A Reliable Authentication Protocol for Peer to Peer Based Applications

Ramesh Kumar
Rajiv Gandhi Technical University, Bhopal, Madhya Pradesh
Email: errameshkumar1972@gmail.com

ABSTRACT

The importance of data communication has taken a sharp increment due to digitalization. The security of data communication is a key issue and authentication mechanisms are the backbone of secure and reliable data communication. Researchers are trying to find lightweight authentication algorithms which can be used in variety of applications and useful for mobile phones as well. In this paper we propose an innovative mechanism of certificate generation for authentication. A user can run the entire mechanism without any external help. The certificate can be verified and stored by the receiver for further cryptographic usage. We also provide security analysis and advantages of the proposed mechanism briefly.

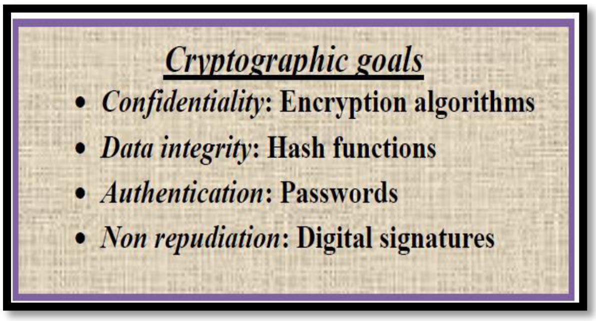
Keywords - **Authentication, Data Communication, Digital Signature, Public-Key Cryptography (PKC)**

Date of Submission: Mar 22, 2021 Date of Acceptance: Apr 01, 2021

I. INTRODUCTION

Wireless communication is vulnerable to various security attacks. Wireless communication channels are always soft target for intruders because security measures are weak compared to wired networks. Cryptography has the responsibility to provide secure data communication over insecure wireless communication channels. So we briefly describe associated cryptographic goals (as shown in figure 1) for better understanding **[1-4]**.

- Confidentiality: It means to safeguard the information from intruders in such a way that only intended receiver can access the information or message content.
- Data integrity: It means any unwanted modification in the data has to be restricted. Data integrity makes sure that no alteration in the message content is done.
- Authentication: It means participating entities mutually recognize each other in such a way that data communication is done between legitimate entities. It is very important in the communication of financial transactions, legal and confidential documents etc.
- Non-repudiation: It is an assurance that a participating entity cannot deny commitments made during the communication **[5]**. Authentication is the prerequisite for non repudiation.



Cryptographic goals

- *Confidentiality*: Encryption algorithms
- *Data integrity*: Hash functions
- *Authentication*: Passwords
- *Non repudiation*: Digital signatures

Fig.1: Showing goals of cryptography

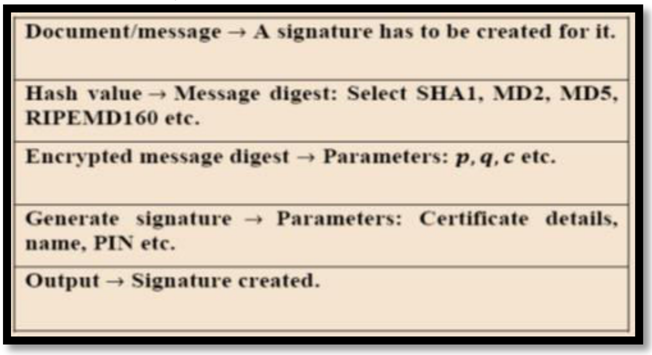
Here our candidate for consideration is authentication because it is very important that entities must recognize each other in an insecure communication medium **[6-8]**. Authentication makes sure the data communication is going on between intended parties. Now days, researchers are trying to find different authentication methods for various applications **[9-11]**. Authentication can be done by variety of methods. Thumb impression, retina detection and PIN (Personal Identification Number) verification or any challenge-response mechanism can be seen as examples of authentication methods **[12]**. Digital signatures are used for authentication. They use public key cryptography for that. Formally, a digital signature is a data string produced from a message with an algorithm called signature generation algorithm. The sender is called as signer and the receiver is known as verifier. The signature certificate can be stored by the receiver and it is a proof that an authentic sender has sent the data **[13]**. The signature algorithm can be any public key algorithm like RSA, DSA (Digital Signature Algorithm), Elgamal signature scheme etc and many variants are also there like ECDSA (Elliptic Curve DSA), Merkle one-time signature scheme etc **[14]**. Here we want to discuss RSA algorithm in brief **[2][15]**. Sender selects two large primes p and q. Here large means good enough for security. Sender computes $n = pq$ and $\Phi = (p-1)(q-1)$. Sender picks a random integer $e,\ 1 < e < \Phi$, such that $\gcd(e, \Phi) = 1$. Then another parameter d can be selected by extended Euclidean algorithm, $1 < d < \Phi$ such that $ed \equiv 1(mod\, \Phi)$. The public key of the sender is (n, e) and private key is d. Suppose receiver wants to send message m to sender. The cipher text can be computed as $c = m^e mod\, n$. Now only sender can compute the decryption because only he has the private key d. The decryption is done by the sender by calculating $m = c^d mod\, n$. The rest of this paper is organized as follows: in section 2 we discuss the proposed method using RSA. In section 3 security analysis is given. In section 4 we discuss the advantages in brief. Conclusion and future scope is given in section 5.

