusion after studying and assessing each of the papers on an individual basis which relates to the research questions. The domains that contribute to the highest count of algorithms are discussed first, and further moving on to the last domain, i.e., ''Core-Modifications'', in which all of its sub-domains are discussed in the same manner. Additionally, a table of algorithm analysis is also included at the end of the section and sub-section for a clear comprehension of each author's approach.

A. HYBRID

Many researchers have proposed several enhanced RSA algorithms in order to improve security or performance that utilizes the properties of other algorithms and thus result in a hybrid version of RSA. This section discusses all of the literature that has proposed an enhanced version(s) of the RSA algorithm utilizing a hybrid approach in their solution. Each study is highlighted and discussed on the basis of its proposal year, starting from 2003 up to the latest hybrid solution of 2020.

In the year of 2003, Alison *et al.* [53] have suggested an extensive approach that discusses an efficient and feasible approach of combining two previously enhanced RSA variants. Those two of the four previously enhanced versions are proposed by Boneh and Shacham [25], which were named as Multi-Prime RSA and Rebalanced RSA. Utilizing a hybrid approach of these two RSA variants, Paixao and Filho have named their variant as R-Prime RSA. Paixao's objective was to reduce the decryption and signature generation times in comparison to the standard RSA algorithm. According to the authors, their proposal achieves good decryption speed and

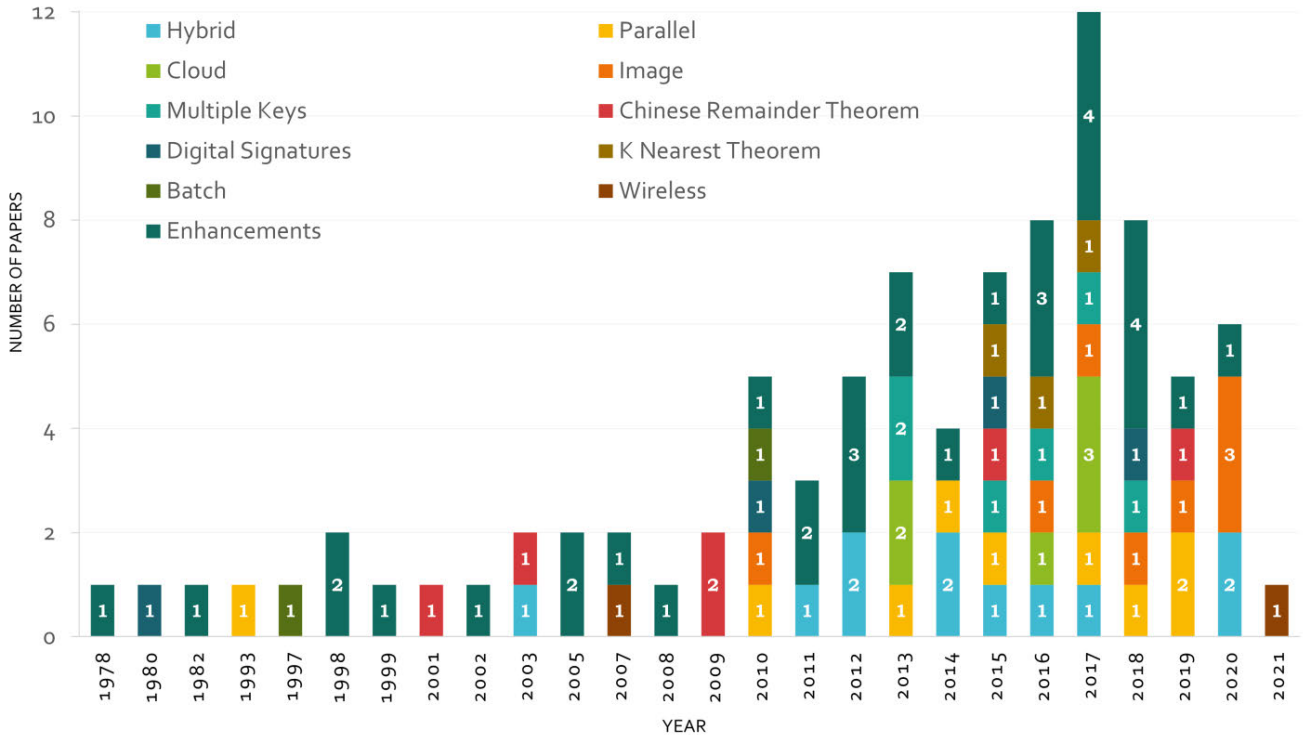


FIGURE 4. Distribution of all studies on the domain and year basis.

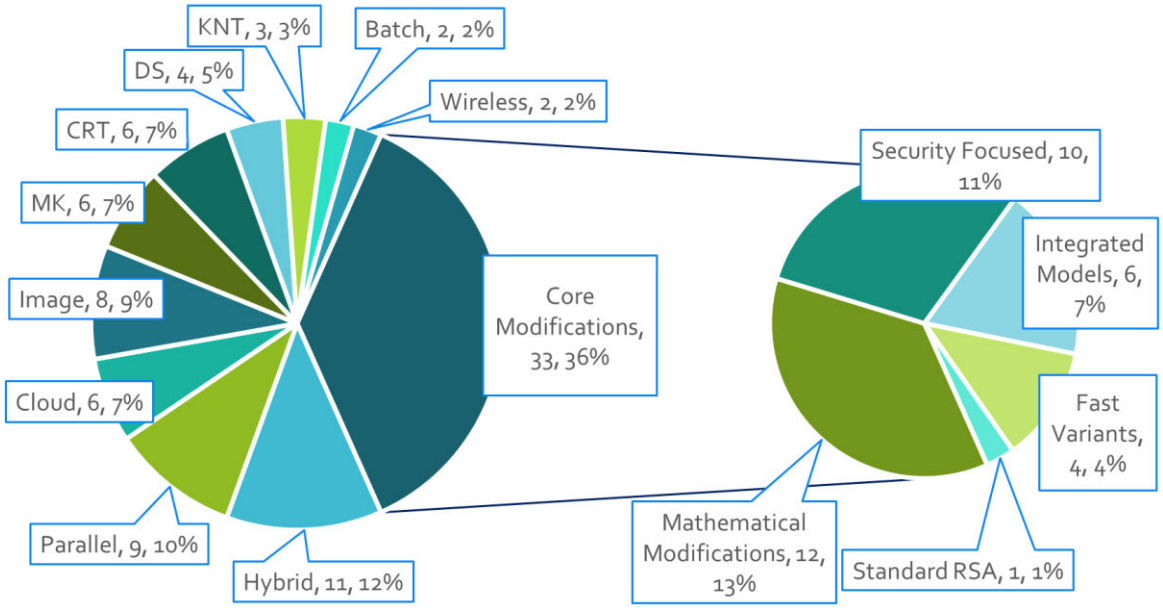


FIGURE 5. Domain distribution of all studied literatures (A pie is represented as: Domain, belonging algorithms, % covered).

performs better with large size moduli, i.e., 27X faster than standard RSA in the decryption process. Similarly, Gupta and Sharma [54] utilized the merge of RSA with another public key cryptographic algorithm referred to as Diffie-Hellman, with an objective to enhance the security levels and overall execution speed of the algorithm. The authors have claimed that an adversary cannot possibly find the generated key, and also it involves higher complexity, and hence that results in the higher security of the algorithm. Furthermore, Dhakar *et al.* [55] proposed a version of RSA, which was named as MREA or Modified RSA Encryption Algorithm. MREA is based on an additive homomorphic attribute and

TABLE 2. Main studies yearly distribution on the domain basis.

Domain	References	Year	Domain	References	Year	Domain	References	Year
Core Modifications	Rivest et al. [20]	1978		Mahalle et al. [57]	2014	Chinese Remainder Theorem	Wu et al. [87]	2001
	Quisquater et al. [21]	1982		Arora et al. [58]	2015		Blomer et al. [88]	2003
	T. Takagi [22]	1998		Karakra et al. [59]	2016		Ou [114]	2009
	Collins et al. [23]	1998		Panda et al. [60]	2017		Garg et al. [115]	2009
	D. Pointcheval [24]	1999		Jintcharadze et al. [61]	2020		Sony et al. [89]	2015
	Boneh et al. [25]	2002		Alamsyah1 et al. [109]	2020		Abdeldaym et al. [90]	2019
	Lenstra et al. [26]	2005						
	Galbraith et al. [27]	2005	Multi-Threading or Parallel	C. Chiou [62]	1993	Digital Signatures	Williams [116]	1980
	Sun et al. [28]	2007		Li et al. [63]	2010		Si et al. [91]	2010
	Aboud et al. [29]	2008		Damrudi et al. [64]	2013		Jaju et al. [92]	2015
	Bahadori et al. [30]	2010		Saxena et al. [65]	2014		Aufa et al. [93]	2018
	Chhabra et al. [31]	2011		Asaduzzaman et al. [66]	2015			
	Sharma et al. [32]	2011		Saxena et al. [67]	2017	K Nearest Theorem	A.K. Huussain [94]	2015
	Al-Hamami et al. [33]	2012		Gupta et al. [68]	2018		Mathur et al. [95]	2016
	Ivy et al. [34]	2012		Ayub et al. [69]	2019		Mathur et al. [96]	2017
	Nagar et al. [35]	2012		Rawat et al. [70]	2019			
	Pradhan et al. [36]	2013				Batch	A. Fiat [97]	1997
	Minni et al. [37]	2013	Cloud	Moghaddam et al. [71]	2013		Liu et al. [98]	2010
	Patel et al. [38]	2014		Patidar et al. [72]	2013			
	Thangavel et al. [39]	2015		Bansal et al. [73]	2016	Wireless	Frunza et al. [99]	2007
	Meneses et al. [40]	2016		Makkaoui et al. [74]	2017		S. Shin [100]	2021
	Kumar et al. [41]	2016		Amalarethinam et al. [75]	2017			
	Mo et al. [42]	2016		Makkaoui et al. [76]	2017			
	K. Somsuk [43]	2017						
	Sahu et al. [44]	2017	Image	Zhao1 et al. [110]	2010			
	Chaudhury et al. [45]	2017		Alsabti et al. [77]	2016			
	Aiswarya et al. [46]	2017		Jagadiswary et al. [78]	2017			
	Chakraborty et al. [47]	2018		Cheltha [111]	2017			
	Islam et al. [48]	2018		Shin et al. [79]	2019			
	Raghunandhan et al. [49]	2018		Huang et al. [80]	2020			
	Yadav et al. [50]	2018		Jiao et al. [81]	2020			
	Barazanchi et al. [51]	2019		Alsaffar et al. [112]	2020			
	S. Reddy [52]	2020						
			Multiple Keys	V. Kapoor [82]	2013			
Hybrid	Alison et al. [53]	2003		Ayele et al. [83]	2013			
	Ahmed et al. [108]	2011		Jahan et al. [84]	2015			
	Gupta et al. [54]	2012		R. Ghosh [85]	2016			
	R. Dhakar [55]	2012		Manu et al.[113]	2017			
	Verma et al. [56]	2014		A.E. Mezher [86]	2018			

cannot be used for authentication via digital signatures, unlike RSA, as the public key is solely used for encryption, whereas the private key is only for decryption. Dhakar *et al.* have shown that MREA is highly resistant to brute force attacks and conclusively provides higher security than standard RSA.

Verma and Garg [56] in 2014 put forward their solution of a hybrid variant of two previously enhanced RSA variants, the first variant is the Dual RSA small-d variant proposed by Sun *et al.* [28] in 2007, and the second variant is DRSA proposed by Pointcheval [24] in 1999. They have

TABLE 3. Algorithm analysis-and-evaluation of the Hybrid domain enhanced models.

Algorithm Model	Total Primes	Intermediate Variables	Encryption Scheme	Key Generation	Decryption Scheme	Features	Enhancement
Alison et al. [53]	k	Not Any	$C=M^E modN$	E = D−1 mod φ(N)	$M=C^D modN$	MPrime and Rebalanced RSA	Overall execution Time
Gupta et al. [54]	2	Not Any	$C=M^E modN$	E*D=1*modφ(N)	$M=C^D modN$	RSA and Diffie-Hellman	Security
R. Dhakar [55]	4	g	$C=g^{M\hat{}e \bmod n}*r^m \bmod m^2$	D= E^{-1}mod (m)	$M=(((C^E modm^2-1)/m)*Dmodm)^2 modn$	Homomorphic Encryption	Security
Verma et al. [56]	4	Not Any	C=M*R-1 mod N1	E = D−1 mod φ(N)	M=C*Rmod N1	Dual RSA and DRSA	Efficiency
Ahmed et al. [108]	2	Not Any	$C=M^E modN$	E*D=1*modφ(N)	$M=C^D modN$	RSA & ElGamal algorithm	Efficiency
Mahalle et al. [57]	2	PHI	$C=M^E modN$	E *D =1 (mod PHI)	$M=C^D modN$	RSA and AES	Security
Arora et al. [58]	3	K	C=K*M mod q	D* e=1 (mod Phi (n))	M = Q*K-1 mod q	RSA+ El-Gamal algorithm	Encryption Method
Karakra et al. [59]	2	R	R= M^2 mod N	E = D−1 mod φ(N)	$M=C^D modN$	Rabin and Huffman coding	Time
Panda et al. [60]	4	P1	$C=M^E modN$	E = D^{-1} mod (Ø (M) * P1)	$M=C^D modN$	Product of four prime-Hybrid RSA	Time
Jintcharadze et al. [61]	-	Not Any	$C=M^E modN$	E*D=1*modφ(N)	$M=C^D modN$	Twofish, AES, RSA and ElGamal	Security
Alamsyah1 et al. [109]	2	Not Any	$C=M^E modN$	f(n) = (p-1) * (q-1).	$M=C^D modN$	One Time Pad algorithm	Security

concluded that their solution consumes less memory and is also carries a less computational cost. As per the authors, this RSA variant is applicable in any field in which the system load is neither balanced nor memory-restricted. [108] offers a security-satisfying paradigm based on the RSA and El-Gamal cryptosystems together. The Integer Factorization Problem (IFP) is used in the RSA Cryptosystem, whereas the Discrete Logarithm Problem is used in the El-Gamal Cryptosystem (DLP). This approach is built on the merge of IFP and DLP to provide a good speed of computation for asymmetric cryptosystems based on the challenges of solving two well-known hard issues. As a consequence, the suggested system's calculation is more efficient than the El-Gamal and RSA algorithms. Moreover, in 2014, Mahalle and Shahade [57] proposed an RSA variant that utilizes the AES scheme and uses three keys, i.e., public key, private key and secret key. Their objective was to secure the upload of data on the cloud even when the admin is oblivious about the message. The authors have concluded that this AES-RSA hybrid will efficiently provide data security to the cloud users since the encrypted data can only be decrypted through the user's private and secret key. Arora and Pooja [58] proposed a novel algorithm that utilizes the hybrid of RSA with the El-Gamal asymmetric algorithm. The main objective was to increase the overall difficulty of factorizing by increasing overall. They conclusively stated that their proposal is higher in complexity and hence offers higher security, and also it is less prone to any factorization attacks in comparison to standard RSA.

