International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020

# An OTP Integrated Optimal Key RSA Based Secure Data Communication

**Mrinmoy Sarkar, Asok Kumar, Bansibadan Maji**

***Abstract*: System security is a basic aspect of data sharing. Aspires have been made to exhaust particular defects over the web. For this, different creative usage and security methods have been made. The measure of information exchange isn't a factor. The major factor is, how much it's secure, the channel gives while transmitting information. Cryptography is one such structure, which grants secure information transmission without losing its protection and uprightness. In light of the key circulation, cryptography is also assembled into two critical forms Symmetric Key Cryptography as well as Asymmetric Key Cryptography. RSA is one of the best conspicuous public-key cryptography based algorithms is unequivocally utilized for encryption/decryption. It's far based on the logical arrangement of factorization of strongly enormous whole numbers which is a compute-intensive way. In this paper, we have provided a novel, secure and profitable information communication system dependent on the RSA algorithm. Mystery updating signal dealing with systems have been proposed in the exploration for the two data transmission and the channel estimation stages. The proposed one facilitates the advantages of both RSA calculation and One Time Password (OTP) produced by the sender and got just by the endorsed customer. Despite that not at all like conventional RSA algorithm, in this work we embrace perfect key assurance by particle swarm optimization (PSO) during both encryption and decryption. The use of PSO for perfect key decision makes the general technique proficient by extending the security level and making the computation procedure very easy.***

***Keywords* : Cryptography, One Time Password (OTP), Particle Swarm Optimization (PSO), RSA, Signal Processing.***

## I. INTRODUCTION

Amidst the most recent decade, there has been a perilous improvement of utilizing PCs, systems, communications and multimedia applications [1]. Web customers demand content, sound, pictures, as well as video [2]. The entwining of PCs, systems, communications, and multimedia applications has happened. The unparalleled advancement of data and communication development, outstanding improvement of system structure and series progression in multimedia signal management procedures has made communication of multimedia substance simpler than at some other time [3]. To consider the more comprehensive accessibility of multimedia data and profitable commercialization of different multimedia related associations, ensuring that multimedia data is uneven utilized just by embraced clients for certified purposes has ended up be important[4]. The present-day fast system structure gives a smart and basic technique for transmitting on the web to convey a lot of information to individuals all around the world [5]. Regardless, the communication channels utilized for sharing information are deplorably unreliable [6]. Moreover, appropriately the subject of data security rises. To address the issue of data security, diverse cryptographic techniques are being utilized [7]. There is a substitute methodology used to decrypt and pack the information to keep up the mystery, yet the encryption of information alone won't be abnormally capable to ensure classification [8]. Cryptography is a standout among other appropriate stages to guarantee secure information transmission where the information encryption and decoding arrangements are consolidated with or without a mystery key [9]. In cryptography, a cryptosystem is a collection of three algorithms: one for key generation, one for encryption, and the other for decryption [10]. They are classified symmetric key cryptosystem (same encryption key has used for decryption), asymmetric key cryptosystem (differing keys for encryption and decryption are used) [11].Asymmetric key cryptography system uses two keys out of which one key is "public key" which ordinarily serves the encryption strategy and another is "private key" is distribute for the decryption methodology [12]. The "public key" cryptography is also guaranteed that the symmetric cryptography. The security of the encryption plot, generally, depends upon the key length and the computational work [13]. This paper focuses on ensuring the protection and accomplishing access control of data, or, as such, the essential security components for specific applications. We focus on accomplishing content security in the midst of data scattering, chronicling, and another delegate managing [14]. We will probably plot encryption devices that can scramble once and safely process from different points of view utilizing the present sign organizing strategies [15]. To accomplish this objective, we generally consider signal managing as well as cryptography in our examination of encryption. We research the probable spaces wherein encryptions can be associated, including the model zone, the quantized change space, the transitional biplanes, and the bit stream region [16]. A regular technique to accomplish content mystery is to scramble the entire progression utilizing a figure, for example, DES, AES, or RSA [17].

Revised Manuscript Received on February 05, 2020.
* Correspondence Author
**Mrinmoy Sarkar*,** ECE, Bankura Unnayani Institute of Engineering, Bankura, W.B. Email: mrinmoysarkar.phd@gmail.com
**Asok Kumar,** ECE, Name MCKV Institute of Engineering, Howrah,W.B. Email: ashokumar.phd@gmail.com
**Bansibadan Maji,** ECE, NIT, Durgapur, India. Email: bansibadanmaji.phd@gmail.com

To overhaul the security of the common RSA calculation, the Enhanced RSA Encryption Algorithm (ERSA) was arranged which extends the figuring multifaceted nature [18]. That the encryption and the decryption advancement is more rapidly than the standard RSA with no further increase in implication by thusly the authentic message can be gotten easily [19].