II. PROPOSED METHOD

Our proposed method is a convenient four step sequential process to generate signature certificate (as shown in figure 2). The ingredients are message, hash function, public key algorithm which is RSA here and associated parameters like prime number generation, calculation of keys etc. It also requires some certificate details like password (or PIN) and name of the signer.

Now suppose sender want to transmit a message signature to receiver over insecure channel. The message is saved in a text file saved as message.txt. As a first step we select the hash function and calculate the hash value of the message. Hash functions are sometimes also known as compression function. The hash function produces fixed length output known as message digest or simply digest. An ideal hash function has certain properties like collision resistance, pre-image resistance etc **[15-16]**. We select SHA-1 as our hash function but it can be MD-2, MD-5, SHA or RIPEMD-160 depending on user's wish **[17]**.

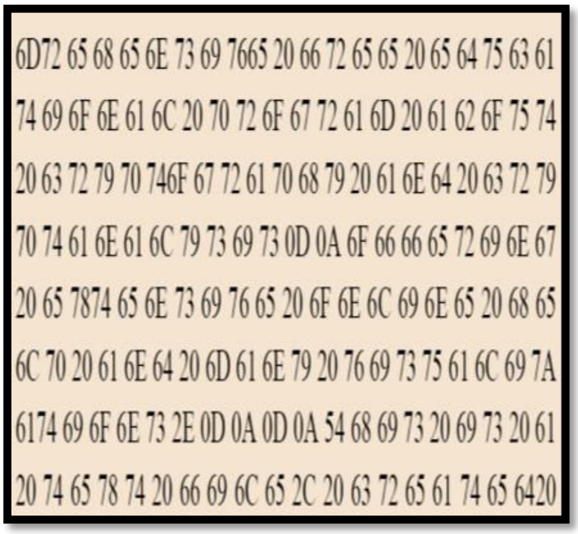
As a second step we have to generate prime numbers for key generation and encryption of the hash value. We select the prime range 2^{155} to 2^{158}. User can change this range also. The primality test selected is Miller-Rabin but it can be Fermat or Solovay-Strassen test etc. Now prime numbers and public and private keys are calculated. It is to mention that $p = 222318126392308625219246827349919612725938064443$ and the value of $q = 155906137099484403201025017960906814389123818737$ which are the required prime numbers with 320 bits length **[18]**. Now we calculate the encrypted value of the hash digest using above parameters which means encryption is done on the hash value of the message and it adds another layer of security. As a third step, we need to fill the required certificate and PSE (Personal Security Environment) details. These parameters are important for certificate generation **[19]**. We need to fill name, first name, key identifier (optional) and PIN here. The PIN works as a password and it is user dependent. Users are supposed to verify the PIN to make sure that the password is filled correctly **[20]**.



Document/message → A signature has to be created for it.
Hash value → Message digest: Select SHA1, MD2, MD5, RIPEMD160 etc.
Encrypted message digest → Parameters: p, q, c etc.
Generate signature → Parameters: Certificate details, name, PIN etc.
Output → Signature created.

Fig.2: Showing the procedure with corresponding parameters.