In 2016, Karakra and Alsadeh [59] proposed another hybrid approach that also uses an asymmetric cryptosystem referred to as the Rabin algorithm along with Huffman Coding algorithm and finally merging them with RSA algorithm, and named it as A-RSA or Augmented RSA. They have shown that A-RSA makes factorization attacks harder and is less prone to related attacks, and furthermore, boosts up the average execution time of the algorithm. They concluded that A-RSA is faster in encryption-decryption phases, highly secure against block attacks and brute-force attacks, and it also results in shorter encoded text size. Similarly, Panda and Chattopadhyay [60] utilized four initial primes with reduced bit lengths and this proposal is motivated by previous recent trends as stated by the authors. The main goal of this proposal is to enhance the existing RSA in terms of security and performance. A recent hybrid implementation was proposed by Jintcharadze and Iavich [61] in the year 2020, who have proposed various hybrid models based on one symmetric algorithm plus one asymmetric algorithm and in this manner, they have proposed two different RSA hybrids, AES+RSA hybrid and Twofish+RSA. The authors have discussed their proposals via diagrams and experiments without actual algorithm inclusion. They have concluded that the RSA+Twofish variant is faster and also consumes low memory between the mentioned hybrid algorithms. [109] seeks to improve the method by merging RSA with the One Time Pad technique, resulting in a novel design that may be used to improve two-factor authentication security. The work's contribution is to develop a new scheme algorithm for an improved RSA scheme.

Above hybrid or cross versions includes the combination of RSA and one more algorithm or two more algorithms or any other mathematical hybrid approaches. In some of the discussed cases, researchers also combine two previously enhanced algorithms. We've discussed each of the 11 hybrid variants of RSA algorithms. Table 3 also illustrates all of the discussed hybrid variants of RSA in a classified manner highlighting their various parameters and shortcomings.

B. PARALLEL

To increase security or speed, several researchers have used parallel or multi-threading schemes. This section reviews all of the literature that has offered improved versions of the

RSA method that use a parallel approach in their solution. Each research is emphasized and analyzed according to the year it was proposed, ranging from 1993 to the most recent hybrid solution in 2019.

Chiou [62], in 1993, contrasts a novel modular exponentiation technique based on a parallel binary approach. The major goal was to minimize the time it took for modular exponentiation to run. This algorithm has a throughput that is roughly 33% faster than traditional ones due to a smaller number of iterations. Yunfeili [63] proposed Encrypt Assistant Multi-Prime RSA (EAMRSA). In modular exponentiation, this was accomplished by decreasing modules and private exponents. In constrained contexts, RSA can be slow since it is dependent on arithmetic modulo big integers. The study's major goal was to improve the speed of RSA decryption and signature. Although EAMRSA decreases the amount of processing required for decryption, it does so at the expense of encryption. In addition, Damrudi and Ithnin [64] suggested RSA encryption using a tree architecture in 2013 known as TRSA. Its parallel characteristics, such as scalability, connectivity processing components, degree, and diameter, are expressed using tree parallel architecture. Their parallel tree design employs higher security and speed. Exponentiations are separated into the number of nodes using tree design, allowing us to have a greater key which eventually increases the security. Saxena and Kapoor [65] enhanced the speed of the suggested RSA method in 2014 by utilizing two techniques: first, using the GMP library to execute modular computations on bigger numbers, and second, parallelizing it using OpenMP on the GCC infrastructure. They conclude that utilizing OpenMP in conjunction with GCC infrastructure and GNU's MP library improves parallel RSA results. In terms of time and energy, the parallel RSA is more efficient than the sequential variant.

In 2015, Asaduzzaman [66] investigated the effect of compute unified device architecture (CUDA) and Pthread on RSA decryption when big numbers are generated via homomorphic encryption. The major goal was to speed up the implementation of public key algorithms. The experimental findings show that the suggested CUDA-accelerated multithreaded solution has the ability to cope successfully with the RSA decryption difficulty. Saxena *et al.* [67] introduces an OpenMP-based RSA variant, which reduces execution time via parallel processing capability of multi-core architecture devices. The testing findings and graphical analysis show a significant speed increase. The suggested parallel solution was found to be almost as fast as GPU implementations, saving electricity and extra resource needs. Gupta *et al.* [68], in 2018, examined existing data encryption methods such as RSA, KB-APE, CP-APE, and AES on computational and storage costs basis in order to study about the differences in sequential and parallel RSA. At the data owner's side, all present methods have one or more issues with user revocation, access policy, ciphertext size, encryption and decryption overhead. They further presented an improvement technique for speeding up RSA encryption utilizing multi-threading on multi-core CPUs. Similarly, Ayub *et al.* [69] proposes an OpenMP-based parallel CPU-based implementation of the RSA algorithm to parallelize the algorithm's exponentiation process. Since exponentiation operations increase the computing time of the RSA algorithm's encryption and decryption processes, parallelizing these operations appears to be important to help quicker encryption-decryption. Their analysis concludes an improved performance in terms of the execution time of the program. Rawat *et al.* [70] presented an RSA method in 2019 that used a novel parallel data structure called Concurrent Indexed List of character blocks for performance improvement. The article offered three alternative simultaneous RSA implementations. With a speed-up factor of up to 4.5, the parallel RSA paradigm all implementation outperforms their respective sequential methods in terms of execution speeds.

We've discussed each of the nine variants of RSA algorithms that utilize parallel implementation or proposal. Table 4 also illustrates all of the discussed parallel variants of RSA in a classified manner highlighting their various parameters and shortcomings.

C. CLOUD

This section looks at all of the literature that has proposed improved versions of the RSA method that use cloud-focused enhancements. Each research is emphasized and analyzed according to the year it was published, beginning in 2013, with the most recent hybrid solution published in 2017.

In 2013, Moghaddam *et al.* [71] suggested an Efficient RSA (HE-RSA) for improving the security of encrypted data in cloud servers while consuming the least amount of time and cost during the encryption-decryption stages. According to the simulation findings, the overall execution time in HE-RSA was reduced by around 50% compared to the original RSA, which may be fair and acceptable given the security level and efficiency of HE-RSA. Patidar and Bhartiya [72] proposed a novel RSA variant in 2013 where the generated keys are saved offline before the procedure begins, which aims to increase overall speed. The given method begins with the sender retrieving the value of the database's public key indexes. The message is then encrypted using public key indexes and sent to the recipient. The value of private key indexes is retrieved by the receiver and stored in the database table alongside the sender's public key indexes. The message is eventually decrypted. The suggested method provides higher security as a consequence of the comparative results. Moreover, Bansal and Singh [73] presented a hybrid cryptosystem based on the RSA and Blowfish algorithms, which focuses on the security side of cloud computing. This method combines symmetric and asymmetric cryptography characteristics, and as a result, the method is an authentication-enabled procedure that improves cloud computing security and is also secure against brute force attacks.

Makkaoui *et al.* [74] proposed an improved RSA encryption method in 2017, which maintains the homomorphic feature and is more resistant to well-known RSA attacks.

TABLE 4. Algorithm analysis-and-evaluation of the Parallel domain enhanced models.

Algorithm Model	Total Primes	Intermediate Variables	Encryption Scheme	Key Generation	Decryption Scheme	Features	Enhancement
C. Chiou [62]	2	Not Any	$C=M^E modN$	$E = D-1 \bmod \varphi(N)$	$M=C^D modN$	Fast exponentiation	Time
Yunfei Li [63]	b	Not Any	$C=M^E modN$	$E = D \bmod \varphi(N)-1$	$M=C^D$	Encrypt Assistant Multi-Prime RSA	Speed
Damrudi et al. [64]	2	Not Any	$C=M^E modN$	$D= E^{-1} \bmod \varphi(N)$	$M=C^D modN$	Tree architecture	Speed and Security
Saxena et al. [65]	2	Not Any	$C=M^E modN$	$E= \bmod \varphi(N)$	$M=C^D modN$	GMP Library	Time and Energy
Asaduzzaman et al. [66]	2	Not Any	$C=M^E modN$	$E= \bmod \varphi(N)$	$M=C^D modN$	Unified device architecture and Pthread	Speed
Saxena et al. [67]	2	Not Any	$C=M^E modN$	$E= \bmod \varphi(N)$	$M=C^D modN$	OpenMP based algorithmic modification	Speed
Gupta et al. [68]	2	Not Any	$C=M^E modN$	$E= \bmod \varphi(N)$	$M=C^D modN$	Attribute based Encryption	Speed
Ayub et al. [69]	2	Not Any	$C=M^E modN$	$E= \bmod \varphi(N)$	$M=C^D modN$	Parallelization	Time and Security
Rawat et al. [70]	2	Not Any	$C=M^E modN$	$E= \bmod \varphi(N)$	$M=C^D modN$	Montgomery Reduction algorithm	Speed

TABLE 5. Algorithm analysis-and-evaluation of the cloud domain enhanced models.

Algorithm Model	Total Primes	Intermediate Variables	Encryption Scheme	Key Generation	Decryption Scheme	Features	Enhancement
Moghaddam et al. [71]	2	r	$C=((M^e modn)^e modn)$	$E*D=1 \bmod \varphi(N)$	$M= ((C^r modn)^d modn)$	RSA Small-e and Efficient RSA	Time
Patidar et al. [72]	3	Not Any	$C=M^E modN$	$E*D=1 \bmod \varphi(N)$	$M=C^D modN$	Architectural design	Security
Bansal et al. [73]	2	Not Any	$C=M^E modN$	$D= E^{-1} \bmod \varphi(n)$	$M=C^D modN$	Blowfish cryptosystem	Security
Makkaoui et al. [74]	2	Not Any	$C=M^E modN$	$E*D=1 \bmod \varphi(N)$	$M=C^D modN$	Homomorphic property	Security
Amalarethinam et al. [75]	2	Not Any	$C=M^E modN$	$E*D=1 \bmod \varphi(N)$	$M=C^D modN$	Cloud resources	Security
Makkaoui et al. [76]	3	Not Any	$C=M^E modN$	$E*D=1 \bmod \varphi(N)$	$M=C^D modN$	Homomorphic encryption	Time

Although it maintains a homomorphic feature, it is best suited for preserving the secrecy of data that has been outsourced to a third party. In 2017, Amalarethinam and Leena [75] presented a method that lowers the time it takes to encrypt and decrypt data. It splits the file into blocks and increases the key size to improve the algorithm's strength. Aside from boosting speed, using the improved method makes the computation more complicated and enhances the security strength. To speed up the Cloud-RSA [74] decryption, Makkaoui *et al.* [76] proposed a fast variation of the Cloud-RSA encryption method in 2017. The fast Cloud-RSA employs a modulus of the type $N = p^r q^s$ for r, $s \geq 2$. The simulation results demonstrate that the Fast Cloud-RSA method outperforms the Cloud-RSA encryption technique in terms of operating time while maintaining a defined security level.

We've discussed each of the 6 variants of RSA algorithms that utilize cloud-focused proposal and their implementation. Table 5 also illustrates all of the discussed parallel variants of RSA in a classified manner highlighting their various parameters and shortcomings.

D. IMAGE

Several studies in the field of image encryption have also been presented as possible improvements to the RSA method. Image-based RSA variants mainly focused on proposing modified RSA algorithms that may particularly improve the image encryption and decryption procedures. In this subsection, we'll look at a few of these suggestions in the years ranging from 2010 to 2020.

In [110], a novel RSA-based digital image encryption technique based on information concealing for sensor data security is presented to address the weaknesses of limited sensor node resources and security threats. To ensure data security, they collected sensitive information in a secure manner in order to make use of the benefit of information concealing techniques without encryption. The simulated tests show that using an existing WSN to transmit sensitive information surreptitiously with lower energy costs and invisibility is feasible and that it is suited for stream data in sensor nodes. Alsabti and Hashim [77] proposed a specific approach in the public key cryptosystem known as the RSA Cryptosystem in 2016, which is shown to be used over grey and colour images using the MATLAB Program. This method of encrypting and decrypting pictures using the RSA cryptosystem with minor changes is more resistant to assaults during image transmission in all agencies in the information age. In 2017, Jagadiswary and Saraswady [78] presented a novel method based on fused biometrics, namely fingerprint, finger vein, and retina, utilizing Modified RSA (MDRSA), a public key

TABLE 6. Algorithm analysis-and-evaluation of the Image domain enhanced models.

Algorithm Model	Total Primes	Intermediate Variables	Encryption Scheme	Key Generation	Decryption Scheme	Features	Enhancement
Zhao1 et al. [110]	2	Not Any	$C=M^E modN$	$D \equiv E^{-1} (mod\ \varphi\ (n))$	$M=C^D modN$	Transmission strategy	Security
Alsabti et al. [77]	2	Not Any	$C=M^E modN$	$D \equiv E^{-1} (mod\ \varphi\ (n))$	$M=C^D modN$	RSA Cryptosystem	Security
Jagadiswary et al. [78]	2	Not Any	$C=M^E modN$	$D \equiv E^{-1} (mod\ \varphi\ (n))$	$M=C^D modN$	Fused biometrics	Genuine Rate and False Rate
Cheltha [111]	2	Not Any	$C=M^E modN$	$D \equiv E^{-1} (mod\ \varphi\ (n))$	$M=C^D modN$	Honey encryption technique	Security
Shin et al. [79]	3	Not Any	$C=M^E modN$	$(E * D) \bmod \varphi\ (n) =1$	$M=C^D modN$	Private medical images	Encryption Capability and Elapsed Time
Huang et al. [80]	2	Not Any	$C=M^E modN$	$D \equiv E^{-1} (mod\ \varphi\ (n))$	$M=C^D modN$	Pixel confusion algorithm	Security
Jiao et al. [81]	2	Not Any	$C=M^E modN$	$D \equiv E^{-1} (mod\ \varphi\ (n))$	$M=C^D modN$	Generalized Arnold map	Security
Alsaffar et al. [112]	2	Not Any	$C=M^E modN$	$D \equiv E^{-1} (mod\ \varphi\ (n))$	$M=C^D modN$	AES	Image encryption quality

cryptosystem that can handle numeric and picture data. The simulation findings reveal that MDRSA has a greater genuine rate of 95.3 percent and a lower false rate of 0.01 percent than HIEA, which has a genuine rate of 92 percent and a false rate of 0 percent. A honey encryption method is utilized in [111] work for securely sharing public keys. While transferring a picture across a communication channel, the image may get damaged owing to noise; thus, noise in the encrypted image must be corrected. This article employs Hamming error correction and detection. Shin *et al.* [79] used the encryption and transportation of confidential medical images to enhance encryption capability and elapsed time. When compared to methods that employ two prime numbers that are not Mersenne prime numbers, it delivers better encryption in medical ultrasound imaging while sending images with appropriate elapsed durations.

Huang *et al.* [80] presented a novel asymmetric pixel confusion method for images in 2020, which was based on the Rivest-Shamir-Adleman (RSA) public-key cryptosystem and the Arnold map. The RSA method was used to create public and private keys, after which the image's pixels were jumbled. To increase the confusion effect, the Arnold confusion method was performed on the image blocks first, and then the complete image was confused. The experimental findings revealed that the suggested method is simple to use and has a high degree of confusion, with test values close to one. Jiao *et al.* [81] presented a novel image encryption technique based on an extended Arnold map and the Rivest–Shamir–Adleman (RSA) algorithm in his paper in 2020. To improve the security of image transmission, the RSA algorithm generates the key utilized in the image encryption technique. Fortunately, this algorithm's implementation is straightforward and efficient. Furthermore, the suggested asymmetric picture encryption system is safe and effective, with high key sensitivity and strong anti-attack capabilities, as demonstrated by experimental findings and testing. Reference [112] uses MATLAB to compare the Advanced Encryption Standard (AES) with RSA encryption methods in image encryption. The comparison is based on the quality of picture encryption for each technique. Furthermore, the results of the histogram and correlation analysis revealed that the AES method has a superior picture encryption quality with more convergent columns in the histogram.