## II. RELATED WORK

Tsun-I Chien and Teh-Lu Liao [20] showed an ensured updated communication system reliant on the chaotic guideline, cryptography, and chaotic synchronization strategies. The system includes a Chaotic Modulator (CM), a Chaotic Secure Transmitter (CST), a Chaotic Secure Receiver (CSR) and a Chaotic Demodulator (CDM). The CM module joins a cluttered structure and a novel Chaotic Differential Peaks Keying (CDPK) change expect to make analog patterns contrasting to the input digital bits. The CST and CSR modules are shaped with a definitive target that a singular scalar signal has transmitted in the public channel. Those two slave structures are driven meanwhile by the transmitted signal and are proposed to synchronize and make appropriate cryptography keys for encryption and decryption aims. In the CDM module, a nonlinear spectator was planned to check the chaotic modifying system in the CM. A demodulation system was then associated with decode the transmitted input digital bits.

Shabir A. Parah et al., [21] proposed another crypto area information disguising technique subject to Intermediate Significant Bit Plane Embedding (ISBPE). The cover picture was encoded and the data to be connected was mixed, and after that presented in the Intermediate Significant Bit (ISB) planes of the scrambled cover picture, at the zones coordinated by a Pseudo-random Address Vector (PAV). The pseudo-random embedding of the scrambled information in the ISB planes of encrypted picture result in three-level security of the information to be joined. The ISBPE embedding results in a basic incredible position that the foreseen plan winds up being totally powerful to the normally utilized assault of Least Significant Bit (LSB) ejection or substitution.

Henry Ker Chang and Jiang-Long Liu [22] private key encryptions plot for two-dimensional picture information. The blueprint depended upon lossless information pressure standard. The arrangement was made to have the two information encryption and pressure performed meanwhile. For the lossless information pressure impact, the quad-tree information structure was utilized to address the picture; for the encryption reason, diverse looking at progressions of picture information is given. The isolating groupings incorporate a private key for encryption. 24 reasonable successions of activities are portrayed for getting to four quadrants.

Firas Ali Sabir [23] proposed a technique of figuring and hiding data alongside a cover of the sound wave record. In the essential stage, the substance is changed over to its corresponding ASCII code. The substance was mixed utilizing DES (Data Encryption Standard) framework per mystery key then the figure content was introduced inside a cover sound wave record utilizing time and repeat area. The clarified structure builds of a mystery key steganography framework, which introduces sure substance subsequent with scrambling into arbitrary positions inside sound wave report notwithstanding the other system utilized there to isolate the cover sound into its repeat sections, were the wavelet change utilizing Haar channel as an assertion work.

G.Kalaiarasi*et al.*, [24] exhibited the data was scrambled utilizing a key-based algorithm by methods for Linear Feedback Shift Register (LFSR) and the scrambled data was requested in the sound signal utilizing Least Significant Bit (LSB) algorithm reasonably and the stego-record was restricted. The stego-record incorporates cover sound and encoded data was transmitted the key delivered in the midst of the encryption was basically perceived to the recipient. Decoding was the contrary technique of encryption from which the sound signal was evacuated and the data was unscrambled.

## III. PROPOSED METHODOLOGY

Signal dealing with procedures accept a basic job in improving the mystery in the multi-antenna remote systems. Cryptography [25] is a system for storing and transmitting the data in a picked frame so those for whom it's proposed can study and process it. Regardless, in the ultra-modern PC driven world, cryptography has as frequently as simultaneously connected with scrambling plaintext (general scholarly substance, every now and then called clear substance) into cipher text (a technique perceived as encryption), by then lower back once more (suggested as decoding). Cryptography apprehensions four objectives:

- Confidentiality

The facts can't be valued by all individuals for whom it ends up unplanned.

- Integrity [26]

The estimations can't be adjusted in storage or transmit among the sender and accepted accumulate without the adjustment being perceived.

- Authentication

The sender and the recipient can check each other distinctive confirmation and the base of the intuitiveness.

- Non-repudiation

The sender of the data can't disprove at a later stage his or her goals in the perception or transmission of the data.

### A.One Time Password (OTP)

A one-time password (OTP) [27] is a password that is veritable for most effortless one login session or exchange, on a PC or assorted modernized gadgets. The most significant preferred standpoint has handled by utilizing OTPs is that an appraisal to static passwords; they are not unprotected against replay assaults. This demonstrates a potential intruder who makes how to demonstrate an OTP that was at the point used to sign into an association or to deal with an exchange won't be able to push it since it will never again be liberal. A second authoritative increment is that a customer, who uses the proportionate (or close) password for various frameworks, isn't made vulnerable on every one of them if the password for one of these is gotten by an assailant.

Distinctive OTP structures besides plan to guarantee that a session can't in actuality be blocked or imitated without the learning of flighty data made amidst the last session, all things considered, diminishing the assault surface further.

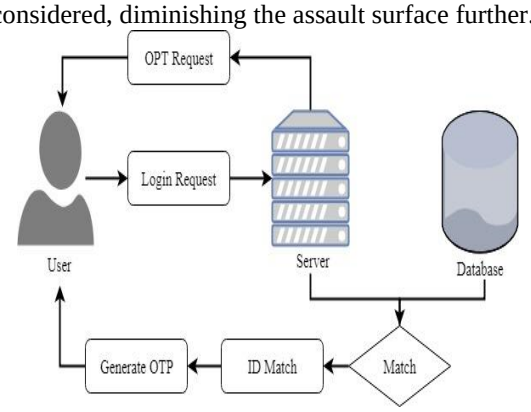


**Fig. 1. OTP Generation**

OTP generation algorithm ordinarily utilizes pseudo-haphazardness. Two-way one-time confirmations fill in as seeks after:

a) The customer drives a login appeal server with its ID and pin (static password).

b) In the occasion that ID and PIN coordinate with the ID and PIN set away in the database, the server prompts an OTP and sends it through SMS or email to the customer.

c) Server request customer for the OTP.

d) The customer penetrates OTP and on the event, it matches, by then the customer has endorsed.