In the last step we have to assemble everything and the final certificate is prepared within seconds which can be store as a separate file used for authentication (as shown in figure 3).



```
6D72 65 68 65 6E 73 69 7665 20 66 72 65 65 20 65 64 75 63 61
74 69 6F 6E 61 6C 20 70 72 6F 67 72 61 6D 20 61 62 6F 75 74
20 63 72 79 70 746F 67 72 61 70 68 79 20 61 6E 64 20 63 72 79
70 74 61 6E 61 6C 79 73 69 73 0D 0A 6F 66 66 65 72 69 6E 67
20 65 7874 65 6E 73 69 76 65 20 6F 6E 6C 69 6E 65 20 68 65
6C 70 20 61 6E 64 20 6D 61 6E 79 20 76 69 73 75 61 6C 69 7A
6174 69 6F 6E 73 2E 0D 0A 0D 0A 54 68 69 73 20 69 73 20 61
20 74 65 78 74 20 66 69 6C 65 2C 20 63 72 65 61 74 65 6420
```

Fig.3: Showing one section of eight lines of the generated signature certificate of the message.

III. SECURITY ANALYSIS

Here we discuss the related security analysis briefly.

- **Password protection**: The signature is password protected means the password is required to retrieve the message or verify the signature. The sender can change the password at any point of time. This increases the flexibility and prevents password based attacks as the same signature can be send to various entities by using different passwords **[21-22]**.
- **Prime factorization security**: Our assumption is that the signature is secure as long as prime factorization problem is hard. Sender can increase the toughness by increasing the range of prime numbers **[23]**.
- **Hash function security**: We apply RSA on the hash value of the message. This enables another layer of security as hash produces one way message digest value and an ideal hash function is a one way compression function.
- **Security of the key**: Kerckhoff's principle says that a cryptographic system has to be secure even if everything about the system, except the key, is publicly known to everyone **[24]**. In our case, if everything is known to adversary except the key then also it is computationally infeasible to retrieve the information because prime factorization problem is hard.
- **Floating frequency**: The high randomness level is always assumed well in cryptography because high randomness enables the given text more difficult to predict **[25]**.

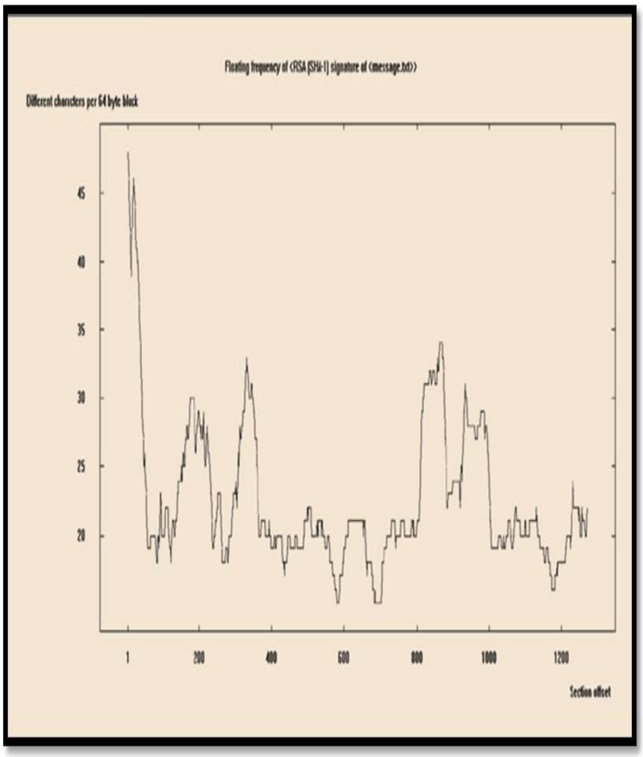


Fig.4: Showing floating frequency curve for the signature of the message.

In the above figure 4 we have shown floating frequency curve for the signature of message.txt file. It is very clear that numbers of different characters are different in every block and the distribution is neither periodic nor symmetric. It is totally random and as a result it becomes next to impossible for the intruder to find any clue.

IV. ADVANTAGES

There are many advantages of the proposed method and we discuss the few of them briefly.