A simple classification of all considered Image domain-based RSA variants is presented in Table 6.

E. MULTIPLE KEYS

This section examines all of the literature that has proposed better versions of the RSA technique that include multiple public or private keys. Each study is highlighted and analyzed based on the year it was published, with the most current solution being published in 2018.

In 2013, Kapoor [82] proposed a modified RSA method based on multiple public keys and n prime integer. They utilized a novel method involving n prime numbers and numerous public keys, which is difficult to break because all brute force assaults may get private keys. The suggested modified RSA method is utilized for systems that give greater security but less speed when compared to the RSA algorithm, as well as increasing data sharing security and efficiency across the network. Instead of sending the e value directly as a public key, Ayele and Screenivasarao [83] developed an efficient implementation of the RSA algorithm using two public key pairs and some mathematical logic. These two public keys are delivered separately, preventing the attacker from learning anything about the key and therefore decrypting the message. In 2015, Jahan *et al.* [84] presented a method that uses two public key pairs and some mathematical logic instead of delivering one public key directly. Though finding the factors of n and obtaining p and q, two large prime integers, is challenging, brute force attacks are more difficult in our proposed approach since the encryption keys are delivered individually rather than all at once. The suggested RSA algorithm is utilized in systems that require strong security but are slow. To improve security, Ghosh [85] produced an efficient implementation of the RSA algorithm based on two public

TABLE 7. Algorithm analysis-and-evaluation of the multiple keys domain enhanced models.

Algorithm Model	Total Primes	Intermediate Variables	Encryption Scheme	Key Generation	Decryption Scheme	Features	Enhancement
Kapoor [82]	2	Not Any	$C=M^{E}modN$	E *D mod ϊ (N) =1	$M=C^{D}modN$	Prime number and multiple public keys	Security
Ayele et al. [83]	2	a, b	$C=M^{b/a}$ modN	E*D=1*modφ(N)	$M=C^{D}modN$	Mathematical logic	Security
Jahan et al. [84]	2	Not Any	$C=M^{E}modN$	E*D=1*modφ(N)	$M=C^{D}modN$	Mathematical logic	Security
R. Ghosh [85]	4	a, b	$C=M^{b/a}$ modN	E*D=1*modφ(N)	$M=C^{D}modN$	Efficient implementation of RSA	Security
Manu et al. [113]	2	N2, D2	$C=(M^{E1}modN1)^{E2}mod N2$	E*D=1*modφ(N)	$M=(C^{D2}modN2)^{D1}$ modN1	Double encryption and decryption	Security
A.E. Mezher [86]	2	Not Any	$C=M^{E}modN$	E*D=1*modφ(N)	$M=C^{D}modN$	Multiple public and private keys	Security

keys in 2016. The modified RSA algorithm is a public key cryptography technique in which four prime integers, two public keys for encryption, and a private key for decryption are utilized. As a result, the public keys in this updated method are {b, n}, {a}, while the private key is {d, n}. The main rationale behind [113] work is that in a traditional RSA method, high-end systems can produce a private key by factoring modulus (n) into its prime values. As a result, they proposed using dual modulus to eliminate this flaw and significantly increase the system's security. Mezher [86], in 2018, devised and developed a way by employing multiple public and private keys. Their algorithm is more robust and resistant to brute force attacks than traditional algorithms. Furthermore, when alternative key sizes are utilized, the enhanced technique is about nine times slower to crack than the traditional approach.

We've discussed each of the 6 variants of RSA algorithms that utilize multiple Keys implementation or proposal. Table 7 also illustrates all of the discussed parallel variants of RSA in a classified manner highlighting their various parameters and shortcomings.

F. CHINESE REMAINDER THEOREM

CRT or the Chinese Remainder Theorem in cryptography is a method that is used to lower the total modular computations via the divide-and-conquer approach, which results in the boost of the overall mathematical calculations. Using the CRT approach, several authors have also proposed their RSA variant, which we'll discuss in this section. All the discussed algorithms will range from the year 2001 to the year 2019.

Wu *et al.* [87], in the year 2001, proposed a CRT based RSA variant and named it CRT-RSA. Their proposal is the implementation of a systolic RSA, which also uses Montgomery's algorithm apart from CRT. Wu's RSA variant resulted in better results for decryption and digital signatures, but their hardware implementation cost higher by 50%. Next, in the year 2003, Blömer *et al.* [88] presented another CRT-RSA, which focuses on solving fault attack problems on RSA based signature algorithms via CRT or Chinese Remainder Theorem. They mentioned that this CRT-RSA is majorly used in smartcard transactions, which is also more prone to such fault attacks. They have done a detailed analysis of their new proposal and concluded that their solution poses more security against such Bellcore attacks. The authors of [114] work propose four methods in which the user can choose the scale of the public key and private key. Scheme I and Scheme III encryption is at least 4.3 times quicker than the original rebalanced CRT-RSA encryption for a 1024-bit modulus, while Scheme II and Scheme IV encryption is at least 4.5 times faster. Scheme III and Scheme IV have somewhat lower decryption costs than the original rebalanced CRT-RSA, whereas Scheme I and Scheme II have slightly higher decryption costs. Reference [115] focused primarily on lowering the cost of decryption and signature creation. They experimented with a mix of Multi-Power RSA and Rebalanced RSA to see if they might improve things. The suggested technique (for key lengths of 2048 bits moduli) is theoretically 14 times quicker than RSA with CRT and 56 times faster than conventional RSA. Sony *et al.* [89] utilized multiple keys and the Chinese Remainder Theorem with an aim to boost the data transmission security by increasing the processing time and algorithm security. They concluded that their CRT based solution is more secure if used with a two-key method as per their proposed algorithm. Lastly, in 2019, Abdeldaym *et al.* [90] used two public keys and CRT. Their model uses four primes and sends two public keys to the receiving side, and to balance out the execution speed and performance, they have used the Chinese remainder Theorem. They concluded that their solution is better than RSA in decryption and reduces the computation cost while taking a higher execution time than standard RSA.

Of all the four discussed CRT based RSA variants, their algorithm analysis is illustrated via Table 8 based on certain algorithm parameters and their suggested shortcomings.

G. DIGITAL SIGNATURES

Several authors have also focused their RSA research on the domain of Digital Signatures, implying that they have enhanced the RSA algorithm in such a way so that the process of digital signature gets efficient in terms of security or performance or any other parameter, since in public key infrastructure, digital signatures play a major role. In this section, we'll review all of such research starting from the initial RSA variant implementation from the year 1980.

TABLE 8. Algorithm analysis-and-evaluation of the CRT domain enhanced models.

Algorithm Model	Total Primes	Intermediate Variables	Encryption Scheme	Key Generation	Decryption Scheme	Features	Enhancement
Wu et al. [87]	4	Not Any	$C=M^E \text{mod} N$	$E*D=1 \text{mod} \varphi(N)$	$M=C^D \text{mod} N$	Modular exponentiation algorithm	Suitable for Decryption
Blomer et al. [88]	2	Not Any	$C=M^E \text{mod} N$	$E*D=1 \text{mod} \varphi(N)$	$M=C^D \text{mod} N$	New algorithm against the Bellcore attack	Security
Ou [114]	2	Not Any	$C=M^E \text{mod} N$	$E*D=1 \text{mod} \varphi(N)$	$M=C^D \text{mod} N$	CRT-RSA, multi-factor RSA, and rebalanced RSA	Cost and Time
Garg et al. [115]	2	Not Any	$C=M^E \text{mod} N$	$E*D=1 \text{mod} \varphi(N)$	$M=C^D \text{mod} N$	MultiPower RSA and Rebalanced RSA.	Time
Sony et al. [89]	2	Not Any	$C=M^E \text{mod} N$	$E*D=1 \text{mod} \varphi(N)$	$M=C^D \text{mod} N$	Multiple Public and Private keys	Security
Abdeldaym et al. [90]	2	Not Any	$C=M^E \text{mod} N$	$E*D=1 \text{mod} \varphi(N)$	$M=C^D \text{mod} N$	Circuit topology	Computational Cost

TABLE 9. Algorithm analysis-and-evaluation of the digital signature domain enhanced models.

Algorithm Model	Total Primes	Intermediate Variables	Encryption Scheme	Key Generation	Decryption Scheme	Features	Enhancement
Williams [116]	2	Not Any	$C=M^E \text{mod} N$	$E*D=1 \text{mod} \varphi(N)$	$M=C^D \text{mod} N$	Broken into operations	Security
Si et al. [91]	2	Not Any	$C=M^E \text{mod} N$	$D= E^{-1} \pmod{(p-1)(q-1)}$	$M=C^D \text{mod} N$	Numeric operation function	Time
Jaju et al. [92]	3	Not Any	$C=M^E \text{mod} N$	$D \equiv E^{-1} \pmod{\emptyset(n)}$	$M=C^D \text{mod} N$	Process data of different sizes	Security
Aufa et al. [93]	2	G,u1,u2	$r=(g^k \bmod p) \bmod q$	$D \equiv E^{-1} \pmod{\emptyset(n)}$	$v=((g^{u1}.y^{u2}) \bmod p) \bmod q$	Digital Signature Algorithm	Time

The goal of [116] was to propose a modified version of the RSA scheme in which the cipher's breaking may be reduced to the issue of factoring a big integer R of a specific type. If the integer R used in the modulus can be factored, the RSA public-key encryption method can be cracked. It is feasible, however, to brew& this method without taking R into account. The RSA scheme is modified in this paper. In 2010, Si *et al.* [91] suggested an efficient RSA signature variant which is more complex in mathematical terms, and its objective is to handle it on low-end storage and devices and also improve the signature process. Conclusively, they have stated that their proposal can generate a 1024-bit RSA Key on any normal PC within 120 seconds, while encryption or decryption can be done in less than 2 seconds. Furthermore, Jaju and Chowhan [92] enhanced the security of digital signatures through RSA. Their RSA variant uses three primes, and their modulus n is not transmitted with the public or private key. They have concluded that in spite of having a higher time complexity of their algorithm, security is highly increased. In 2018, Aufa *et al.* [93] combined RSA 1024 and Digital Signature algorithms to improve security and performance. Their implementation showed that key generation time is relatively high, while the encryption and signature process is faster by 60%. They also concluded that their proposal provides digital signatures more safely and faster.

Table 9 also differentiates all 4 above discussed digital signature variants considering their algorithm parameters and their shortcomings.

H. K NEAREST APPROACH

Similar to CRT based RSA variants, researchers have also used the K-Nearest approach to improve the efficiency of the standard RSA algorithm. In this section, we'll discuss some RSA variants that use the K Nearest algorithm for their proposals.

In 2015, Hussain [94] put forward an RSA scheme with an aim to eliminate and lessen the number of redundant text occurrences. They pointed that for some n values, the corresponding encoded text could be the same, which offers more vulnerability. They applied K Nearest neighbour of either or both primes in the algorithm in order to enhance the security. They also mentioned that their algorithm sends only e exponent to the receiver, not modulus n. They also suggested frequently changing the nearest neighbour distance for more security purposes. Mathur and Gupta [95] in 2016 proposed to secure data exchanges, and their variant includes an exponential type of RSA that takes advantage of the K Nearest neighbour algorithm, four primes and two public keys. They have stated several advantages of their proposal over standard RSA algorithm that it's less prone to brute force attacks, lower execution time, more reliable for huge files, and overall, it offers more security and efficiency. Again in 2017, Mathur *et al.* [96] suggested using exponential powers, n primes approach and the KNN model. Through several analyses, they concluded that their proposal enhances randomness of the computed encoded message, and it also converts the message to its respective ASCII values, which

TABLE 10. Algorithm analysis-and-evaluation of the KNT domain enhanced models.

Algorithm Model	Total Primes	Intermediate Variables	Encryption Scheme	Key Generation	Decryption Scheme	Features	Enhancement
A.K. Huussain [94]	2	Not Any	$C=M^{E}modN$	E *D mod Ï (N) =1	$M=C^{D}modN$	Eliminate the redundant messages	Security
Mathur et al. [95]	2	Not Any	$C=M^{b/a}$ modN	E*D=1*modφ(N)	$M=C^{D}modN$	Data exchange	Security and Time
Mathur et al. [96]	n	Not Any	$C=M^{E}modN$	$D \equiv E^{-1}$ (mod Ø (n))	$M=C^{D}modN$	Exponential powers, n prime numbers, multiple public keys	Security and Time

TABLE 11. Algorithm analysis-and-evaluation of the Batch domain enhanced models.

Algorithm Model	Total Primes	Intermediate Variables	Encryption Scheme	Key Generation	Decryption Scheme	Features	Enhancement
A. Fiat [97]	2	Not Any	$C=M^{b/a}$ modN	E*D=1*modφ(N)	$M=C^{D}modN$	Distributed Batch RSA process	Enhancement in the several encryption exponents
Liu et al. [98]	2	Not Any	$C=M^{b/a}$ modN	E*D=1*modφ(N)	$M=C^{D}modN$	Batch Encrypt Assistant Multi-Prime RSA	Performance Improvement in the Exponentiation Phase

further boosts up the complexity. Their proposal is faster in the encryption-decryption stages and enhances the overall security.

There is a total of 3 modified RSA variants that utilize the KNN approach. Table 10 represents their algorithm analysis in a detailed and classified manner.

I. BATCH

Batching is a process that distributes any whole task in several batches or sets. The first Batch variant of RSA was proposed by Fiat [97] in the year 1997, and then one more of its variants was proposed, which we will discuss in the following paragraphs.

Fiat [97] proposed the first Batch RSA comprised of two noteworthy properties. The first is that his variant operates effectively on multiple modular exponentiations at the expense of just sole modular exponentiation, which eventually results in a fast RSA-based scheme. The second property of Batch RSA is that it offers distributive property that would segregate the private key from the system, no matter what the system sizes or the total number of executable operations. Fiat also compared his Batch RSA with other schemes. He also stated that this Batch RSA would be at a disadvantage in two-way communications. He mentioned that relative to standard RSA, the Batch variant is at an advantage since it utilizes several encryption exponents. Later in 2010, Liu *et al.* [98] followed above discussed Fiat's and Boneh and Shacham [25] method and proposed two different Batch named BEARSA (Batch Encrypt Assistant RSA) and BEAMRSA (Batch Encrypt Assistant Multi-Prime RSA), respectively. BEARSA is an upgraded variant of Batch RSA itself, and the computation phase follows the binary-tree approach and is performed in two stages, i.e., leaf to root tree traversal and again the reverse process. BEARSA also executes the full exponentiation process via four stages, i.e., Setup, Percolate-Up, Exponentiation-Phase and Percolate-Down. Another variant is BEAMRSA, which is itself an enhancement to BEARSA, and it uses the Multi-prime RSA scheme of Boneh and Shacham [25]. They concluded that BEARSA shifts several decryption computations to the process of encryption and hence speeds up the decryption phase. While BEAMRSA also does the same shifting process as BEARSA, but additionally it also reduces the modulus N during the modular exponentiation. The authors finally guarantee for higher decryption rate and reliable security.