### B. Asymmetric RSA algorithm

Asymmetric [28] cryptography or public-key cryptography will be cryptography in which a few keys have used to encode and decode a message all together that it arrives safely. As an issue of first importance, a framework customer gets public and private key pair from a certificate authority. Each and every other individual who needs to drive an encoded message can get the typical beneficiary's public key from the public index. They utilize this key to encipher the message, and they pass on it to the recipient.

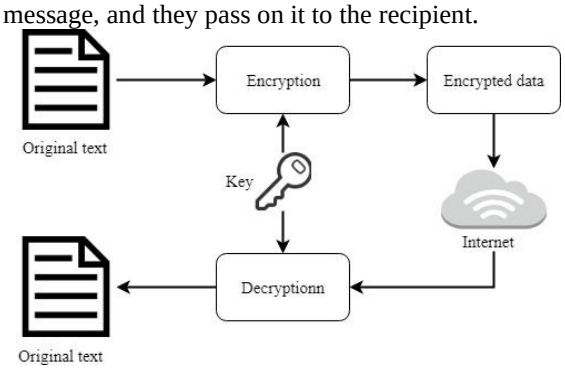


**Fig. 2. RSA Cryptography**

Exactly when the beneficiary gains the message, they decode it with their private key, which nobody else should approach. The Rivest-Shamir-Adleman (RSA) algorithm is standout among the most common and anchors the public key encryption techniques. The algorithm gains by the route that there is no effective technique to factor generous (100-200 digit) numbers. The RSA algorithm incorporates four phases:

- Key generation
- Key appropriation
- Encryption
- Decryption

The open key can be perceived by everyone and is utilized for encoding the messages. The aim is that the messages have encoded with the public key must be decoded in a reasonable measure of time utilizing the private key. Here, the plaintext has encoded in blocks. This sort of cryptosystem guarantees that simply the perfect individuals who realize the key can examine the data. Here, the sender and the beneficiary can ensure each other's identity and beginning/goal of the data. For this condition, the scope of the subsequent encoded substance has more than the real plaintext measure. In any case, the key generation and decryption rate are moderate in this cryptosystem.

### Key Generation

In the key generation stage, we require keys that are public and private. We will convey the public and the private key [29] by utilizing the accompanying advances.

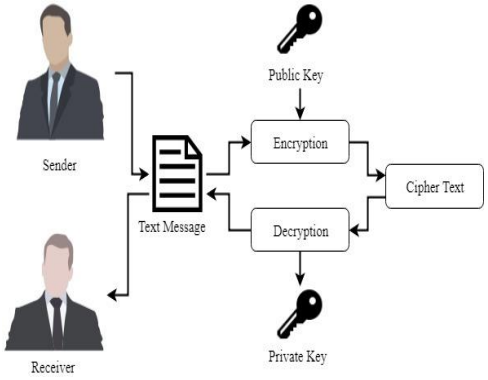


**Fig. 3. Key Generation**

The public key has seen commonly the sender and the collector. In any case, the private key is kept secret and no longer detectable to the end customer. The stages of key generation are:

**Key Generation**

**Generate Public Key**

a) Choose two particular prime numbers $m$ and $n$.

b) For sanctuary intentions, these prime numbers $m$ and $n$ ought to be picked indiscriminately, and must be of comparable bit-length.

c) Compute $a$

$$a = mn. \quad (1)$$

i. Where $n$has utilized as the modulus for both the public and private keys. Its length is communicated in bits which is key length.

**Generate Private Key**

d) Figure $\delta(a)$

$$\delta(a) = \delta(m)\delta(n) = (m-1)(n-1) = a-(m+n-1), \quad (2)$$

Where$\delta$is Euler's totient function.

e) Pick a whole number $e$ such an extent that $(1 < e < \delta a) and \gcd(e, \delta(n)) = 1;$

i. i.e.,$e$ and $\delta(n)$ are co-prime.

ii. $e$ is a public key exponent. $e$ is having a short bit-length and small Hamming weight results, for example: $216 + 1 = 65{,}537$. Notwithstanding, if the estimation of $e$ is small.

e.g:- $e = 3$ have been less secure.

f) Determine $k$

$$k \equiv e - 1 \left(mod\delta(a)\right) \quad (3)$$

i.e., $k$ denotesthe multiplicative inverse of $e$ $(modulo\delta(a))$.

g) Solve $k$ given $k \cdot e \equiv 1 \left(mod\delta(a)\right)$

**Encryption**

Utilizing an encryption key [30]$(e, a)$, the encode and the decode function can be explained in the following two equations.

$$j \equiv i^e (moda) \quad (4)$$

$$i \equiv j^e (moda) \quad (5)$$

The public key $(e, a)$, resolve the private key $(d, a)$. The technique is for all intents and purposes hard to execute. Known decided $(e, a)$. That the calculation of the encryption method j≡i^e (moda) the time essential is I polynomial capacity (decryption process is similar); while, in case you have to decipher the prerequisite for a to do prime factorization. To do prime factorization (or the unpredictability of what could be compared to this). Moreover, when differentiated the general encryption algorithm, the RSA algorithm has obvious focal points of another, without sending and getting simultaneously on the opposite sides related with the encryption methodology.

