International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V70I5P104

Volume 70 Issue 5, 33-38, May 2022

Original Article

Design of Hybrid Cryptography System Based on Vigenere Cipher and Polybius Cipher

Anzar Ahmad Raina[1], Saood Rasool Shah[2], Mehwar Raj[3], Waqqas Manzoor[4]

[1,2,3,4]*Lovely professional university, Punjab.*

Received: 18 March 2022 Revised: 10 May 2022 Accepted: 18 May 2022 Published: 28 May 2022

Abstract *- Cryptography is gotten from a Greek word that suggests the specialty of guaranteeing information by transforming it into a tangled association and unintelligible organization. It is a blend of math and computer programming. The explosive development of the internet has made an extended knowledge of interest vulnerability issues. Even though security is the action stressed over the web,various applications have been made and organized, disregarding principal objections of information security: secrecy, validation, and insurance. As our step-by-step practices become progressively more subject to information organizations, the meaning of comprehension of such security issues and inconvenience will likewise increment. Cryptography is required to prevent a few unwanted clients or people from acquiring induction to the information. This paper presents another half-breed security figure by joining the two most significant Ciphers, Polybius Cipher and Vigenére Cipher. This half and half encryption figure give more noteworthy security than exemplary codes. Index Terms—Encryption, Cryptography, Polybius Ciphers, Vigenére Ciphers.*

Keywords *- Encryption, Cryptography, Polybius Ciphers, Vigenére Ciphers.*

1. Introduction

In the current bearing of the world, the advancements have progressed such a lot that most individuals incline toward using the web as the fundamental plan to consign data beginning with one end and then onto thefollowing over the world. There are various likely ways to deal with conveying data utilizing the web: through messages, talks, etc. The data change is made very snap, speedy and careful using the internet. One of the essential testswith sending data over the web is the "security risk"; for example, the individual or privy information can be stashed or hacked according to different points of view. It turns out to be fundamental to think about information security along these lines. It is one of the mostvital factors that need to be thought about during the interaction of data move. Security is a critical variable in the open framework, and cryptography expects a huge occupation in this field. Cryptography is old and ensures the arrangement of information out in the open framework. Nevertheless, the objective of cryptography is used not only to give classification but also to give plans to various issues: data trustworthiness, check, and non-refusal [2]. Cryptographyis characterized as embodying and inventing strategies that license significant data and information to be sent in a safeguarded structure. The goal is that the vitally individual prepared to recuperate this data is the cognisant recipient [2]. Cryptography is a deliberate methodand strategy to conceal information and data over acorrespondence channel. It is craftsmanship to conceal the information from outcasts. As the development develops bit by bit, the requirement for information security over thecorrespondence channel is extended to a serious level. Encryption is characterized as a precise strategy of evolving plain messages into ciphertext. The encryption process needs a modified encryption calculation and a key tochange over the plain message in figure [3]. In cryptography, framework encryption executes at the message source side. Encryption executes the message next to the senderpreviously sending it to the collector.

2. Literature Survey

The security for web keeping cash, account passwords,messages, secret account words, and so on requires contentprotection in automated media [4]. It shows the security besides tension for the data with the move encryption standard. The number of persistent rounds increments the greater security that can be broken by dynamic and latent attacks by programmers, interlopers, and programmers.

Caesar figure, generally called the shifting figure, is the least perplexing and enormous known old-style encryption framework. It is a substitution figure in which each letter in the plaintext is superseded. For example, with a move of 2, A would be replaced by C, B would become D, and similarly. The encryption strategy framework performed by Caesar ciphers is a blend. It completely goes with an intricate development plan asVigenére Cipher, and to date, it enjoys benefits in the ROT13 and paraphrase systems. Likewise, in replacement figures, the Caesar figure is effortlessly and prudently broken, and in present-day structure, the use shows no correspondence between security and assurance [5]. Caesar Cipher's methodology is one of the earliest and least complex strategies for the encryption strategy. It's a benevolent replacement figure, i.e., each letter of a given text is supplanted by a

letter with a decent number ofpositions down the letters in order. For example, with a move of 1, M would be supplanted by N, N would
become O, etc. This strategy is named after Julius Caesar, who used it to talk with his authorities. Accordingly, to encode a given text, we want an entire number worth, known as a move which shows the amount of position each letter of the text has been slipped.