Above discussed 2 of the literatures mentioning Batch RSA approaches and their implementation. Table 11 also elaborates their algorithm in a more extracted manner.

J. WIRELESS

Several methods have been proposed in the domain of wireless networks or WSN focusing on the RSA algorithm. In this section, we will consider a couple of such proposals which lies in the year 2007 and 2021.

In the year 2007, Frunza and Scripcariu [99] have proposed an improvised RSA variant to further increase the security of wireless transmissions. Their proposal is based on the concept of AFF (Algebraic Finite Field). In order to boost computational speed and security level, they utilize the maximum acceptable size of the encryption key, which also allows the performance efficiency of the processor. They have conclusively stated that partial exchange of keys can be done on public channels. A recent version named PSRSA was proposed by Shin [100] in 2021, which they named as PSRSA focuses on the applications within small systems like Wireless Body Area Networks and enhancing the security. The proposal's experimented results state that it could be helpful in preventing more attacks.

A more detailed structural analysis of the above 2 discussed Wireless domain-based RSA variants are represented in Table 12.

K. CORE-MODIFICATIONS

This domain comprises of all sub-domains which initially consists of algorithms having mathematical modifications,

TABLE 12. Algorithm analysis-and-evaluation of the Wireless domain enhanced models.

Algorithm Model	Total Primes	Intermediate Variables	Encryption Scheme	Key Generation	Decryption Scheme	Features	Enhancement
Frunza et al. [99]	2	Not Any	$C=M^{b/a}$ modN	E*D=1*modφ(N)	$M=C^{D}$modN	Optimized encryption method	Efficiency
S. Shin [100]	2	Not Any	$C=M^{E}$modN	φ(N)=lcm(p-1,q-1)	$M=C^{D}$modN	Full security protocol designed for	Security

TABLE 13. Algorithm analysis of standard RSA.

Algorithm Model	Total Primes	Intermediate Variables	Encryption Scheme	Key Generation	Decryption Scheme	Features	Enhancement
Rivest et al. [20]	2	Not Any	$C=M^{E}$modN	$E\cdot D \equiv 1 \pmod{(p-1)\cdot(q-1)}$	$M=C^{D}$modN	Standard RSA	Standard RSA

or modifications to improve security and performance. The first algorithm we're considering in this domain is the standard RSA algorithm itself, on the basis of which this survey is based upon. Some other algorithms are also fast variants, whereas some papers include more than one proposed modified algorithm which we'll cover in this section. This section covers up the proposed RSA variants ranging from the year 1978 up to the year 2020.

1) STANDARD RSA

Rivest *et al.* proposed a new public key algorithm in 1978 focused onto obtain Digital Signatures and named it as RSA algorithm [20]. They have concluded that the whole security of RSA is based upon the large primes factorization. As a whole, this RSA algorithm is one of the most popularly used asymmetric key cryptographic algorithms in today's modern period, even though having some vulnerabilities. Several essential parameters of the standard are mentioned in Table 13.

2) FAST VARIANTS

In 1982, Quisquater and Couvreur [21] proposed a fast decryption scheme as an upgrade to the RSA cryptosystem. They have identified some vulnerabilities in the standard RSA and presented their deciphering method of RSA that utilizes an improved modular exponentiation approach and is based on the Chinese Remainder Theorem with an aim to increase its overall performance time.

In 1998, Takagi [22] presented an algorithm that uses the modulo as $p^{k}q$ (as modulus in standard RSA is pq). Their goal was to improve the performance and security of existing RSA, and they concluded that their proposed fast variant offers higher decryption speed than the Quisquater's [21] RSA algorithm. Additionally, their private keys consisted of 3 private exponents, whereas plaintext can be fetched through the Chinese Remainder Theorem. In the year 2002, Boneh and Shacham [25] suggested four different fast variants and named them as Batch RSA, Multi-Prime RSA, Multi-Power RSA and Rebalanced RSA. Their survey was aimed to speed the decryption execution and backwards compatibility in comparison to standard RSA. Their conclusion on his variants was that they can be combined for an additional boost in speed and can also use modular exponentiation and multiplication for their enhanced performance. Moreover, Chaudhury *et al.* [45] updated the RSA cryptosystem method "Asymmetric key Based Cryptographic Algorithm using Four Prime Numbers to Secure Message Communication (ACAFP)" in 2017 to handle four prime numbers while maintaining security. Four prime numbers are difficult to disintegrate, resulting in improved network effectiveness. Table 14 summarizes the algorithms of all the discussed fast variants.

3) INTEGRATED SCHEMES

Aboud *et al.* [29] in 2008 presented an RSA scheme on the basis of a linear algebraic group on the ring of integer mod n, where n is the generated modulus. They have stated that since RSA is fundamentally a block cipher, thus they generalized it and concluded it to be a more reliable and effective solution. Bahadori *et al.* [30] focused on smart cards, which offers a faster generation of public-private key pairs. Their proposal is an approach for large random primes generation, which is a major component of the RSA cryptosystem. They concluded that this solution reduces the overall key generation time and hence overall efficiency. Sharma *et al.* [32] in 2011 proposed MSSRPKC, which is a modified subset-sum over RSA system in order to increase the security level, as they have concluded that Brute force and Shamir attacks are not efficient against their proposal. They also stated that their solution is ineffective in the authentication process since it utilizes a one-way function. Mo *et al.* [42] presented a solution that hides the public key and keeps it out of public channels. As a result, not only can RSA's security characteristics be preserved, but traditional RSA's security may be considerably enhanced.

In 2018, Chakraborty *et al.* [47] investigated the performance of an Artificial Neural Network (ANN)-based RSA method in order to reduce RSA execution time. The results of simulations demonstrate that neural network-based RSA outperforms the standard RSA method. In a recent study, Reddy [52] presented a new type of public key cryptography system that is roughly four times more efficient in data storage and operating time than RSA and has a security

TABLE 14. Algorithm analysis of the fast variant models.

Algorithm Model	Total Primes	Intermediate Variables	Encryption Scheme	Key Generation	Decryption Scheme	Features	Enhancement
Quisquater et al. [21]	2	Not Any	$C=M^E \text{mod} N$	$E \cdot D \equiv 1 \pmod{(p-1)\cdot(q-1)}$.	$M=C^D \text{mod} N$	Deciphering cryptograms	Decryption Time
T. Takagi [22]	2	Not Any	$C=M^E \text{mod} N$	$E \cdot D \equiv 1 \pmod{(p-1)\cdot(q-1)}$.	$M=C^D \text{mod} N$	Elliptic curve method	Decryption Time
Boneh et al. [25]	2	Not Any	$C=M^E \text{mod} N$	$E \cdot D \equiv 1 \pmod{(p-1)\cdot(q-1)}$.	$M=C^D \text{mod} N$	Backwards compatibility	Speed
Chaudhury et al. [45]	4	Not Any	$C=M^E \text{mod} N$	$(E * D) \bmod f(n) = 1$	$M=C^D \text{mod} N$	Four Prime + Secure	Security

TABLE 15. Algorithm analysis of the integrated schemes of RSA.

Algorithm Model	Total Primes	Intermediate Variables	Encryption Scheme	Key Generation	Decryption Scheme	Features	Enhancement
Aboud et al. [29]	2	Not Any	$C=M^E \text{mod} N$	$D \equiv E^{-1} \pmod{\emptyset(n)}$	$M=C^D \text{mod} N$	Linear group	Reliable and Effective
Bahadori et al. [30]	2	Not Any	$C=M^E \text{mod} N$	$D \equiv E^{-1} \pmod{\emptyset(n)}$	$M=C^D \text{mod} N$	Generating large random prime numbers	Time and Efficiency
Sharma et al. [32]	2	Not Any	$C=M^E \text{mod} N$	$D \equiv E^{-1} \pmod{\emptyset(n)}$	$M=C^D \text{mod} N$	Modified Subset-Sum	Security
Mo et al. [42]	2	Not Any	$C=M^E \text{mod} N$	$(E * D) \bmod f(n) = 1$	$M=C^D \text{mod} N$	Discrete sliding mode controller	Security
Chakraborty et al. [47]	2	Not Any	$C=M^E \text{mod} N$	$(E * D) \bmod f(n) = 1$	$M=C^D \text{mod} N$	Artificial Neural Network	Time
S. Reddy [52]	2	Not Any	$C=M^E \text{mod} N$	$(E * D) \bmod f(n) = 1$	$M=C^D \text{mod} N$	Strong pseudo prime test	Security

complexity that is possibly one-fourth that of RSA. Only one of the powerful pseudo prime tests, the Rabin- Miller test, makes this new crypto scheme viable. As a result, they called it RM-RSA. Table 15 presents several parameters considering all of the discussed integrated schemes.

4) SECURITY FOCUSED

Pointcheval [24] put forwarded RSA variant in 1999, named as Dependent-RSA or DRSA and is based on 'dependent RSA problem'. They included two additional versions of DRSA itself, based on decisional dependent RSA and extraction dependent RSA problems, and named as DRSA-1 and DRSA-2. They proved DRSA to be semantically secure to chosen plaintext attacks. Their proposal follows the same key generation as of RSA, but encryption-decryption varies. In 2007, Sun *et al.* [28] Dual RSA, whose algorithm of key generation results in two different pairs of keys, both having the same private and public components. They have stated that applications of blind signatures and authentication can be utilized via Dual RSA. They have finally concluded that Dual RSA is most effective in cases where memory reduction is more prior than computation costs. Next, Chhabra and Mathur [31] in 2011 have suggested an algorithm that offers higher security as there is no transmission of modulus n in their approach, and they claim their solution to overcome standard RSA in security terms. Another proposal of 2012 by Nagar and Alshamma [35] aims to boost the execution time of the RSA algorithm via a novel key generation scheme named as RSA-Key Generation Offline, which stores the keys in the database indexed tables before encryption-decryption stages. Their solution proposes four stages of security, each consisting of their own databases, whereas such levels are recognized via key sizes and public exponent e. They state their solution as a faster version compared to standard RSA.

Al-Hamamai and Aldariseh [33], in 2012, have put forward an enhanced RSA algorithm that uses three primes instead of two in order to improve the complexity and hence security. They have concluded that their proposal increases the analysis difficulty of the modulus n and also enhances the overall speed. Furthermore, Pradhan and Sharma [36] proposed a security upgrade in 2013, recommending the use of randomized parameters in the encryption process to make RSA resistant to many of the attacks documented in the literature; this change made RSA semantically safe. Meneses *et al.* [40] published a study in 2016 that attempts to improve the security, integrity, and availability of information by optimizing the RSA encryption method. They created and developed a general system that could encrypt and decrypt data, improving the efficiency and security of messages sent over the network. The results demonstrate the RSA algorithm's efficiency and usefulness in terms of information security.

To improve the security of RSA, Aiswarya *et al.* [46] presented a new encryption method called Binary RSA Encryption Algorithm (BREA) in 2017. The security of BREA is further enhanced by transforming the MREA-encrypted cypher text into binary code format. As a result, the intruder will have a tough time decrypting the data. By modifying the original RSA method, Sahu *et al.* [44] presented a technique in 2017 that is more secure than the

TABLE 16. Algorithm analysis of the security focused schemes of RSA.

Algorithm Model	Total Primes	Intermediate Variables	Encryption Scheme	Key Generation	Decryption Scheme	Features	Enhancement
D. Pointcheval [24]	2	k	$C=M(k+1)^E modN$	$D \equiv E^{-1} (mod \emptyset (n))$	$M=C(k+1)^E modN$	Decisional Dependent–RSA Problem	Security
Sun et al. [28]	2	Not Any	$C=M^E modN$	$D \equiv E^{-1} (mod \emptyset (n))$	$M=C^D modN$	Key storage reduction	Memory Reduction
Chhabra et al. [31]	2	Not Any	c = m ^ kp mod (d)	D E ≡mod Ø (n)	m = [c ^ ks mod (d)] ^ ½	Eliminates 'n' transfer	Security
Nagar et al. [35]	2	Not Any	$C=M^E modN$	(E * D) mod f (n) =1	$M=C^D modN$	Indexes Exchange	Time
Al-Hamami et al. [33]	3	Not Any	$C=M^E modN$	$D \equiv E^{-1} (mod \emptyset (n))$	$M=C^D modN$	Use of additional third prime number	Security
Pradhan et al. [36]	2	Not Any	$C=M^E modN$	$E * D \equiv 1 (mod \varphi(n))$.	$M=C^D modN$	Randomized parameters	Security
Meneses et al. [40]	2	Not Any	$C=M^E modN$	(E * D) mod f (n) =1	$M=C^D modN$	Asymmetric cryptographic algorithms	Efficiency
Aiswarya et al. [46]	4	g, r	C= g^(M^(e) mod n)×((r^m) mod (m^2))	$D \equiv E^{-1} (mod \emptyset (n))$	M = ((((c ^mod (m^2)) – 1)/ m) x μ mod m)^d)mod n	Binary RSA Encryption Algorithm	Security
Sahu et al. [44]	2	Not Any	$C=M^E modN$	(E * D) mod f (n) =1	$M=C^D modN$	Eliminates 'n' transfer	Security
Barazanchi et al. [51]	2	Not Any	$C=M^E modN$	(E * D) mod f (n) =1	$M=C^D modN$	Increased complexity	Security

original. The method avoids the need to store n, the product of two random prime integers, in the public key, making it harder for an intruder to guess the factors of n and therefore keeping the encrypted message secure from prying eyes. In 2019, Barazanchi *et al.* [51] focused on the RSA method by increasing the difficulty of the 3keys (3k). This modification improved the algorithm's security and complexity while keeping the encryption and decryption times the same. In addition, the study describes a method for enhancing cryptographic security using public key encryption. The testing findings showed that the suggested technique for three keys retrieves encoded text with a low error rate. Security focused RSA variants are summarized in Table 16.

5) MATHEMATICAL MODIFICATIONS

In 1998, Collins *et al.* [23] presented one of the initial versions of RSA variants that utilize k random large primes instead of 2, i.e., $k > 2$. Their objective was to increase the computational speed of the algorithm. Moreover, Twin RSA was presented by Lenstra and Weger [26] in the year 2005, which aims to attain the matching 'compression ratio' for RSA moduli in a more efficient manner, which could offer higher security as well. As per the authors, the term twin implies the moduli pair generated by the proposed algorithm. They initially utilized the integer difference property of the Chinese Remainder Theorem. Galbraith *et al.* [27] presented a key generation technique to lessen the overall encryption-decryption cost on the applications, and this solution is more applicable where operations cost matter. They also have cryptanalysis their proposal for security checks. Ivy *et al.* [34] devised another n-primes based RSA cryptosystem in 2012 that simply utilizes n primes instead of 2. Key generation, encryption, and decryption phases are the same as of standard RSA except for the number of primes. They concluded that their solution improves the overall security.