**C. The Particle Swarm Optimization Algorithm**

The Particle Swarm Optimization (PSO) [31] algorithm is an adaptable algorithm of a masses of individuals (for the most part known as particles), altering through returning stochastically toward ahead of time effective regions. PSO's basic managers are speeds resuscitate and role invigorate. All through every consideration, a particle is lifted toward particles in a before magnificent position and worldwide best position. Each particle's new pace cost has resuscitated at emphasizes, this being set up on current speed, distance from going preceding quality function, and distance from a worldwide appealing position and this computes the particle's ensuing position in the inquiry zone. The method stops both on the emphasis of the exact wide collection of events or until the procurement of a base blunder.

**D. Objective Function**

The classic reason for the PSO algorithm is to manage the storge minimization issue: The goal of work is similarly called the fitness function. The number of bits in a specific decimal whole number. A positive whole numben has b bits when

$$2^{b-1} \leq n \leq 2^b - 1 \quad (6)$$

PSO starts with a pack of irregular particles/solutions, looking for optima by means of reviving generations. The two "quality" values - $pbest$ and $gbest$ of a molecule is upto date with every iterations. '$pbest$'is the best solution(fitness) carried out till at that point and '$gbest$' amazing regard got up to that point by techniques for any populace's molecule. PSO is computationally clear including handiest unrefined scientific administrators. Molecule positions/speeds are subjectively consigned to the pack of guidelines' start.

**E. Update velocities of particles**

PSO refreshes all velocities and positions of particles iteratively as pursues:

$$Ve_x^d = wgtVe_x^d + Const_1 r_1 (P_x^d - newp_x^d) + Const_2 r_2 (P_g^d - newp_x^d) \quad (7)$$

$$newp_x^d = newp_x^d + Ve_x^d \quad (8)$$

Where, $x$ - Size of the populace,

$wgt$ - Inertia weight,

$r_1$ and $r_2$ are random values in the range [0, 1],

$Const_1, Const_2$ are the positive constants,

$newp_x^d$ - The particle's new position.

$d$- Number of dimensions,

$Ve_x^d$ - new velocity of the $xth$ particle registered dependent on the particle's past velocity, distance between the past best position and the current position and distance between the best particle of the swarm.

In the ordinary PSO, particles are gotten in an adjacent perfect in $gbest$ zone if $gbest$ is a long way from ideal. To vanquish this, particles fly through a more noteworthy interest space with a molecule's $pbest$ work being state-of-the-art reliant on the $pbest$ function of all swarm particles so improving swarm range and keeping up a distance from off best quality. The molecule's invigorating speed is given with the guide of:

$$Ve_x^d = wgt * Ve_x^d + Const * rand_x^d * (pbest_{fx(d)}^d - newp_x^d) \quad (9)$$

Where $f_x = [f_x(1), f_x(2) \ldots . f_x(d)]$ refers to the $pbest$ that the particle $x$ used and $f_x(d) pbest$ is the measurement of particle's $pbest$ . Two particles are pickedarbitrarily and one whose speed is resuscitated is overlooked. To energize the speed, particles pbest's fitness values are analyzed and the best valuation has selected.

**F. Stopping principle**

The algorithm has finished after a predefined number of iterations, or once the fitness estimations of the particles (or the particles themselves) are connecting in some sense.

**Favorable circumstances of the PSO algorithm**

The fitness limit can be non-differentiable (just estimations of the fitness work are utilized). The system can be associated with the optimization issues of significant estimations, normally conveying quality arrangements more quickly than elective strategies

**Inconveniences of the PSO algorithm**

There is no expansive association theory appropriate to experiment, multidimensional issues. For sufficient outcomes, tuning of data parameters notwithstanding exploring differing ways as for different kinds of the PSO system is significant at some times. Stochastic fluctuations of the PSO results are high for certain issues and some estimation of the parameters. In like way, a few kinds of the PSO technique rely on the choice of the ease system.

In our foreseen shape; we used the following advances:

i. RSA algorithm used for moored unequal communication..
ii. After the encryption, we have to use the PSO algorithm for optimization.
iii. Uneven length One Time Password (OTP) with a combination of numeric, alphanumeric as well as an extraordinary character.
iv. OTP can't be recognized more than once (even by the authorized client) inside a permissible time span (approx.1-2 minute) if another way or some other user gives it wrong for the first time.
v. The client will be logged out even from the first stage of confirmation for example login reliant on the static secret word if the wrong OTP has given. In the anticipated security form the primary client needs to create keysets, using any public key cryptography algorithm (for example RSA algorithm)