The transposition figure is a cycle and versatile system ofencryption framework. The area and position held by units of plaintext are moved by a standard design or modelso that the ciphertext incorporates a period of the plaintext. The location is the super substitute that is generally involved and pre-location development by giveninferred measurement chart that can be used by string or message given by the shipper [6] [7]. In [8], a changing variety of Vigenére figure calculation was derived as scrabbled, and dispersing is given by combination and summation of an emotional part of every byte and bit before the message and string are blended utilizing the system Vigenére figure. This methodology fails the so-called Kasiski assault spectacularly to find the length of the key because of the cushioning of the message and string with irregular bits. The focal disadvantage and nothing improvement of this frameworkis that the size of the blended message and string will be expanded by approximately determined 56%.

One more procedure for executing the Vigenére calculation was introduced and raised as through typically and systematically for encryption and dispersion of message need key to be supplanted repeatedly. Yet, here, essential keys act as Continuation for the trade of substituted keys for the cycle [9]. The new method has been introduced in this paper as Vigenére Cipher comprises alphabetic mathematical and punctuation marks as colon,comma, semicolon, question marks, underline, full stop, and sections are utilized as the key rather than character toshape it progressively hard for dynamic and latent assaultand assaults and spreading this spread the rang, so literatepeople who comprehend fundamental of cryptography can recognize the message [10] [11].

The web is one of the most dangerous communication mediums due to its tremendous affiliation andopen framework. Information confirmation is one of the essential parametric prerequisites. At present unique security, calculations are proposed to achieve security during correspondence. Every one of them has specific legitimate explanations and certain awful points. To work on the nature of the encryption algorithm, they proposed a mixed-race model. The proposed model is a blend combination of AES and DES algorithmic cryptographic. The two calculations are symmetric key strategies, and they are particularly capable of encryption. Compromise of AES and DES would give a strong level of safety at the encryption end. A basic improvement in outcomes has been seen with the proposed plan [12]

3. Theories

Laptops will be unreliable, assuming they are related to a worldwide framework, especially the web [2]. The locales visited an extraordinary degree have diseases, malware, or the like that can take particular information from a PC. Security is fundamental to keep up a decent critical way from information replication, stealing, visualizing, discovery and interruption. The center of PC security is done to ensure the PC and its framework guarantee the data are safe and secure inside the framework.[13].

PC security works and consolidates a couple of points, forexample:

- Privacy is generally that is classified. The reality of the matter is an expectation with the objective that unapproved individuals don't get data and information. Avoidance is possible by using encryption advancement so that the information owner can find veritable information.
- Confidentiality includes many rules or a promise usually executed through privacy rule agreements that limit access or put limitations on specific types of data. When mentioned to demonstrate somebody's bad behavior, it shows whether or not the information keeper will offer data to the individual who referenced it or keep up the customers.
- Non-disavowal is the interaction that sides to the capacity to ensure that associated with an understanding or a communication can't keep the realness from securingtheir mark on a document or the sending of a message that they began. To repudiate means to deny. For a long time, specialists have hoped to make disavowal unthinkable in certain conditions. We might send enrolled mail, for instance, so the recipient can't reject that a letter was conveyed. Consequently, a legitimate file routinely expects observers to check with the objective that the individual who signs can't deny having done this way. On the internet, and progressed mark is used not solely to guarantee that a message or report has been electronically marked by the person that suggested signing the document yet additionally since one individual should make an automated imprint to ensure that an individual can't later reject that they furnished the mark.
- Integrity, Data honesty insinuates the dependability and unwavering quality of information all through its lifecycle. It can depict the state of your information, e.g., significant or invalid, or the most common way of ensuring and safeguarding the legitimacy and accuracy of information.
- Authentication is a well-being exertion arranged and processed to develop the authenticity and unity of a transmission, message, or pre originator, or techniques for Checking a person’s approval to get express groupings ofdata. It is done to check the login client who is trying tosign in to obtain the message. It checks first the client subtleties for login as username and password. Then after

checking the entire subtleties, it permits entering the framework. It is a significant interaction for the protection of information.

- Availability guarantees that frameworks, applications, and data are open to clients when they need them. The most broadly perceived attack that impacts accessibility isthe denial of an organization in which the assailant interferes with admittance to information, system, devices, or other network resources. A refusal of organization in an inward vehicular organization could achieve an ECU not havingthe choice to get to the information expected to work. The ECU could become non-operational or, most noticeably, horrible; it could convey the structure to a hazardous state. It is vital to consolidate reiteration ways and failover procedures in the arranging stage to avoid availability issues. Similarly, incorporate interruption evasion frameworks that can screen network traffic configuration and conclude whether there is an irregularity and square network traffic when required.