Minni *et al.* [37] introduced a modified RSA method with improved security in 2013. The removal of n from the original RSA method is the security feature here. Instead, both keys can utilize the freshly created substitute for n. With a minor increase in time complexity, the technique proposed in this work removes this problem, making it safer. Besides, Patel and Shah [38] examined several techniques for quicker implementation of the RSA algorithm that had been updated by various academics and scholars. In order to produce a high-speed implementation of the RSA algorithm, they employed a variety of approaches and methodologies. The proposed approach reduced the traditional algorithm's factoring complexity by at least six times. Thangavel *et al.* [39] presented an approach in 2015 that uses four large prime numbers, increasing the system's complexity above the standard RSA technique, which uses just two large prime numbers. The public component n is the product of two big prime numbers in the proposed Enhanced and Secured RSA Key Generation Scheme (ESRKGS), while the values of the Encryption (E) and Decryption (D) keys are based on the product of four large prime numbers (N), making the system very safe. As a result, the system is extremely secure and difficult to crack. Kumar and Chaudhary [41] used a method based on n prime numbers and bit stuffing in 2016. Because big prime numbers are difficult to factorize, they employ n prime numbers in this approach, and bit stuffing adds an extra layer of encryption, ensuring maximum security and efficiency for data sent over the network.

Somsuk [43] suggested an enhanced RSA decryption technique called as New Private Key of RSA (d-RSA) in 2017 to minimize the decryption process's calculation cost. The objective is to create a new private key with low Hamming weight while keeping the public key and modulus values

TABLE 17. Algorithm analysis of the mathematically modified RSA variants.

Algorithm Model	Total Primes	Intermediate Variables	Encryption Scheme	Key Generation	Decryption Scheme	Features	Enhancement
Collins et al. [23]	k	Not Any	$C=M^E modN$	$E\cdot D \equiv E^{-1} (\text{mod } (p_1-1)\cdot(p_2-1)\ldots)$.	$M=C^D modN$	Inventive method.	Computational Speed
Lenstra et al. [26]	2	Not Any	$C=M^E modN$	(E * D) mod f (n) =1	$M=C^D modN$	Twin RSA	Security
Galbraith et al. [27]	2	Not Any	$C=M^E modN$	$D \equiv E^{-1} (\text{mod } Ø\ (n))$	$M=C^D modN$	Small public exponents	Security
Ivy et al. [34]	2	Not Any	$C=M^E modN$	(E * D) mod f (n) =1	$M=C^D modN$	'n' primes	Security
Minni et al. [37]	2	k1, k2	$C= M^{k1}$ Mod(X)	k1 x k2 Mod (X) = 1	$M = \sqrt{(C^{k2}}$ Mod(X))	Conditional public-component generation	Security
Patel et al. [38]	2	Not Any	$C=M^E modN$	(E * D) mod f (n) =1	$M=C^D modN$	6X secure than RSA + High Decryption time	Security and Time
Thangavel et al. [39]	4	Not Any	$C=M^E modN$	$D \equiv E^{-1} (\text{mod } Ø\ (n))$ E1	$M=C^D modN$	Four large prime numbers	Security
Kumar et al. [41]	2	Not Any	$C=M^E modN$	$D \equiv E^{-1} (\text{mod } Ø\ (n))$	$M=C^D modN$	Bit stuffing	Security
Somsuk [43]	2	d	$C=M^E modN$	(E * D) mod f (n) =1	$M = (C^d \text{ mod } n)^{1/x}$	Better for lightweight devices	Speed
Islam et al. [48]	2	Not Any	$C=M^E modN$	(E * D) mod f (n) =1	$M=C^D modN$	3 component keys	Efficiency and Security
Raghunandhan et al. [49]	4	Not Any	$C=M^E modN$	(E * D) mod f (n) =1	$M=C^D modN$	Modulus n elimination	Security
Yadav et al. [50]	2	k1, k2	$C= M^d$ Mod(X)	k1 x k2 Mod (X) = 1	$M = \sqrt{(Cd}$ Mod(X))	Modulus n elimination	Security

the same. In 2018, Islam *et al.* [48] presented a cryptosystem based on ''n;; unique prime numbers. Two distinct public keys and private keys are produced from the big factor of the variable ''N'' in this technique, and a double encryption-decryption process is performed, which provides additional security. As a result, this method is more efficient, secure, and difficult to crack. Raghunandan *et al.* [49] developed a method that uses a fake public key exponent f instead of e and modulus X instead of 'n' to raise the factoring difficulty of public keys. The advantages of this approach outweigh the disadvantages of the integer factorization attack. Yadav *et al.* [50] presented a technique in 2018 by removing the requirement to send n, the product of two random prime numbers, in the public key, making it impossible for an intruder to guess the factors of n and thereby protecting encrypted messages from assault.

Table 17 analyses each of the discussed mathematically modified algorithms in a more classified manner considering all the undertaken parameters.

We have discussed a total of 33 ''Core-Modifications'' domain algorithms, in which several sub-domains or focused areas are discussed, initially after discussing Standard RSA. We comprised four variants in the Fast Variants sub-section, six variants in the Integrated Models sub-section, ten variants in Security Focused sub-section, and finally, 12 variants in the Mathematical modification sub-section, including the initial standard RSA algorithm.

V. FINDINGS AND INDICATIONS

In this section, we will be considering the overall findings of our study, which relies on the basis of the above conclusive

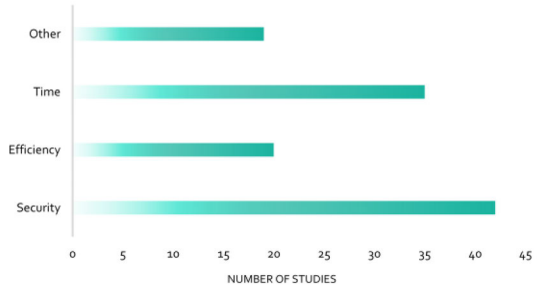


FIGURE 6. Enhancement Types in all considered RSA variants.

studies, observed trends in those domains of the studies, comparative analysis and analytical assessment followed by the discussion and deliberations among all the authors. The considerable findings of our under-studied literature are summarized as follows:

- Among all the distribution of the algorithms depicted in Fig. 5, we can easily notice that the Hybrid domain, Parallel domain and Mathematical modifications in the ''Core-Modifications'' domain are the most popular domains as far as RSA variant proposals are concerned.
- Overall execution speed and relative security are the most common objectives of all the under-studied literature, as can be depicted from Table [3-17], while some fewer common objectives include the enhancement of RSA in respect to a particular domain like Cloud, Image or Wireless areas.
- Since the standard RSA proposal in 1978, its initial yearly research in RSA's enhancements was quite less in

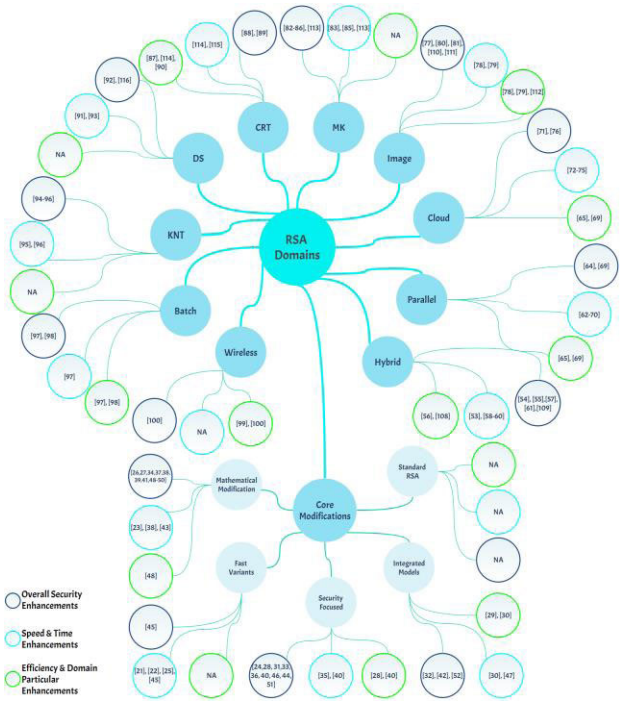


FIGURE 7. Taxonomy of Enhancements in each considered Domains of RSA variants.

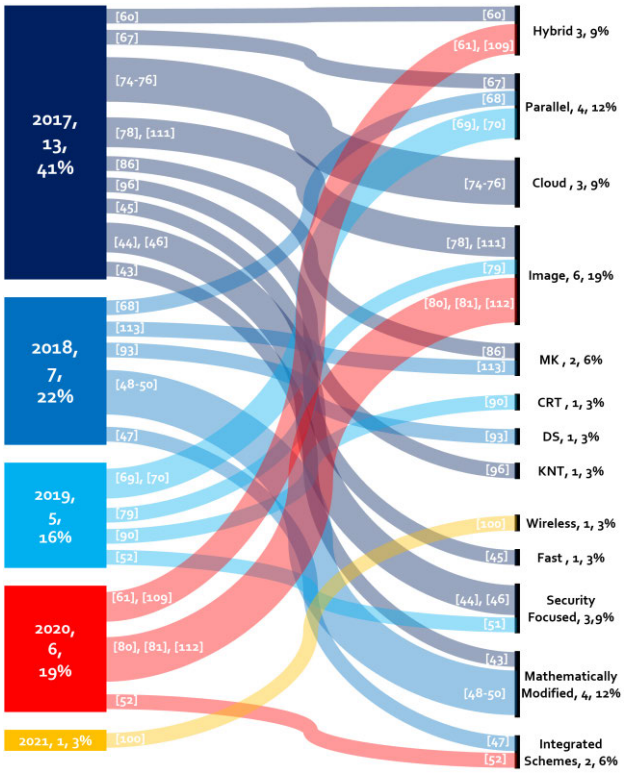


FIGURE 8. Classification of most prominent domains of last 5 years (2017-2021).

number, but recently, like from the 2010 year onwards, it can be seen from Fig. 4 and Fig. 9 (which represents the trend of RSA areas in various domains on a yearly basis) that there has been a huge increment in those RSA enhancements, as the year 2017 itself only showed a total of 10 proposals, whereas, from 1978 up to 2003, there was a total of 10 enhancements.

- Most of the studied literature were able to achieve their objective whether in terms of security enhancement or execution speed/time enhancement (Fig 6), and it can be seen that most of them are able to resolve the existing limitations and issues as mentioned in their studies, which is also shown in Table 19 of Appendix A.
- The least explored domains include the ones as Wireless and Batch variants, as is depicted in the domain distribution of Fig 5. The Wireless and Image domains are good areas to extend further RSA research, as the trend shown in Fig 4 and Fig 9 that such studies were made in Wireless and Image domains only in the later years.
- Of all the RSA proposals focusing on increasing the security levels, most of them try to increase the

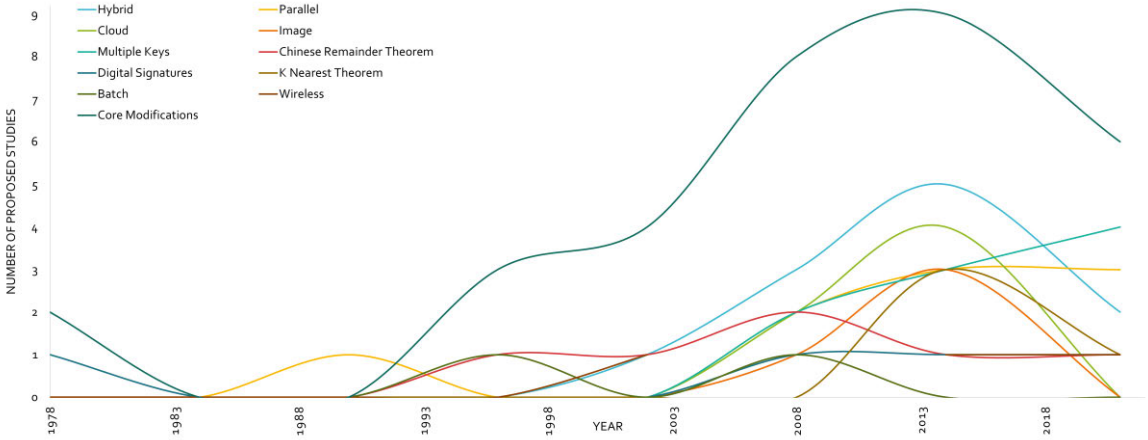


FIGURE 9. Domain trend depicting growth and downfall for each RSA variants from 1978 to 2021.

algorithm complexity, which subsequently increases the overall time to break the proposed cipher, hence in this way, their proposal implies higher security in comparison to the standard RSA algorithm.

Our findings indicate that RSA variants in the domains like ''Core-Modifications'', Hybrid and Parallel have the highest publication frequency and represent the most adaptable researches, and as extracted from Tables 3-12, most of such proposals improve the security by increasing the algorithm complexity (Fig. 7 represents the enhancement made in each considered domain/sub-domain study on the basis of an extensive taxonomy). Since the starting of the 1980s up to today, i.e., 2021, implying the gap of over 40 years, the security levels of RSA have proven to be continuously increasing as per our analytical observation and assessment. In naive words, it can be said that the security of all the proposed RSA variants indicates a more secure and better performing versions, and for many coming years, the possibility is high that they won't be easily breakable as even the standard RSA is considered a secure cryptosystem. However, one would ask about prior attacks done on the RSA implementations, considering this situation, most of the attacks include cryptanalyses done by the researchers only in order to assess the algorithm [102], [103]. And even so, if any of those attacks are made on a real-world application or framework, that is often due to the improper implementation of the algorithm on the system in a very weak manner, whether that system is any network protocol or key exchange framework or IoT devices [104]. Another scenario of those attacks may be an improper generation of the random primes, i.e., unstable PRNGs usage in the implementation. Even research was done in which a researchers group tried to estimate the factor of an RSA-232-bit number, and they estimated that it would take more than 1500 years to crack the cipher [105], but recently in the year 2020, RSA-232 was factored by [117], [118]. It can be said from the prior summaries and discussion that there has been numerous research that has already been done for the RSA security development (Fig 6), and for many upcoming years, it can be said that, in terms of security enhancements via mathematical modifications and complexity increment, we have a possibility to rely on these already proposed RSA variants after testing and comparing their authenticity on some real-world applications. But considering several domain-specific developments, for instance, cloud-focused enhancements [106], wireless focused, or even IoT devices focused enhancements, researchers can work on their future RSA enhancements in terms of performance improvement considering execution speed alongside retaining the security. Since the RSA algorithm is a computation costly method to implement, so researchers can also further utilize the same effort to enhance RSA, its key generation and distribution such that it may be easily implemented on such IoT and wireless devices on the framework itself rather than on the server side. One such proposal by Mumtaz *et al.* [6] was given in 2019, in which an RSA based solution was designed specifically for improving the securities in IoT environments as it was based on secure intelligent proxies. Hence such more possibilities are possible and will be a better solution utilizing RSA. As the standard RSA algorithm is a relatively slow algorithm in comparison to other popular cryptographic algorithms, hence there is still a vast number of opportunities needed to be explored in speeding up the algorithms, particularly in the domains of Digital Signatures, Cloud, parallel, and wireless networks (Fig. 8 shows an extensive classification of the most emphasised domains of last 5 years). Furthermore, through our aforementioned assessment and also as Fig. 4 and Fig. 9 suggests, we can summarize the research directions as:

- Researchers might need to limit their further RSA enhancements on the direct mathematical modifications and complexity increments because an excessive number of such algorithms have already been explored as per our study, and they already claim to increase security in terms of complexity.
- Instead, they need to focus their research on the less explored domains like wireless networks, IoT devices and others (Fig. 8), as these domains utilize low processing power [9] and hence low computational energy, which could be an exciting challenge to explore for the RSA enhancements and also, these domains present higher future potential, particularly in public sectors. Since the objective of any proposal of a cryptographic scheme is to reduce cyber risks, it would also be quite interesting if artificial intelligence, machine learning, and real-time intelligence could be incorporated in related future studies [119]. This would enhance the cryptographic approaches in low-memory devices as well [120].
- Since, among the studied literature, few proposed fast variants of the RSA algorithm maintaining or improving the level of security were designed [21], [22], [25], which have been proposed long back, so furthermore, studies can be focused on to design several other fast variants of RSA that offer higher performance and execution speed in key generation, key distribution, encryption or decryption phases.
- Researchers can further integrate other domains, for instance, Hybrid with Parallel implementation, or any other hybrid combination, which specifically focuses on improving the RSA implementation in other considered domains like cloud domain, IoT devices or wireless networks.