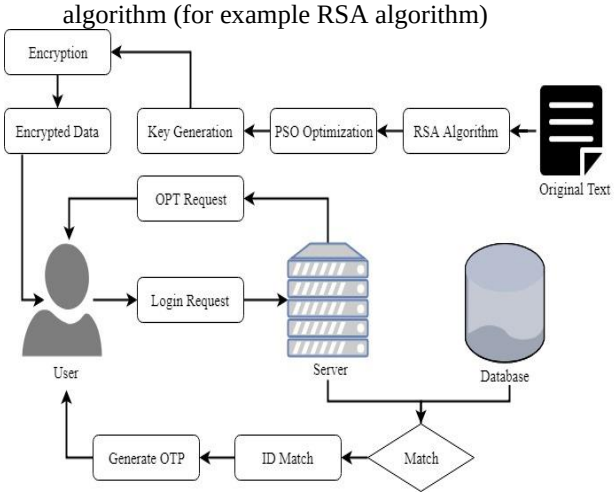


**Fig. 4: Proposed Block Diagram**

In the formed structure, the customer will demand the login with ID and mystery word. If the data offered by the customer coordinates the data gathered in the database, the server conveys an OTP. In our proposed system, the variable-length one-time password has been utilized for checking the customer. The variable-length mystery key ought to be of least 6 characters and most outrageous 10 characters long. The OTP ought to be an authentic combination capitalized character, lower case character, numeric and special characters.

The customer should not be series the length of variable OTP [32] and its incorporation that would be recommended by the server for that specific session. This system will update the security and position moreover trouble for software engineers and intruders since it will abolish the settled precedent being made in a standard OTP. What's more, the variable-length OTP ought to be considered for a constrained limit of time (1-2 minutes, configurable from the server side). Generally inside that time range, if the customer outfits the wrong OTP, a wrong message is being demonstrated alluding that the wrong OTP had been entered. Notwithstanding, the customer can even now sign in case he can offer the right OTP inside that timeframe. Regardless, in our anticipated structure it has been prepared, the OTP can't be recognized more than once (even by authentic customer) inside a acceptable timeframe (approx.1-2 minute) if by certain strategies the customer gives it wrong at the first level, customer will be logged out even from the main phase of affirmation for instance login subject to static mystery key if the wrong OTP is given, with the target that the gatecrasher doesn't get any opportunity to avert the true customer and retry the OTP on their advantage. The customer needs to begin once more.

## IV. MATHEMATICAL MODEL

Protection in data communication is an extra important issue to be considered while planning systems, as remote sensor systems, might be passed on in threatening regions, for example, battle areas. In light of threatening situations and unprecedented properties of frameworks, it is a demanding task to ensure delicate information transmitted by remote sensor systems. Some preliminary methodologies are utilized, for example, particular encoding methods for encryption, unique key sizes. One of a kind key size is utilized to seek after the execution of the picked algorithms explicitly time use.

### A. Key Management of algorithms

The key organization is the central and most important perspective for security data in the cryptosystem. In case the key is strong and secure from the unapproved organization, the cryptography algorithms will have all the more compelling capable. We would state that we utilize the key size of 125 bits, 512 bits, 2048 bits, and 3096 bits

### B. Average Time

The average time is the time in between of which a program is running (executing), rather than other program lifecycle stages, for instance, execute time, interface time just as the heap time. The instruction to find out the average encryption time has determined in the condition (9).

$$Avg.Time = \frac{1}{N}\sum_{i=1}^{N}\frac{M_i}{T_i} \quad (10)$$

Where, $N$ - Number of Messages
$M_i$ - Message Size
$T_i$ - Time taken to Encrypt Message $M_i$
Encryption time has used to decide the throughput of an encryption plot. It exhibits the speed of encryption. The throughput of the encryption plot has enlisted as in condition (11).

### C. Throughput

On account of the encryption plot, throughput has figured as the average of consolidated plain substance in k bytes separation by the normal encryption time and by virtue of decryption plan, throughput has prepared as the average of accumulation figure content is segregated by the average decoding time.

$$Throughput = \frac{Totalplaintext\ (bytes)}{Encryptiontime\ (second)} \quad (11)$$

### D. Simulation time

The time essential by the algorithm for arranging absolutely a particular length of information has set apart as the recreation time. It relies on the processor speed, the complex design of the algorithm, and so forth. The small estimation of reenactment time is approved through (12).

$$SimulationTime = \frac{datasize}{speed} \quad (12)$$

## V. PERFORMANCE MEASURES

The execution ration of encoding and decoding plans were coordinated utilizing some execution estimations, for example, normal encryption time, reenactment time, throughput, adjusting the packet size and altering the key size for the picked cryptographic algorithms. The assessments are played out certain times to guarantee that the outcomes are steady and are authentic to watch the modified algorithms.

The encryption time was checked for the RSA-PSO with four different key sizes. The complete time is taken to convey a cipher-text from plain-content. The collected encryption time is then used to figure the throughput of the encrypted algorithm.

**Table I: Performance Measure of RSA-PSO Encryption, Decryption Time**

| Key Size (bits) | File Size | Encryption Time (s) | Decryption Time (s) |
|---|---|---|---|
| | (byte) | | |
| 125 | 640 | 11.8085 | 16.41 |
| 512 | 640 | 11.5581 | 9.568 |
| 2048 | 640 | 11.9839 | 14.839 |
| 3096 | 640 | 11.6294 | 17.8085 |

The Table 1 shows that the encryption and decryption time cipher text using special key sizes. The key size of the algorithm has used in these experiments is furthermore mentioned in the table. The majority of the outcomes are gotten with a due discussion, for accomplishing higher exactness of total execution time were taken then an average of tests were taken for the estimation and relative examination among algorithms. Encryption and decryption time have prepared in second and the data measure is taken in bytes. All the individual recognition readings have appeared.