Cryptography has four essential parts, for example:

- The plaintext is characterized as a message that can beperused.
- The ciphertext is an irregular unscripted, questioned, and informal message that can't be perused.
- The key is an imperative angle for characterizing the cryptographic techniques, for example, symmetric andasymmetric.
- A calculation is a procedural answer for executing encryption and unscrambling calculations in the framework.

Cipher: In cryptography, a code (or code) is an algorithm for performing encryption or decoding (unscrambling) a movement of especially described propels that can be followed as a strategy. Another choice, a less ordinary term, is encipherment. To encipher or encode is to change data from plaintext into code or code. In non-technical use,a 'cipher' is something comparative to a 'code'; in any case, the ideas are obvious in cryptography. In standard cryptography, ciphers were perceived from codes. Codes generally substitute differing length plans of characters in the yield, while ciphers routinely substitute a muddled number of characters from are input. There are extraordinary cases, and some cipher systems may utilize conceivably more or less characters when yield versus the number that was input.

3.1. Vigenére Cipher

Vigenére Cipher is a procedure for scrambling [A to Z] letters. It uses an essential kind of polyalphabetic replacement. A polyalphabetic figure is a known code that relies on replacement, using various substitution letter sets. The encapsulation of the first plaintext is done using the Vigenére square table [14].

A	B	C	D	E	F	G	H	I	J	K	L	M	NM	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	DE	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fig. 1 Vigenére Square Table Encryption

The principal letter of the plaintext, letter set S that is ina row joined with letter set L is the key that is a section, the primarily given letter of the source and beneficiary side key that results in the result as D. Then, at that point, E is a line, and key I is a column. It will result as M in the hybrid of both rows as a message by shipper and section as the key. Likewise, other letters will be handled in a similar organization, resulting in an encoded message. The plaintext (P) and key (K) are added to the modulus of 26.

The plaintext (P) and key (K) are added to modulus of 26. Ei = [Pi + Ki] modulus (26) -(1) Using (1), one may convert plaintext intociphertext, as shown below.

Plaintext: SECURITY Key: LION LION Ciphertext: DM Q H C Q H LDecryption

Decryption is come about by deliberately taking off to the row in the table contrasting with the key, tracking down the circumstance of the ciphertext letter that is in this column,and subsequently using the column's name as plaintext. Asan example, in column L (from LION LION) that is critical, and the ciphertext seems D in the column will result in the plaintext yield as S in therow. Along these lines, also, different letters in order will be found in columns and column, and afterward, the specific plaintext will come asoutput.

The less complex and more straightforward methodology is to see Vigen'ere logarithmically and changing over letter sets [A-Z] into numerically as [0-25].

Di = (Ei − Ki + 26) modulus26 -(2)

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Fig. 2 Polybius Square

3.2. Polybius Square Cipher

The Polybius square is displayed as a figure of 5x5 grids occupied with letters inside for encryption. Polybius Square is a table that grants someone to change over letters into numbers. This table can be randomized and granted to the recipient to make the insignificant encryption harder. To fit the 26 letters of the letters all together into the 25 cells made by the table, the letters 'I' and 'J' are by and large merged into a lone cell. At first, there was no such issue because the old Greek letters all together had 24 letters. A table of greater size could be used assuming that a language contains a colossal number of letters altogether [15].

Encryption: Example: D is set in line 1 and segment 4, so it brings about yield coded as 14; O is put in column 3, column 3, it is result yield coded as 34. In this way, Encrypted messages result in message DOG as 14, 34, 23.

Decryption: Polybius unscrambling requires knowing the grid and comprises a replacement of several directions by the relating letter in the grid.

Example: 12 envision for the first-line and second section, as result letter B, 45 imagine for fourth line and fifth segment that results from U and go on as same. Decoded message result as BUS.

4. Methodology

The procedure uses a mix of Vigen'ere cipher and Polybius Square Cipher in its encryption cycle. The ciphertext will at first be chipped away at using the Vigen'ere cipher. A chosen key from erratic will begin the cycle.

Toward the finish of the interaction, the resulting ciphertext then turns into a key for the Polybius Square Cipher process. The key is used to chip away at the message, which is the plaintext, to create the last ciphertext. This1 cycle will make the last ciphertext continuously difficult to break using existing cryptanalysis processes. The recipient will finish decryption in a switch request for retrieval of a message from the sender.

A product program will be formed to display the viability of the estimation using python coding, and different cryptanalysis procedures will be performed on the ciphertext. A flowchart portraying the Hybrid Algorithm is displayed in Fig. 3.