Based on the literature survey and analytical assessments of the RSA proposals, we have looked into several domain-specific RSA variants like Hybrid, Cloud, Image, Parallel, Wireless and more, and have mentioned some future directions as per our assessments. The results and conclusions of our study examine and suggest a number of new pathways that are crucial in order to establish the best practice in the field of RSA researches pertaining to the development and enhancements of the RSA algorithm and further guide RSA's consequent researches.

VI. VALIDITY THREATS

Inconsistency in the data extraction method, subjective inclusion selection, exclusion criteria and quality assurance issues, lack of some articles owing to restrictions on search engines or analytical assessment are potential risks to validity in this research. All these concerns are described in depth in four categories of validity threats.

A. EXTERNAL VALIDITY

External validity addresses the generalization of the results whose scope doesn't align with the study [107]. It can be related to the extent to which the primary researches reflect the overarching objective of the review. Our review procedure allowed us to get a more representative group of papers. There are several RSA algorithms that are utilized in showcasing the applications using standard RSA without any modifications or enhancements like image applications, so we do not include these studies as they are outside the scope of this study. Furthermore, we also did not include the additional relevant studies into our primary studies beyond the time period 1978–2021 because the initial RSA was developed in 1978 only and RSA research has been started since then only.

B. INTERNAL VALIDITY

Threats to internal validity may include concepts like biasness, methodology or instrumentation, testing and so on. Also, unpublished research which has undesirable results or proprietary literature which is not available poses a danger to internal validity. In addition, the application of the inclusion/exclusion critique relies on the expertise and judgement of the researchers that might further contribute personal bias to the study. Thus, it is not an easy task to formulate and implement quality evaluation questions during the selection procedure and may include the subjective opinion and judgement of all authors of the study.

C. CONSTRUCT VALIDITY

The degree to which inferences may be made legitimately from the operationalizations in the study to the theoretical conceptions on which those operationalizations were founded is referred to as construct validity [107]. Construct validity, like external validity, is linked to generalization. The exclusion of relevant research is one potential danger to construct validity. To mitigate this risk, we devised a thorough search approach that comprised several steps and would eventually shield us against risks to build validity.

D. CONCLUSION VALIDITY

The statistically significant link between the therapy and the result is referred to as conclusion validity [107]. Bias in performing quality evaluation and data extraction might be a danger to conclusion validity. To reduce this risk, we define the inclusion and exclusion criteria openly, which we feel is sufficient to offer an evaluation of how we arrived at the final selection of publications for analysis. The conclusions of this study are based on a thorough examination of RSA methods in the literature and some analytic evaluation of these approaches by the authors, which may involve some subjectivity.

VII. CONCLUSION

Cryptography is required to ensure the secrecy, integrity and authentication of data transferred over networks. The RSA method has been used in a variety of applications to improve the security of information through encryption and decryption over the years. However, advances in computer technology and hacking techniques have rendered the original RSA algorithm attack more prone in terms of data security. In light of this, several academics have concentrated on the approach of improving the RSA algorithm by adding additional complexity to the process.

The RSA algorithm has been widely utilized to protect data and information transfer in a variety of settings, including cloud servers, key exchanges, internet protocols, and any other situation requiring secure communication between two parties. This Systematic Literature Review analyses and organizes recent literature results on RSA algorithm enhancement in a way that integrates and adds insight to the RSA field's efforts. It focuses on categorizing current literature in order to build a viewpoint on specific major RSA topics and domains, as well as analyzing research trends using conventional SLR methodology. Our systematic approach led us to extract most of the literature that showcases modified RSA algorithms covering all the major academic databases. Hybrid (11 papers), Parallel (9 papers), Cloud (6 papers), Image (8 papers), Multiple-Keys-Based (6 papers), Chinese-Remainder-Theorem-Based (6 papers), Digital Signatures (4 papers), K-Nearest-Theorem-Based (3 papers), Batch (2 papers), Wireless (2 papers), and ''Core-Modifications'' domains (33 papers) comprising mathematically modified and secured models are among the 90 extracted literature distributed in 11 domains according to their focused area.

The improved RSA methods are compared during the study based on key generation, encryption-decryption schemes, key features and enhancements. The most frequent aims of all the under-studied literature are overall execution speed and relative security, while other fewer common purposes include improving RSA in a specific domain, such as the Cloud, Image, or Wireless domains.

To summarize, we have found that more study on RSA improvement is required to adopt in the security of resource constraint devices such as IoT. Furthermore, a consistent taxonomy is required to align various concepts such as execution time, security, and performance. As a result, new techniques and models in the area of RSA must be proposed to account for these challenges. Our study's findings explore and recommend a number of new paths that are critical in establishing best practices in the field of RSA research relating to the modification and enhancement of the RSA algorithm. The study also gives several directions to the RSA security practitioners and researchers since it is the first survey of its kind.

TABLE 18. List of in-text abbreviations and full forms.

Abbreviations	Full Form
RSA	Rivest Shamir Adleman
ECC	Elliptic Curve Cryptography
PKC	Public Key Cryptography
AES	Advanced Encryption Standard
DES	Data Encryption Standard
SLR	Systematic Literature Review
IoT	Internet of Things
LWC	Lightweight Cryptography
IFP	Integer Factorization Problem
DLP	Discrete Logarithm Problem
GPU	Graphical Processing Unit
GCC	GNU Compiler Collection
DS	Digital Signature
CRT	Chinese Remainder Theorem
KNN	K Nearest Neighbor
KNT	K Nearest Theorem
BEARSA	Batch Encrypt Assistant RSA
BEAMRSA	Batch Encrypt Assistant Multi-Prime RSA
PSRSA	Pre-processed Symmetric Rivet Shamir Adleman
AFF	Algebraic Finite Field
ANN	Artificial Neural Network
ESRKGS	Enhanced and Secured RSA Key Generation Scheme

APPENDIX A: SEARCH STRINGS, STUDY QUALITY ASSESSMENT, & ABBREVIATIONS

Abstracts: RSA AND (model OR scheme OR algorithm) AND (enhanced OR efficient OR Improved OR modified OR improvised OR hybrid OR variant OR optimized OR parallel OR secured) AND (cryptosystem OR public OR private OR encryption OR decryption OR cryptography OR complexity OR prime OR asymmetric OR security)

Titles: RSA AND (model OR scheme OR algorithm) AND (enhanced OR efficient OR Improved OR modified OR improvised OR hybrid OR fast OR cloud OR parallel OR secured) AND (cryptographic OR public OR private OR encryption OR decryption OR cryptography OR complexity OR prime OR asymmetric OR secure)

Keywords: RSA AND (model OR scheme OR algorithm) AND (enhanced OR efficient OR Improved OR modified OR improvised OR hybrid OR variant OR optimized OR parallel OR secured) AND (cryptosystem OR public OR private OR encryption OR decryption OR cryptography OR complexity OR prime OR asymmetric OR security)

QUALITY ASSESSMENT CRITERIA

A. Do the selected papers, which are comprised of proposed algorithms, have been practically implemented or not?

B. Do the selected papers involve the comparison of their proposed algorithms with others?

TABLE 19. Study quality assessments.

Domain	References	Criteria A	Criteria B	Criteria C	Criteria D	Criteria E
Core Modifications	[20]	✓	×	×	✓	✓
	[21]	×	✓	×	✓	✓
	[22]	×	✓	×	✓	✓
	[23]	×	×	×	✓	✓
	[24]	✓	✓	×	✓	✓
	[25]	✓	✓	×	✓	✓
	[26]	✓	×	×	×	✓
	[27]	✓	✓	×	✓	✓
	[28]	✓	✓	×	✓	✓
	[29]	×	✓	×	✓	✓
	[30]	✓	✓	×	✓	✓
	[31]	×	×	×	✓	✓
	[32]	✓	✓	×	✓	✓
	[33]	✓	✓	×	✓	✓
	[34]	×	×	×	✓	✓
	[35]	✓	✓	×	✓	✓
	[36]	✓	✓	×	✓	✓
	[37]	✓	✓	×	✓	✓
	[38]	✓	✓	×	✓	✓
	[39]	✓	✓	×	✓	✓
	[40]	✓	✓	×	✓	✓
	[41]	✓	✓	×	✓	✓
	[42]	✓	×	×	✓	✓
	[43]	✓	✓	×	✓	✓
	[44]	×	✓	×	✓	✓
	[45]	✓	✓	×	×	✓
	[46]	✓	✓	×	✓	✓
	[47]	✓	✓	×	✓	✓
	[48]	✓	✓	×	✓	✓
	[49]	✓	✓	×	✓	✓
	[50]	×	✓	×	✓	✓
	[51]	✓	✓	×	✓	✓
	[52]	✓	✓	×	✓	✓
DS	[91]	×	×	×	✓	✓
	[92]	✓	✓	×	✓	✓
	[93]	✓	✓	×	✓	✓
KNT	[94]	×	✓	×	✓	✓
	[95]	✓	✓	×	✓	✓
	[96]	✓	×	×	✓	✓
Batch	[97]	×	✓	✓	✓	✓
	[98]	✓	×	×	×	✓
Wireless	[99]	×	×	×	✓	✓
	[100]	✓	✓	×	×	✓
Hybrid	[53]	✓	✓	×	✓	✓
	[108]	×	✓	×	✓	✓
	[54]	✓	×	×	✓	✓
	[55]	✓	✓	×	✓	✓
	[56]	✓	✓	×	✓	✓
	[57]	✓	×	×	✓	✓
	[58]	✓	✓	×	✓	✓
	[59]	✓	✓	×	✓	✓
	[60]	✓	✓	×	✓	✓
	[61]	✓	✓	×	×	✓
	[109]	×	✓	×	✓	✓
Parallel	[62]	✓	×	×	✓	✓
	[63]	✓	✓	×	✓	✓
	[64]	✓	✓	×	✓	✓
	[65]	✓	✓	×	✓	✓
	[66]	✓	✓	×	✓	✓
	[67]	✓	✓	×	✓	✓
	[68]	✓	✓	×	✓	✓
	[69]	✓	✓	×	×	✓
	[70]	✓	×	×	×	✓
Cloud	[71]	✓	✓	×	✓	✓
	[72]	×	✓	×	✓	✓
	[73]	✓	×	×	✓	✓
	[74]	✓	✓	×	✓	✓
	[75]	✓	✓	×	✓	✓
	[76]	✓	×	×	✓	✓
Image	[110]	✓	×	×	✓	✓
	[77]	✓	×	×	✓	✓
	[78]	✓	✓	×	×	✓
	[111]	✓	✓	×	✓	✓
	[79]	✓	×	×	✓	✓
	[80]	✓	×	×	✓	✓
	[81]	✓	×	×	✓	✓
	[112]	✓	✓	×	✓	✓
Multiple Keys	[82]	×	✓	×	✓	✓
	[83]	×	×	×	✓	✓
	[84]	×	✓	×	✓	✓
	[85]	✓	✓	×	✓	✓
	[113]	×	×	×	✓	✓
	[86]	✓	✓	×	✓	✓
CRT	[87]	✓	×	×	×	✓
	[88]	✓	✓	×	✓	✓
	[114]	✓	✓	×	✓	✓
	[115]	✓	✓	×	✓	✓
	[89]	✓	✓	×	✓	✓
	[90]	✓	×	×	✓	✓

C. Do the methods which are partially proposed in the conference papers are subsequently extended in the Journals or not?

D. Do the proposed methods evaluate each phase of the algorithm (i.e., key generation, encryption and decryption phases)?

E. Are the objective and discussion corresponding exactly with the conclusion described by the authors?

REFERENCES

[1] W. Stallings, *Cryptography and Network Security*, 4th ed. 2006.

[2] H. Zhu, Y. Yuan, Y. Chen, Y. Zha, W. Xi, B. Jia, and Y. Xin, "A secure and efficient data integrity verification scheme for cloud-IoT based on short signature," *IEEE Access*, vol. 7, pp. 90036–90044, 2019, doi: 10.1109/ACCESS.2019.2924486.

[3] A. Gupta and N. K. Walia, "Cryptography algorithms: A review," *Int. J. Eng. Develop. Res.*, vol. 2, no. 2, pp. 1667–1672, 2014. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=FEF3E8340DC536679E3C83BF43F1616C?doi=10.1.1.674.7141&rep=rep1&type=pdf

[4] E. Ochoa-Jimenez, L. Rivera-Zamarripa, N. Cruz-Cortes, and F. Rodriguez-Henriquez, "Implementation of RSA signatures on GPU and CPU architectures," *IEEE Access*, vol. 8, pp. 9928–9941, 2020, doi: 10.1109/ACCESS.2019.2963826.

[5] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," *IEEE Des. Test Comput.*, vol. 24, no. 6, pp. 522–533, Nov./Dec. 2007, doi: 10.1109/MDT.2007.178.

[6] M. Mumtaz, J. Akram, and L. Ping, "An RSA based authentication system for smart IoT environment," in *Proc. IEEE 21st Int. Conf. High Perform. Comput. Commun.; IEEE 17th Int. Conf. Smart City; IEEE 5th Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Aug. 2019, pp. 758–765, doi: 10.1109/HPCC/SmartCity/DSS.2019.00112.

[7] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering–A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009, doi: 10.1016/j.infsof.2008.09.009.

[8] M. S. A. Mohamad, R. Din, and J. I. Ahmad, "Research trends review on RSA scheme of asymmetric cryptography techniques," *Bull. Electr. Eng. Informat.*, vol. 10, no. 1, pp. 487–492, Feb. 2021, doi: 10.11591/eei.v10i1.2493.

[9] M. Rashid, M. Imran, A. R. Jafri, and T. F. Al-Somani, "Flexible architectures for cryptographic algorithms—A systematic literature review," *J. Circuits, Syst. Comput.*, vol. 28, no. 3, 2019, Art. no. 1930003, doi: 10.1142/S0218126619300034.

[10] S. S. Al-Kaabi and S. B. Belhaouari, "Methods toward enhancing RSA algorithm: A survey," *Int. J. Netw. Secur. Appl.*, vol. 11, no. 3, pp. 53–70, 2019, doi: 10.5121/ijnsa.2019.11305.

[11] P. P. Santoso, E. Rilvani, and A. B. Trisnawan, "Systematic literature review: Comparison study of symmetric key and asymmetric key algorithm," in *Proc. IOP Conf., Mater. Sci. Eng.*, 2018, vol. 420, no. 1, Art. no. 012111, doi: 10.1088/1757-899X/420/1/012111.