### A. RSA-PSO Optimization for Different Key size

**Table II: RSA with PSO Optimization**

| Key Size (bits) | Average Time (s) | Simulation Time (s) | Throughput (s) |
|---|---|---|---|
| 125 | 69.626 | 830.81 | 133.8764 |
| 512 | 77.731 | 1294.6 | 154.991 |
| 2048 | 79.437 | 1521.549 | 171.4686 |
| 3096 | 78.401 | 1452.214 | 148.8429 |

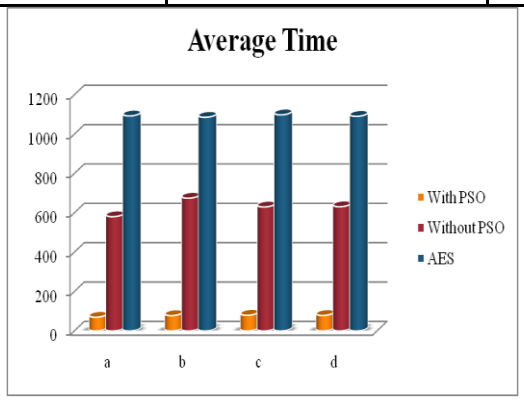


**Fig. 5. Comparison between Average Processing Time for different Key sizes a)125 bit b)512 bit C) 2048 bit d)3096 bit**

Figure 5 exhibits that the proposed average handling time of RSA-PSO utilizing the particular arrangement of keys fluctuated with the current strategy. That the figure addresses the proposed system contains base managing time separated from different procedures.

The throughput of the encryption plan portrays the speed of encryption. Right when there is an advancement in the throughput of the encryption algorithm, there is a reducing in the power use algorithm. Having a high throughput, the prescribed structure is set up to be associated in speedy nonstop encryption applications.

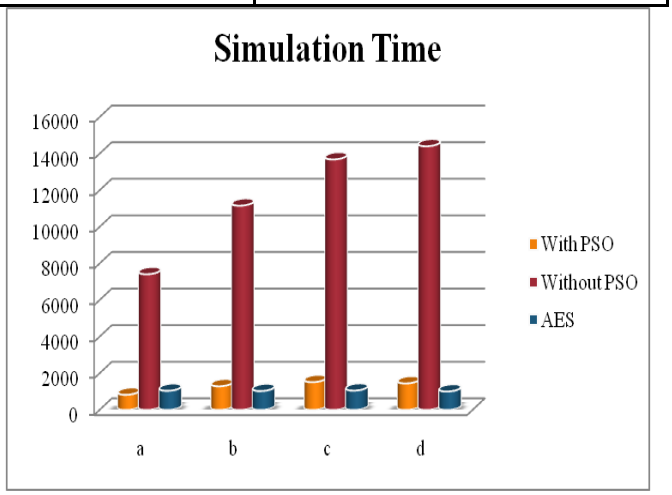


**Fig. 6. Comparison between Simulation time for different Key sizes a) 125 bit b) 512 bit C) 2048 bit d) 3096 bit**

### B. Without Optimization for Different Key size

The Tables 3 and Fig. 5-7 exhibit the connection of security nature of RSA-PSO, RSA, and AES. It is found that when the little length of the key for RSA is used, by then RSA is more potent.

### C. Existing AES for Different Key size

AES is a block cipher with a block length of 128 bits. AES licenses differing key lengths: 125, 512, 2048, and 3096 bits. Encryption contains 10 rounds of getting ready for 125-bit keys, 12 rounds and 14 rounds for 512-bit keys, etc. Each round of managing combines one single-byte based substitution step, a line smart stage step, a segment insightful mixing, and furthermore the round key. The solicitation in which these four phases are executed is differing for encryption and decryption.

Table 4 shows the encryption throughput, recreation and average time of the AES for the four steps. The throughput also illuminated that the encryption speed of AES is high when diverged from the "without optimization" algorithm for the four steps. The tables 2, 3, and 4 show the throughput, average time and reenactment time of encryption algorithms with different key sizes. From the examination, it shows that RSA-PSO has favored throughput over that of existing algorithms.