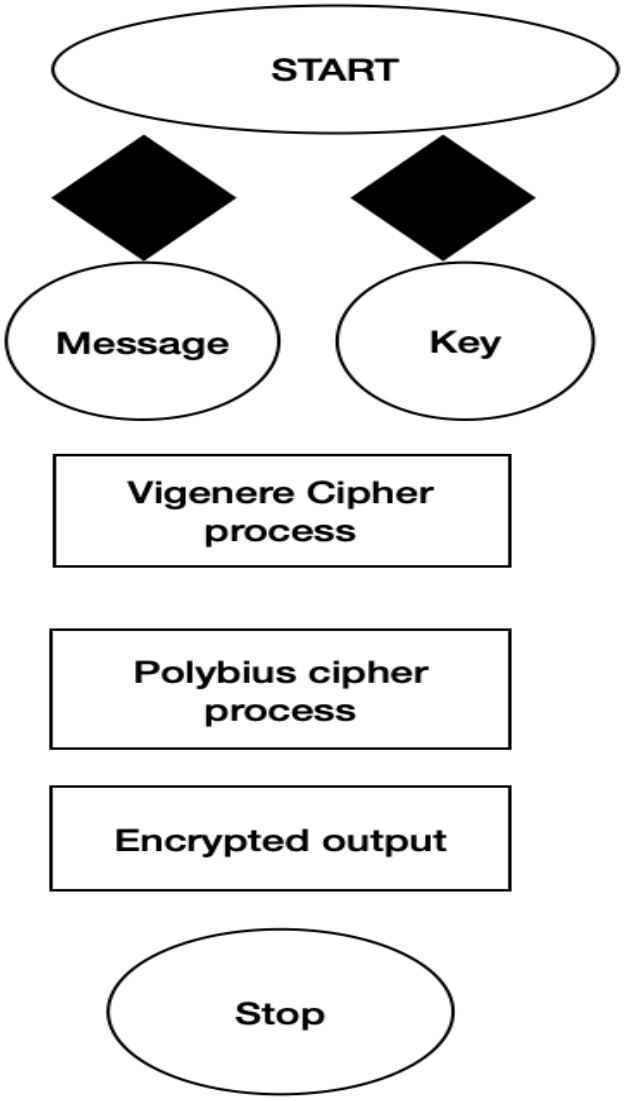

Fig. 3 Flowchart of Hybrid Algorithm A

4.1. Encryption

Phase 1 (Vigen'ere Cipher)
STEP1: MESSAGE - AMERICANVIRUSSTEP2: KEY- DELHI

STEP3: OUTPUT- DQPYQFEYCQUYD

Phase 2 (Polybius Cipher)

STEP4: TEXT-DQPYQFEYCQUYDSTEP5: OUTPUT-411453451412514531145445 41

We can see yield is in a NUMERICAL configuration where the shipper has sent as in ALPHABETICAL organization. Indeed, even the Vigen'ere figure result yields as in dispersed, messy, and unformatted ALPHABETS, which is likewise gotten; however, once more passing that treating Vigen'ere yields as Polybius input and then, at that point, brings about the mathematicalorganization that makes it more prominent secure also, complex than the utilization of single codes.

4.2 Decryption

Phase 1 (Polybius Cipher) STEP1: MESSAGE- 41 STEP2: OUTPUT- D Phase 2 (Vigen'ere Cipher) STEP3: TEXT- D STEP3: KEY- DELHI STEP4: OUTPUT-A

We can see decipher yield is showing up after Switching the interaction of through Polybius figure and then Vigenére figure above all else. This makes it intricacy for gate crashers, aggressors, and programmers to befuddle them and stop them from imitating, duplicating, or damage the framework through different sorts of dynamic and aloof assaults. The Biggest benefit of this cycle can be utilizing armed force, police framework, and secure message correspondence and transmission. Thus, we can see the execution of the encryption also the Decryption cycle of the Hybrid code process thatstreams methodically through the Polybius and Vigenére figure framework. Python Program is composed concerning the Implementation of a Hybrid figure.