[12] C. Vyas and J. Dangra, "A review of modern cryptography techniques with special emphasis on RSA," *Int. J. Technol. Res. Manage.*, vol. 4, pp. 2348–9006, Jul. 2017, Accessed: Aug. 12, 2021. [Online]. Available: http://cs.unc.edu/~fabian/course_papers/diffie.hellman.pdf

[13] S. Saxena and B. Kapoor, "State of the art parallel approaches for RSA public key based cryptosystem," *Int. J. Comput. Sci. Appl.*, vol. 5, no. 1, pp. 81–88, Feb. 2015, doi: 10.5121/ijcsa.2015.5108.

[14] P. O. Asagba and E. O. Nwachukwu, "A review of RSA cryptosystems and cryptographic protocols," *West Afr. J. Ind. Academic Res.*, vol. 10, no. 1, pp. 3–16, 2014.

[15] S. S. Dhanda, B. Singh, and P. Jindal, *Lightweight Cryptography: A Solution to Secure IoT*, vol. 112, no. 3. New York, NY, USA: Springer, 2020.

[16] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Elliptic curve lightweight cryptography: A survey," *IEEE Access*, vol. 6, pp. 72514–72550, 2018, doi: 10.1109/ACCESS.2018.2881444.

[17] W. J. Buchanan, S. Li, and R. Asif, "Lightweight cryptography methods," *J. Cyber Secur. Technol.*, vol. 1, nos. 3–4, pp. 187–201, Sep. 2017, doi: 10.1080/23742917.2017.1384917.

[18] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017, doi: 10.1109/ACCESS.2017.2673239.

[19] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Keele Univ., Univ. Durham, U.K., EBSE Tech. Rep. EBSE-2007-01, Version 2.3, 2007.

[20] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[21] J. J. Quisquater and C. Couvreur, "Fast decipherment algorithm for RSA public-key cryptosystem," *Electron. Lett.*, vol. 18, no. 21, pp. 905–907, Oct. 1982, doi: 10.1049/el:19820617.

[22] T. Takagi, "Fast RSA-type cryptosystem modulo $p^k q$," in *Proc. Annu. Int. Cryptol. Conf.*, 1998, pp. 318–326.

[23] T. Collins, D. Hopkins, S. Langford, and M. Sabin, "Public key cryptographic apparatus and method," U.S. Patent 5 848 159, Aug. 12, 1998.

[24] D. Pointcheval, "New public key cryptosystems based on the dependent-RSA problems," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 1999, pp. 239–254, doi: 10.1007/3-540-48910-X_17.

[25] D. Boneh and H. Shacham, "Fast variants of RSA," *CryptoBytes*, vol. 5, no. 1, pp. 1–10, 2002.

[26] A. K. Lenstra and B. M. M. de Weger, "Twin RSA," in *Progress in Cryptology—Mycrypt 2005* (Lecture Notes in Computer Science), vol. 3715, E. Dawson and S. Vaudenay, Eds. Berlin, Germany: Springer, 2005, pp. 222–228, doi: 10.1007/11554868_16.

[27] S. D. Galbraith, C. Heneghan, and J. F. McKee, "Tunable balancing of RSA," in *Information Security and Privacy* (Lecture Notes in Computer Science), vol. 3574, C. Boyd and J. M. G. Nieto, Eds. Berlin, Germany: Springer, 2005, pp. 280–292, doi: 10.1007/11506157_24.

[28] H. M. Sun, M. E. Wu, W. C. Ting, and M. J. Hinek, "Dual RSA and its security analysis," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2922–2933, Aug. 2007, doi: 10.1109/TIT.2007.901248.

[29] S. J. Aboud, M. A. Al-Fayoumi, M. Al-Fayoumi, and H. S. Jabbar, "An efficient RSA public key encryption scheme," in *Proc. 5th Int. Conf. Inf. Technol.: New Gener. (ITNG)*, Apr. 2008, pp. 127–130, doi: 10.1109/ITNG.2008.199.

[30] M. Bahadori, M. R. Mali, O. Sarbishei, M. Atarodi, and M. Sharifkhani, "A novel approach for secure and fast generation of RSA public and private keys on smartcard," in *Proc. 8th IEEE Int. NEWCAS Conf.*, Jun. 2010, pp. 265–268, doi: 10.1109/NEWCAS.2010.5603937.

[31] A. Chhabra and S. Mathur, "Modified RSA algorithm: A secure approach," in *Proc. Int. Conf. Comput. Intell. Commun. Netw.*, Oct. 2011, pp. 545–548, doi: 10.1109/CICN.2011.117.

[32] S. Sharma, P. Sharma, and R. S. Dhakar, "RSA algorithm using modified subset sum cryptosystem," in *Proc. 2nd Int. Conf. Comput. Commun. Technol. (ICCCT)*, Sep. 2011, pp. 457–461, doi: 10.1109/ICCCT.2011.6075138.

[33] A. H. Al-Hamami and I. A. Aldariseh, "Enhanced method for RSA cryptosystem algorithm," in *Proc. Int. Conf. Adv. Comput. Sci. Appl. Technol. (ACSAT)*, Nov. 2012, pp. 402–408, doi: 10.1109/ACSAT.2012.102.

[34] B. P. U. Ivy, P. Mandiwa, and M. Kumar, "A modified RSA cryptosystem based on 'n' prime numbers," *Int. J. Eng. Comput. Sci.*, vol. 1, no. 2, pp. 63–66, 2012. [Online]. Available: http://www.rsa.com/rsalabs/node.asp?i

[35] S. A. Nagar and S. Alshamma, "High speed implementation of RSA algorithm with modified keys exchange," in *Proc. 6th Int. Conf. Sci. Electron., Technol. Inf. Telecommun. (SETIT)*, Mar. 2012, pp. 639–642, doi: 10.1109/SETIT.2012.6481987.

[36] S. Pradhan and B. K. Sharma, "A new design to improve the security aspects of RSA cryptosystem,"' *Int. J. Comput. Sci. Bus. Inform.*, vol. 3, no. 1, pp. 1694–2108, 2013.

[37] R. Minni, K. Sultania, S. Mishra, and D. R. Vincent, "An algorithm to enhance security in RSA," in *Proc. 4th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2013, pp. 1–4.

[38] S. R. Patel and K. Shah, "Security enhancement and speed monitoring of RSA algorithm," *Int. J. Eng. Develop. Res.*, vol. 2, no. 2, pp. 2057–2063, 2014. [Online]. Available: http://www.ijedr.org

[39] M. Thangavel, P. Varalakshmi, M. Murrali, and K. Nithya, "An enhanced and secured RSA key generation scheme (ESRKGS)," *J. Inf. Secur. Appl.*, vol. 20, pp. 3–10, Feb. 2015, doi: 10.1016/j.jisa.2014.10.004.

[40] F. Meneses, W. Fuertes, J. Sancho, S. Salvador, D. Flores, H. Aules, and F. Castro, "RSA encryption algorithm optimization to improve performance and security level of network messages," *Int. J. Comput. Sci. Netw. Secur.*, vol. 16, no. 8, pp. 55–62, Aug. 2016. [Online]. Available: http://www.dspace.uce.edu.ec/handle/25000/14663

[41] N. Kumar and P. Chaudhary, "Implementation of modified RSA cryptosystem for data encryption and decryption based on n prime number and bit stuffing," in *Proc. 2nd Int. Conf. Inf. Commun. Technol. Competitive Strategies (ICTCS)*, 2016, pp. 1–6, doi: 10.1145/2905055.2905180.
[42] F. Mo, Y.-C. Hsu, H.-H. Chang, S.-C. Pan, J.-J. Yan, and T.-L. Liao, "Design of an improved RSA cryptosystem based on synchronization of discrete chaotic systems," in *Proc. Int. Conf. Inf. Syst. Artif. Intell. (ISAI)*, Jun. 2016, pp. 9–13, doi: 10.1109/ISAI.2016.0012.
[43] K. Somsuk, "The improving decryption process of RSA by choosing new private key," in *Proc. 8th Int. Conf. Inf. Technol. Electr. Eng. (ICITEE)*, Oct. 2016, pp. 2–5, doi: 10.1109/ICITEED.2016.7863242.
[44] J. Sahu, V. Singh, V. Sahu, and A. Chopra, "An enhanced version of RSA to increase the security," *J. Netw. Commun. Emerg. Technol.*, vol. 7, no. 4, pp. 1–4, 2017.
[45] P. Chaudhury, S. Dhang, M. Roy, S. Deb, J. Saha, A. Mallik, S. Bal, S. Roy, M. K. Sarkar, S. Kumar, and R. Das, "ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm," in *Proc. 8th Annu. Ind. Autom. Electromech. Eng. Conf. (IEMECON)*, Aug. 2017, pp. 332–337, doi: 10.1109/IEMECON.2017.8079618.
[46] P. M. Aiswarya, A. Raj, D. John, L. Martin, and G. Sreenu, "Binary RSA encryption algorithm," in *Proc. Int. Conf. Control, Instrum., Commun. Comput. Technol. (ICCICCT)*, Dec. 2016, pp. 178–181, doi: 10.1109/ICCICCT.2016.7987940.
[47] M. Chakraborty, B. Jana, T. Mandal, and M. Kule, "An performance analysis of RSA scheme using artificial neural network," in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2018, pp. 1–5, doi: 10.1109/ICCCNT.2018.8494032.
[48] M. A. Islam, M. A. Islam, N. Islam, and B. Shabnam, "A modified and secured RSA public key cryptosystem based on 'n' prime numbers," *J. Comput. Commun.*, vol. 6, no. 3, pp. 78–90, 2018, doi: 10.4236/jcc.2018.63006.
[49] K. R. Raghunandhan, S. Shetty, G. Aithal, and N. Rakshith, "Enhanced RSA algorithm using fake modulus and fake public key exponent," in *Proc. Int. Conf. Elect., Electron., Commun., Comput., Optim. Techn. (ICEECCOT)*, Dec. 2018, pp. 755–759.
[50] J. S. Yadav, A. S. Sheregar, V. M. Panjri, and S. L. Gharat, "Secure approach for encrypting data," in *Proc. Int. Conf. Smart City Emerg. Technol. (ICSCET)*, Jan. 2018, pp. 1–3, doi: 10.1109/ICSCET.2018.8537290.
[51] I. Al-Barazanchi, S. A. Shawkat, M. H. Hameed, and K. S. L. Al-Badri, "Modified RSA-based algorithm: A double secure approach," *Telkomnika (Telecommun. Comput. Electron. Control.*, vol. 17, no. 6, pp. 2818–2825, 2019, doi: 10.12928/TELKOMNIKA.v17i6.13201.
[52] L. S. Reddy, "RM- RSA algorithm," *J. Discrete Math. Sci. Cryptogr.*, May 2020, doi: 10.1080/09720529.2020.1734292.
[53] C. A. M. Paixao and D. L. G. Filho, "An efficient variant of the RSA cryptosystem," *IACR Cryptol. ePrint Arch.*, vol. 2003, p. 159, 2003.
[54] S. Gupta and J. Sharma, "A hybrid encryption algorithm based on RSA and Diffie-Hellman," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res.*, Dec. 2012, pp. 1–4.
[55] R. S. Dhakar, A. K. Gupta, and P. Sharma, "Modified RSA encryption algorithm (MREA)," in *Proc. 2nd Int. Conf. Adv. Comput. Commun. Technol.*, Jan. 2012, pp. 426–429, doi: 10.1109/ACCT.2012.74.
[56] S. Verma and D. Garg, "An improved RSA variant," *Int. J. Advancements Technol.*, vol. 5, no. 2, pp. 161–169, 2014. [Online]. Available: http://ijict.org/
[57] V. S. Mahalle and A. K. Shahade, "Enhancing the data security in Cloud by implementing hybrid (RSA & AES) encryption algorithm," in *Proc. Int. Conf. Power, Automat. Commun. (INPAC)*, Oct. 2014, pp. 146–149, doi: 10.1109/INPAC.2014.6981152.
[58] S. Arora, "Enhancing cryptographic security using novel approach based on enhanced-RSA and Elamal: Analysis and comparison," *Int. J. Comput. Appl.*, vol. 112, no. 13, pp. 35–39, 2015.
[59] A. Karakra and A. Alsadeh, "A-RSA: Augmented RSA," in *Proc. SAI Comput. Conf. (SAI)*, Jul. 2016, pp. 1016–1023.
[60] P. K. Panda and S. Chattopadhyay, "A hybrid security algorithm for RSA cryptosystem," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Jan. 2017, pp. 1–6.
[61] E. Jintcharadze and M. Iavich, "Hybrid implementation of twofish, AES, ElGamal and RSA cryptosystems," in *Proc. IEEE East-West Design Test Symp. (EWDTS)*, Sep. 2020, pp. 1–4, doi: 10.1109/EWDTS50664.2020.9224901.
[62] C. W. Chiou, "Parallel implementation of the RSA public-key cryptosystem," *Int. J. Comput. Math.*, vol. 48, nos. 3–4, pp. 153–155, Jan. 1993.
[63] Y. Li, Q. Liu, and T. Li, "Design and implementation of an improved RSA algorithm," in *Proc. Int. Conf. E-Health Netw. Digit. Ecosyst. Technol. (EDT)*, Apr. 2010, pp. 390–393.
[64] M. Damrudi and N. Ithnin, "Parallel RSA encryption based on tree architecture," *J. Chin. Inst. Eng.*, vol. 36, no. 5, pp. 658–666, Jul. 2013, doi: 10.1080/02533839.2012.737113.
[65] S. Saxena and B. Kapoor, "An efficient parallel algorithm for secured data communications using RSA public key cryptography method," in *Proc. IEEE Int. Advance Comput. Conf. (IACC)*, Feb. 2014, pp. 850–854, doi: 10.1109/IAdCC.2014.6779433.
[66] A. Asaduzzaman, D. Gummadi, and P. Waichal, "A promising parallel algorithm to manage the RSA decryption complexity," in *Proc. SoutheastCon*, Apr. 2015, pp. 1–5, doi: 10.1109/SECON.2015.7132926.
[67] R. Saxena, M. Jain, D. Singh, and A. Kushwah, "An enhanced parallel version of RSA public key crypto based algorithm using openMP," in *Proc. 10th Int. Conf. Secur. Inf. Netw.*, Oct. 2017, pp. 37–44, doi: 10.1145/3136825.3136866.
[68] P. Gupta, D. K. Verma, and A. K. Singh, "Improving RSA algorithm using multi-threading model for outsourced data security in cloud storage," in *Proc. 8th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Jan. 2018, pp. 14–15.
[69] M. A. Ayub, Z. Ahmed Onik, and S. Smith, "Parallelized RSA algorithm: An analysis with performance evaluation using OpenMP library in high performance computing environment," in *Proc. 22nd Int. Conf. Comput. Inf. Technol. (ICCIT)*, Dec. 2019, pp. 18–20, doi: 10.1109/ICCIT48885.2019.9038275.
[70] A. Rawat, K. Sehgal, A. Tiwari, A. Sharma, and A. Joshi, "A novel accelerated implementation of RSA using parallel processing," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 2, pp. 309–322, Feb. 2019, doi: 10.1080/09720529.2019.1582864.
[71] F. F. Moghaddam, M. T. Alrashdan, and O. Karimi, "A hybrid encryption algorithm based on RSA small-e and efficient-RSA for cloud computing environments," *J. Adv. Comput. Netw.*, vol. 1, no. 3, pp. 238–241, 2013, doi: 10.7763/jacn.2013.v1.47.
[72] M. R. Patidar and R. Bhartiya, "Modified RSA cryptosystem based on offline storage and prime number," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res.*, Dec. 2013, pp. 1–6.
[73] V. P. Bansal and S. Singh, "A hybrid data encryption technique using RSA and blowfish for cloud computing on FPGAs," in *Proc. 2nd Int. Conf. Recent Adv. Eng. Comput. Sci. (RAECS)*, Dec. 2015, pp. 1–5, doi: 10.1109/RAECS.2015.7453367.
[74] K. El Makkaoui, A. Ezzati, and A. Beni-Hssane, "Cloud-RSA: An enhanced homomorphic encryption scheme," in *Europe and MENA Cooperation Advances in Information and Communication Technologies* (Advances in Intelligent Systems and Computing), vol. 520, Á. Rocha, M. Serrhini, and C. Felgueiras, Eds. Cham, Switzerland: Springer, 2017, doi: 10.1007/978-3-319-46568-5_48.
[75] I. G. Amalarethinam and H. M. Leena, "Enhanced RSA algorithm with varying key sizes for data security in cloud," in *Proc. World Congr. Comput. Commun. Technol. (WCCCT)*, Feb. 2017, pp. 172–175, doi: 10.1109/WCCCT.2016.50.
[76] K. El Makkaoui and A. Beni-Hssane, "Fast cloud-RSA scheme for promoting data confidentiality in the cloud computing," *Proc. Comput. Sci.*, vol. 113, pp. 33–40, Jan. 2017, doi: 10.1016/j.procs.2017.08.282.
[77] K. D. M. Alsabti and H. R. Hashim, "A new approach for image encryption in the modified RSA cryptosystem using MATLAB," *Global J. Pure Appl. Math.*, vol. 12, no. 4, pp. 3631–3640, 2016.
[78] D. Jagadiswary and D. Saraswady, "Estimation of modified RSA cryptosystem with hyper image encryption algorithm," *Indian J. Sci. Technol.*, vol. 10, no. 7, pp. 1–5, Feb. 2017, doi: 10.17485/ijst/2017/v10i7/111000.
[79] S.-H. Shin, W. S. Yoo, and H. Choi, "Development of modified RSA algorithm using fixed Mersenne prime numbers for medical ultrasound imaging instrumentation," *Comput. Assist. Surg.*, vol. 24, pp. 73–78, Oct. 2019, doi: 10.1080/24699322.2019.1649070.
[80] X.-L. Huang, Y.-X. Dong, K.-X. Jiao, and G.-D. Ye, "Asymmetric pixel confusion algorithm for images based on RSA and Arnold transform," *Frontiers Inf. Technol. Electron. Eng.*, vol. 21, no. 12, pp. 1783–1794, Dec. 2020, doi: 10.1631/FITEE.2000241.
[81] K. Jiao, G. Ye, Y. Dong, X. Huang, and J. He, "Image encryption scheme based on a generalized Arnold map and RSA algorithm," *Secur. Commun. Netw.*, vol. 2020, Jun. 2020, Art. no. 9721675, doi: 10.1155/2020/9721675.