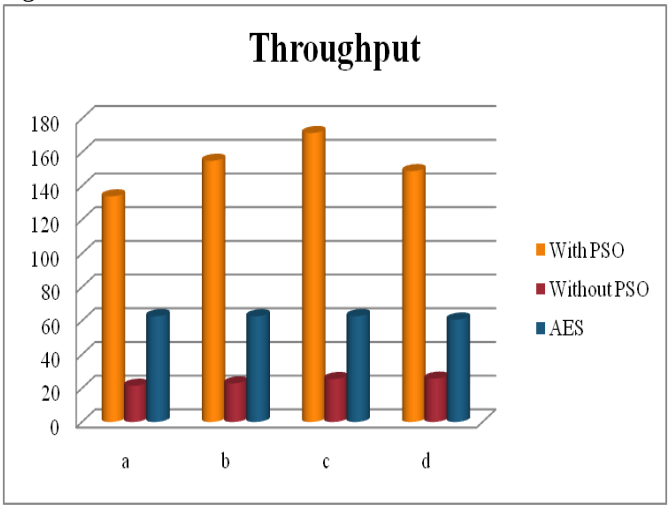


**Fig.7. Comparison between throughputs for different Key sizes a)125 bit b)512 bit C) 2048 bit d)3096 bit**

**Table III: Without PSO Optimization**

| Key Size (bits) | Average Time (s) | Simulation Time (s) | Throughput (s) |
|---|---|---|---|
| 125 | 580.4896 | 7418.314 | 21.47497 |
| 512 | 674.7848 | 11164.8 | 22.8621 |
| 2048 | 630.1243 | 13693.12 | 25.4568 |
| 3096 | 631.2571 | 14411.15 | 25.7074 |

**Table IV: Existing Method AES**

| Key Size (bits) | Average Time (s) | Simulation Time (s) | Throughput (s) |
|---|---|---|---|
| 125 | 1092.758 | 1047.216 | 62.7769 |
| 512 | 1085.882 | 1033.042 | 62.7139 |
| 2048 | 1098.399 | 1058.759 | 62.8187 |
| 3096 | 1090.853 | 1010.34 | 60.7781 |

## VI. CONCLUSION

Both symmetric, as well as the asymmetric key algorithms, are significantly capable of anchoring the exchanged data over any communication medium. In this paper, asymmetric key cryptography utilizes two separate keys to hold any illegal access to the data. The public key stays public and the private key isn't shared. This framework ensures favored security over the past. Moreover, the use of OTP generation if there should develop an event of asymmetric key cryptography gives high data security and non-repudiation. Nonetheless, symmetric-key cryptography has some prominent applications in context on its ease.
It is computationally infeasible to process the plaintext from the public key and the cipher text.

OTP is considered to anticipate replay ambushes which have a high ground over static mystery phrase-based confirmation. In this paper, we utilized public-key cryptography (RSA algorithm) for encoding and decoding the OTP. In addition, OTP can't be perceived more than once (even by the veritable client) inside an appropriate time span (approx.1-2 minute) if sometimes customer gives it wrong in the main stage. Everything considered, will be logged out even from the first stage of checking for instance login subject to the static mystery key if the wrong OTP is given and needs to start fresh. This framework is especially secure in examination with the current similar certification strategies.

## REFERENCES

1. Dang, Philip P., and Paul M. Chau. "Image encryption for secure internet multimedia applications." IEEE Transactions on consumer electronics 46, no. 3 (2000): 395-403.
2. Mangold, W. Glynn, and David J. Faulds. "Social media: The new hybrid element of the promotion mix." Business horizons52, no. 4 (2009): 357-365.
3. Gambardella, Alfonso, and Salvatore Torrisi. "Does technological convergence imply convergence in markets? Evidence from the electronics industry." Research policy 27, no. 5 (1998): 445-463.
4. Zissis, Dimitrios, and DimitriosLekkas. "Addressing cloud computing security issues." Future Generation computer systems 28, no. 3 (2012): 583-592.
5. Toole, Jameson L., SerdarColak, Bradley Sturt, Lauren P. Alexander, Alexandre Evsukoff, and Marta C. González. "The path most traveled: Travel demand estimation using big data resources." Transportation Research Part C: Emerging Technologies 58 (2015): 162-177.
6. Perrig, Adrian, Robert Szewczyk, Justin Douglas Tygar, Victor Wen, and David E. Culler. "SPINS: Security protocols for sensor networks." Wireless networks 8, no. 5 (2002): 521-534.
7. Messerges, Thomas S., Ezzat A. Dabbish, and Robert H. Sloan. "Examining smart-card security under the threat of power analysis attacks." IEEE transactions on computers 51, no. 5 (2002): 541-552.
8. Bajaj, Sumeet, and RaduSion. "Trusteddb: A trusted hardware-based database with privacy and data confidentiality." IEEE Transactions on Knowledge and Data Engineering 26, no. 3 (2014): 752-765.
9. Potlapally, Nachiketh R., Srivaths Ravi, AnandRaghunathan, and Niraj K. Jha. "A study of the energy consumption characteristics of cryptographic algorithms and security protocols." IEEE Transactions on mobile computing 5, no. 2 (2006): 128-143.
10. Boyd, Colin, and Juan Manuel González Nieto. "Round-optimal contributory conference key agreement." In International Workshop on Public Key Cryptography, pp. 161-174. Springer, Berlin, Heidelberg, 2003.
11. Pareek, N. K., VinodPatidar, and K. K. Sud. "Discrete chaotic cryptography using external key." Physics Letters A 309, no. 1-2 (2003): 75-82.
12. Chao, Hui-Mei, Chin-Ming Hsu, and Shaou-Gang Miaou. "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records." IEEE Transactions on Information Technology in Biomedicine 6, no. 1 (2002): 46-53.
13. Boneh, Dan, and Matt Franklin. "Identity-based encryption from the Weil pairing." In Annual international cryptology conference, pp. 213-229. Springer, Berlin, Heidelberg, 2001.
14. Subashini, Subashini, and VeerarunaKavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34, no. 1 (2011): 1-11.
15. Lagendijk, Reginald L., ZekeriyaErkin, and Mauro Barni. "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation." *IEEE Signal Processing Magazine*30, no. 1 (2013): 82-105.
16. Mao, Yinian, and Min Wu. "A joint signal processing and cryptographic approach to multimedia encryption." IEEE Transactions on Image Processing 15, no. 7 (2006): 2061-2075.