5. Conclusion

Cryptography is the most used procedure for the security, protection, classification, and dependability of information. Single exemplary codes are cryptographic strategies seen as least intricate and most helpless in light of various hindrances, limitations, and smooth frameworks. One of thewell-known figures is Vigenére Cipher, yet it likewise has not many downsides. To overcome the obstructions of the Vigenére figure, another method is available an overhauled variation as a mix of Polybius figure and Vigenére that is much safer against assaults like Active, inactive, Kasiski, and Friedman attacks (assaults). Cryptanalysis, repeat assessment, men in center assaults, recurrence investigation, issue examination assaults, plan assumption, and animal power assaults on the proposed technique are moreover much irritating because of the usage of item tables for

encryption. The adjusted crossover blend of the Caesar Figure and Vigenére Cipher is the outcome of an undeniable level of intricacy, dispersing, dissemination, and disarray in the calculation that makes them making it extraordinarily strong figures and difficult to break. Even though there arevarious cryptographic systems yet, this space requires veritable thought of the examination network for the up-degree, refinement, and improvement of information protection and security. Our motivation is to endorse the proposed approachby executing security assaults and execution investigations on messages in the future.

References

[1] S. Chaudhari, M. Pahade, S. Bhat, C. Jadhav, and T. Sawant, A research paper on new hybrid cryptography algorithm.
[2] K. Jakimoski, Security techniques for data protection in cloud computing, International Journal of Grid and Distributed Computing, 9(1) (2016) 49–56.
[3] A. A. Soofi, I. Riaz, and U. Rasheed, An enhanced vigen'ere cipher for data security, Int. J. Sci. Technol. Res, 5(3) (2016) 141–145.
[4] P. Kumar and S. B. Rana, Development of modified aes algorithm for data security, Optik, 127(4) (2016) 2341–2345.
[5] A. Saraswat, C. Khatri, P. Thakral, P. Biswas, et al., An extended hybridization of vigen´ere and caesar cipher techniques for secure communication, Procedia Computer Science, 92 (2016) 355–360.
[6] J. Chen and J. S. Rosenthal, Decrypting classical cipher text using markov chain monte carlo, Statistics and Computing, 22(2) (2012) 397–413.
[7] M. B. Pramanik, Implementation of cryptography technique using columnar transposition, International Journal of Computer Applications, 945 (2014) 8887.
[8] C. Sanchez-Avila and R. Sanchez-Reillol, The rijndael block cipher (aes proposal): a comparison with des, in Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No. 01CH37186). IEEE, (2001) 229–234.
[9] Q.-A. Kester, A cryptosystem based on vigen'ere cipher with varying key, International Journal of Advin Computer Engineering & Technology (IJARCET), 1(10) (2012) 108–113.
[10] C. Bhardwaj, Modification of vigen'ere cipher by random numbers, punctuations & mathematical symbols, Journal of Computer Engineering (IOSRJCE) ISSN, (2012) 2278–0661.
[11] F. M. S. Ali and F. H. Sarhan, Enhancing security of vigen'ere cipher by stream cipher, International Journal of Computer Applications, 100(1) (2014) 1–4.
[12] P. Gutmann, Cryptographic security architecture: design and verification. Springer Science & Business Media, (2003).
[13] A. P. U. Siahaan, Protection of important data and information using gronsfeld cipher, (2018).
[14] S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, Data security using vigen'ere cipher and goldbach codes algorithm, Int. J. Eng. Res. Technol, 6(1) (2017) 360–363.
[15] M. Maity, A modified version of polybius cipher using magic squareand western music notes, International Journal For Technological Research In Engineering, ISSN, (2014) 2347–4718.
[16] A. Author, Name of paper, Abbrev. Title of Periodical*, vol. x, no. y, pp. zzz-zzz, Mon, year. DOI
[17] J. Grundy and J. Hosking, Developing adaptable user interfaces for component-based systems, Interact. Comput., 14 (2002) 175-194. DOI:10.1016/S0953-5438(01)00049-2
[18] W. Stuerzlinger, et al., User interface facades: towards fully adaptable user interfaces, in Proc. 19th Annu. ACM Symp. on User Interface Software Technology, Montreux, Switzerland, (2006) 309-318. DOI: 10.1145/1166253.116630
[19] C. Stephanidis, User interfaces for all: concepts, methods, and tools. Mahwah, NJ, USA: Lawrence Erlbaum Associates Inc., (2001).
[20] C. Stephanidis, User interfaces for all: concepts, methods, and tools. Mahwah, NJ, USA: Lawrence Erlbaum Associates Inc., (2001).
[21] M. Miller, Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online. Que, (2009).
[22] I. Foster, et al., Cloud Computing and Grid Computing 360-Degree Compared, Proc. Grid Computing Environments Workshop (GCE '08), (2008)1-10.
[23] R. Buyya, et al., Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility, Future Generation Computer Systems, 25(6) (2009) 599-616.