[82] V. Kapoor, "Data encryption and decryption using modified RSA cryptography based on multiple public keys and 'n' prime number," *Int. J. Sci. Res. Netw. Secur. Commun.*, vol. 1, no. 2, pp. 35–38, 2013.

[83] A. A. Ayele and V. Screenivasarao, "A modified RSA encryption technique based on multiple public keys," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 1, no. 4, pp. 859–864, 2013. [Online]. Available: http://www.ijircce.com

[84] I. Jahan, M. Asif, and L. Jude Rozario, "Improved RSA cryptosystem based on the study of number theory and public key cryptosystems," *Amer. J. Eng. Res.*, vol. 4, no. 1, pp. 143–149, 2015. [Online]. Available: http://www.ajer.org.

[85] R. Ghosh, "An efficient and robust modified RSA based security algorithm in modern cryptography," *J. Comput. Sci. Eng. Inf. Technol. Res.*, vol. 6, no. 2, pp. 15–22, 2016.

[86] A. E. Mezher, "Enhanced RSA cryptosystem based on multiplicity of public and private keys," *Int. J. Elect. Comput. Eng.*, vol. 8, no. 5, pp. 3949–3953, 2018, doi: 10.11591/ijece.v8i5.pp3949-3953.

[87] C.-H. Wu, J.-H. Hong, and C.-W. Wu, "RSA cryptosystem design based on the Chinese remainder theorem," in *Proc. Conf. Asia South Pacific Design Autom. (ASP-DAC)*, 2001, pp. 391–395.

[88] J. Blömer, M. Otto, and J. P. Seifert, "A new CRT-RSA algorithm secure against Bellcore attacks," in *Proc. 10th ACM Conf. Comput. Commun. Secur.*, 2003, pp. 311–320, doi: 10.1145/948148.948151.

[89] K. Sony, D. Shaik, B. Divya Sri, and G. Anitha, "Improvised asymmetric key encryption algorithm using MATLAB," *IOSR J. Electron. Commun. Eng.*, vol. 10, no. 2, pp. 31–36, 2015.

[90] R. S. Abdeldaym, H. M. A. Elkader, and R. Hussein, "Modified rsa algorithm using two public key and Chinese remainder theorem," *Int. J. Electron. Inf. Eng.*, vol. 10, no. 1, pp. 51–64, 2019, doi: 10.6636%2fIJEIE.201903_10(1).06.

[91] H. Si, Y. Cai, and Z. Cheng, "An improved RSA signature algorithm based on complex numeric operation function," in *Proc. Int. Conf. Challenges Environ. Sci. Comput. Eng.*, 2010, pp. 397–400, doi: 10.1109/CESCE.2010.257.

[92] S. A. Jaju and S. S. Chowhan, "A modified RSA algorithm to enhance security for digital signature," in *Proc. Int. Conf. Workshop Comput. Commun. (IEMCON)*, Oct. 2015, pp. 1–5.

[93] F. J. Aufa and A. Affandi, "Security system analysis in combination method: RSA encryption and digital signature algorithm," in *Proc. 4th Int. Conf. Sci. Technol. (ICST)*, Aug. 2018, pp. 1–5.

[94] A. K. Hussain, "A modified RSA algorithm for security enhancement and redundant messages elimination using K-nearest neighbor algorithm," *IJISET-Int. J. Innov. Sci., Eng. Technol.*, vol. 2, no. 1, pp. 159–163, 2015.

[95] S. Mathur and D. Gupta, "A modified RSA approach for encrypting and decrypting text and images using multi- power, multi public keys, multi prime numbers and K-nearest neighbor algorithm," in *Proc. Int. Conf. Adv. Inf. Commun. Technol. Comput.*, 2016, pp. 1–6, doi: 10.1145/2979779.2979833.

[96] S. Mathur, D. Gupta, V. Goar, and M. Kuri, "Analysis and design of enhanced RSA algorithm to improve the security," in *Proc. 3rd Int. Conf. Comput. Intell. Commun. Technol. (CICT)*, Feb. 2017, pp. 1–5.

[97] A. Fiat, "Batch RSA," *J. Cryptol.*, vol. 10, no. 2, pp. 75–88, 1997, doi: 10.1007/s001459900021.

[98] Q. Liu, T. Li, and Y. Li, "Design and implementation of two improved batch RSA algorithms," in *Proc. 3rd Int. Conf. Comput. Sci. Inf. Technol.*, Jul. 2010, pp. 156–160.

[99] M. Frunza and L. Scripcariu, "Improved RSA encryption algorithm for increased security of wireless networks," in *Proc. Int. Symp. Signals, Circuits Syst.*, Jul. 2007, pp. 1–4.

[100] S. Shin, "Lightweight encryption based security package for wireless body area network," Ph.D. dissertation, Dept. Comput. Sci., South Dakota State Univ., Brookings, SD, USA, 2021.

[101] S. Shin, K. Won, and S. Shin, "Size efficient preprocessed symmetric RSA for wireless body area network," *ACM SIGAPP Appl. Comput. Rev.*, vol. 20, no. 1, pp. 15–23, Apr. 2020, doi: 10.1145/3392350.3392352.

[102] M. Mumtaz and L. Ping, "Forty years of attacks on the RSA cryptosystem: A brief survey," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 1, pp. 9–29, Jan. 2019, doi: 10.1080/09720529.2018.1564201.

[103] W. N. A. Ruzai, M. R. K. Ariffin, M. A. Asbullah, Z. Mahad, and A. Nawawi, "On the improvement attack upon some variants of RSA cryptosystem via the continued fractions method," *IEEE Access*, vol. 8, pp. 80997–81006, 2020, doi: 10.1109/ACCESS.2020.2991048.

[104] M. A. Khan, M. T. Quasim, N. S. Alghamdi, and M. Y. Khan, "A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data," *IEEE Access*, vol. 8, pp. 52018–52027, 2020, doi: 10.1109/ACCESS.2020.2980739.

[105] T. Kleinjung *et al.*, "Factorization of a 768-bit RSA modulus," in *Advances in Cryptology—CRYPTO 2010* (Lecture Notes in Computer Science), vol. 6223, T. Rabin, Ed. Berlin, Germany: Springer, 2010, doi: 10.1007/978-3-642-14623-7_18.

[106] I. Mustafa, I. U. Khan, S. Aslam, A. Sajid, S. M. Mohsin, M. Awais, and M. B. Qureshi, "A lightweight post-quantum lattice-based RSA for secure communications," *IEEE Access*, vol. 8, pp. 99273–99285, 2020, doi: 10.1109/ACCESS.2020.2995801.

[107] C. Wohlin, P. Runeson, M. Höst, M. C. Ohlsson, B. Regnell, and A. Wesslén, *Experimentation in Software Engineering: An Introduction*. Springer, 2012, doi: 10.1007/978-3-642-29044-2.

[108] J. Mohammed Ahmed and Z. M. Ali, "The enhancement of computation technique by combining RSA and el-gamal cryptosystems," in *Proc. Int. Conf. Electr. Eng. Informat.*, Jul. 2011, pp. 1–5.

[109] Z. Alamsyah, T. Mantoro, U. Adityawarman, and M. A. Ayu, "Combination RSA with one time pad for enhanced scheme of two-factor authentication," in *Proc. 6th Int. Conf. Comput. Eng. Design (ICCED)*, Oct. 2020, pp. 1–5.

[110] G. Zhao, X. Yang, B. Zhou, and W. Wei, "RSA-based digital image encryption algorithm in wireless sensor networks," in *Proc. 2nd Int. Conf. Signal Process. Syst.*, Jul. 2010, pp. V2–640.

[111] C. J. N. Cheltha, "An innovative encryption method for images using RSA, honey encryption and inaccuracy tolerant system using Hamming codes," in *Proc. Int. Conf. Comput. Power, Energy Inf. Commuincation (ICCPEIC)*, Mar. 2017, pp. 796–799.

[112] D. M. Alsaffar, A. Sultan Almutiri, B. Alqahtani, R. M. Alamri, H. Fahhad Alqahtani, N. N. Alqahtani, G. Mohammed Alshammari, and A. A. Ali, "Image encryption based on AES and RSA algorithms," in *Proc. 3rd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, Mar. 2020, pp. 1–5.

[113] A. Goel, "Encryption algorithm using dual modulus," in *Proc. 3rd Int. Conf. Comput. Intell. Commun. Technol. (CICT)*, Feb. 2017, pp. 1–4.

[114] H. Ou, "Multi-factor rebalanced RSA-CRT encryption schemes," in *Proc. 2nd Int. Conf. Biomed. Eng. Inform.*, Oct. 2009, pp. 1–5.

[115] D. Garg and S. Verma, "Improvement over public key cryptographic algorithm," in *Proc. IEEE Int. Advance Comput. Conf.*, Mar. 2009, pp. 734–739.

[116] H. Williams, "A modification of the RSA public-key encryption procedure (Corresp.)," *IEEE Trans. Inf. Theory*, vol. I-26, no. 6, pp. 726–729, Nov. 1980.

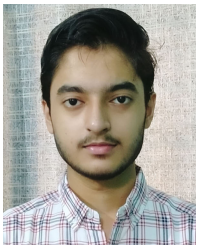
[117] *RSA Numbers—Wikipedia [Internet]*. Accessed: Oct. 11, 2021. [Online]. Available: https://en.wikipedia.org/wiki/RSA_numbers#cite_note-rsa-232-35

[118] *RSA-232 Number Has Been Factored—HBM PAH [Internet]*. Accessed: Oct. 11, 2021. [Online]. Available: https://www.inm.ras.ru/math_center_en/rsa-232-number-has-been-factored-5/

[119] P. Radanliev, D. de Roure, K. Page, M. van Kleek, O. Santos, L. T. Maddox, P. Burnap, E. Anthi, and C. Maple, "Design of a dynamic and self-adapting system, supported with artificial intelligence, machine learning and real-time intelligence for predictive cyber risk analytics in extreme environments–cyber risk in the colonisation of Mars," *Saf. Extreme Environ.*, vol. 2, no. 3, pp. 219–230, 2020.

[120] P. Radanliev and D. de Roure, "Review of algorithms for artificial intelligence on low memory devices," *IEEE Access*, vol. 9, pp. 109986–109993, 2021.

RAZA IMAM is currently pursuing the bachelor's degree with the Department of Computer Science, Aligarh Muslim University. His recent experiences involve working as a Research Assistant and a Research Intern at the Computer Science Department, AMU, and the Department of IT, IIIT Allahabad, respectively. He has also worked as a Research Intern at UKM Malaysia. He has contributed to several research projects, where he worked on projects pertaining to information security, blockchain, lightweight cryptography, and machine learning. He has multiple scientific articles published in international conferences and journals.



QAZI MOHAMMAD AREEB is currently pursuing the bachelor's degree with the Department of Computer Science, Aligarh Muslim University. He has worked as a Research Assistant at the Computer Science Department, AMU, and the Department of IT, University Technology Petronas (UTP), Malaysia. He has experience in the field of artificial intelligence, machine learning, and cybersecurity. He has published several research papers in international conferences and peer-reviewed journals. His main research interest includes developing serviceable technologies through artificial intelligence and computer vision.

ABDULRAHMAN ALTURKI received the B.Sc. (Hons.) degree in electrical and communication engineering from Qassim University, Buraydah, Saudi Arabia, in 2008, and the M.Sc. and Ph.D. degrees in electrical engineering from the University of Dayton, OH, USA, in 2012 and 2017, respectively. He joined as a Teaching Staff with the Department of Electrical and Communications, Faculty of Engineering, Qassim University, in 2017. He has published several scientific papers in national and international conference proceedings and journals. His current research interests include computer vision, image restoration, multi-carrier communication systems, digital signal processing, digital communications, and channel equalization.

FAISAL ANWER received the master's degree in computer application and the Ph.D. degree in information security from Jamia Millia Islamia, New Delhi. He is currently working as an Assistant Professor with the Department of Computer Science, AMU, Aligarh. Prior to joining AMU, he worked as a Senior Software Engineer at Computer Science Corporation (CSC), Noida. He has also worked with CSC, U.K., from 2009 to 2010. He has published several research papers in international/national conferences and journals. His research interests include software security, cryptography, and program robustness.