17. Pareek, Narendra K., VinodPatidar, and Krishan K. Sud. "Image encryption using chaotic logistic map." Image and vision computing 24, no. 9 (2006): 926-934.
18. Panda, Prabhat K., and SudiptaChattopadhyay. "A hybrid security algorithm for RSA cryptosystem." In Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on, pp. 1-6. IEEE, 2017.
19. Kwok, H. S., and Wallace KS Tang. "A fast image encryption system based on chaotic maps with finite precision representation." Chaos, solitons& fractals 32, no. 4 (2007): 1518-1529.
20. Chien, Tsun-I., and Teh-Lu Liao. "Design of secure digital communication systems using chaotic modulation, cryptography and chaotic synchronization." Chaos, Solitons& Fractals 24, no. 1 (2005): 241-255.
21. Parah, Shabir A., Javaid A. Sheikh, Abdul M. Hafiz, and GhulamMohiuddinBhat. "Data hiding in scrambled images: A new double layer security data hiding technique." Computers & Electrical Engineering 40, no. 1 (2014): 70-82.
22. Chang, Henry Ker-Chang, and Jiang-Long Liu. "A linear quadtree compression scheme for image encryption." Signal Processing: Image Communication, vol. 10, no.4, pp.279-290, 1997.
23. Sabir, Firas Ali. "Hiding Encrypted Data in Audio Wave File." International Journal of Computer Applications 91, no. 4 (2014).
24. Kalaiarasi, G., C. Umadevi, A. Shanmugapriya, P. Kalaivani, F. Dallemer, and R. Prabhakaran. "DNA (CT), protein (BSA) binding studies, anti-oxidant and cytotoxicity studies of new binuclear Ni (II) complexes containing 4 (N)-substituted thiosemicarbazones." InorganicaChimicaActa 453 (2016): 547-558.
25. Madaan, Vishu, Dimple Sethi, PrateekAgrawal, Leena Jain, and Ranjit Kaur. "Public Network Security by Bluffing the Intruders Through Encryption Over Encryption Using Public Key Cryptography Method." In Advanced Informatics for Computing Research, pp.249-257. Springer, Singapore, 2017.
26. Ourivski, Alexei V., and Thomas Johansson. "New technique for decoding codes in the rank metric and its cryptography applications." Problems of Information Transmission, vol.38, no.3, pp.237-246, 2002.
27. Huang, Yun, Zheng Huang, Haoran Zhao, and Xuejia Lai. "A new one-time password method." IERI Procedia, vol.4, pp.32-37, 2013.
28. Al-Riyami, Sattam S., and Kenneth G. Paterson. "Certificateless public key cryptography." In International Conference on the Theory and Application of Cryptology and Information Security, pp. 452-473. Springer, Berlin, Heidelberg, 2003.
29. Brakerski, Zvika, and Gil Segev. "Function-private functional encryption in the private-key setting." Journal of Cryptology, vol.31, no.1, pp.202-225, 2018.
30. Liu, Yang, Shanyu Tang, Ran Liu, Liping Zhang, and Zhao Ma. "Secure and robust digital image watermarking scheme using logistic and RSA encryption." Expert Systems with Applications, vol.97, pp.95-105, 2018.
31. Nouiri, Maroua, AbdelghaniBekrar, AbderezakJemai, SmailNiar, and Ahmed ChihebAmmari. "An effective and distributed particle swarm optimization algorithm for flexible job-shop scheduling problem." Journal of Intelligent Manufacturing, vol.29, no.3, pp.603-615, 2018.
32. Florêncio, Dinei, and Cormac Herley. "One-time password access to any server without changing the server." In International Conference on Information Security, pp. 401-420. Springer, Berlin, Heidelberg, 2008.


## AUTHORS PROFILE

**Mr. Mrinmoy Sarkar**
Mr. Mrinmoy Sarkar is now Head of The Department of ECE at Bankura Unnayani Institute of Engineering, Bankura, W.B. His Main research are on Data Security and Networking. Communication and Signal Processing. He has more than 8 publications in different International and National Journals and Conference Proceedings.

**Prof. (Dr.) Asok Kumar**
Prof. Asok Kumar is the Principal of MCKV Institute of Engineering, Howrah, W.B. His main research area on Data Security and Networking. Communication and Signal Processing. He has more than 41 publications in different International and National Journals and Conference Proceedings.

**Pr (Dr.) Bansibadan Maji,** Prof. Bansibadan Maji is now a senior Professor of ECE Department in NIT, Durgapur, and West Bengal, India. He is now Head of The Department of ECE at NIT. His main research area on Microwave, Antenna, VLSI Design and Low power Device and Circuits. He has more than 56 publications in different International and National Journals and Conference Proceedings. He has published more than 50 research articles in peer-reviewed international journals, national and international conferences.