- **Password and password length can be changed any time**: Sender can change the password if he thinks that the password is leaked or the existing password length can be increased in order to enhance security keeping other parameters as constant.
- **Prime number range and associated test can be change any time**: Any change or increment in the selected prime number's range enhances the security level. Sender can select other algorithms for primality testing which increases randomness and it is good for security **[26-27]**.
- **Peer to Peer (P2P) based wireless applications:** The proposed method is very suitable for P2P-wireless communication. Wireless communication channels are more insecure than wired mediums so additional security is desired in wireless P2P communications. In the proposed method, the signature file is generated and can be transmitted to receiver which enhances the level of security and trust between transmitter and receiver **[28-29]**. The scenario remains useful in variety of applications including ad-hoc connections, chatting applications or in the transmission of sensitive information etc.
- **User can select hash output of his choice**: The message digest value is encrypted using public key algorithm which is RSA in our case. Sender can change the hash function like one can use MD5 or RIPEMD-160 in place of MD2 keeping other parameters same which makes prediction very difficult for intruders **[30-32]**.
- **Broadcasting of a message is possible**: Sender can transmit a message to more than one user. Sender need to change only one parameter like password or values of primes etc keeping other parameters as fixed **[33]**.
- **Anybody can use that**: The proposed method is easily understandable for even those who are not familiar with cryptography or do not belong to technical background. Anybody can utilize the method by simply following the given step by step procedure. The method can be applied to various other applications like Electronic Health Record (EHR) systems or data storage etc **[34-35]**.
- **Data compression:** Many data compression techniques can be applied on the output signature file **[36]**. It will enhance the long term storage capacity of the system which saves the generated signature files and computational resources will be saved. It will have a positive impact on software implementation.
- **Sequential process**: The proposed method is a sequential process that means every intermediate outcome is the input for next step. This makes it very suitable for GUI (Graphical User Interface) based software implementations because users need to provide inputs sequentially and the signature file (or the compressed signature file) will be created.
- **Computational overheads are very low**: The proposed method is a convenient sequential process and additional memory, high performance processors etc are not required. The size of the signature file can also be reduced so it can be said that computational overheads are very low **[37-38]**.
- **Software implementation is possible**: Since the proposed method is a very effective method of generating required digital signatures keeping computational overheads minimum, the software implementation of the proposed system is also possible **[39-40]**. One needs to put the message and the hash algorithm (selected) and after that, the required parameters can be selected and the corresponding signature will be created as an output. It will make the overall usage very effective. As discussed above (in data compression), inbuilt data compression methods can be applied on generated signatures in the software implementation **[41-42]**.

V. CONCLUSION & FUTURE SCOPE

We have proposed a convenient method of creating digital signatures for authentication. It will enhance the level of trust among entities communicating over insecure wireless communication channel. They are so useful because a non technical person can also generate the same. There is nothing to purchase and no dependency on third party. The certificate can be stored as it requires space in KB and binds entities in such a way so that non repudiation as a cryptographic goal is also achieved. The future scope is very vast as one can incorporate other signature schemes like Elgamal and the hash function varieties can also be extended and different combinations can be selected. Time stamp concept can be added to create session oriented signature certificates. The proposed method and concept is very useful for transmitting sensitive information, financial transactions or usage in military services.

REFERENCES

[1]. A.J.Menezes, P.C.V.Oorschot, S.A.Vanstone, Handbook of applied cryptography, fifth edition, CRC press Inc., USA, ISBN 9780849385230, 2001.

[2]. W.Stallings, Cryptography and network security, principles and practices, fourth edition, Prentice Hall, ISBN-13: 978-0131873162, ISBN-10: 0131873164, 2005.

[3]. V. Shukla, A. Chaturvedi, N. Srivastava, Nanotechnology and cryptographic protocols: issues and possible solutions, Nanomaterials and energy, volume 8, issue 1, 2019, 1-6, DOI: 10.1680/jnaen.18.00006

[4]. V. Shukla, A. Chaturvedi, N. Srivastava, A secure stop and wait communication protocol for disturbed networks, Wireless personal communications, volume 110, 861-872, 2019, DOI: https://doi.org/10.1007/s11277-019-06760-w

[5]. W. Wu, J. Zhou, Y. Xiang, L. Xu, How to achieve non-repudiation of origin with privacy protection in cloud computing, Journal of computer and system sciences, volume 79, issue 8, 2013, 1200-1213, DOI: https://doi.org/10.1016/j.jcss.2013.03.001

[6]. S. Vaudenay, Secure communications over insecure channels based on short authenticated strings, Advances in cryptology (part of the lecture notes in computer science book series (LNCS, volume 3621)), 2005, 309-326, DOI: https://doi.org/10.1007/11535218_19

[7]. J.Moon, Y.Lee, J.Kim, D.Won, Improving an anonymous and provably secure authentication protocol for a mobile user, Security and communication networks, volume 2017, 2017, 1-13, DOI: https://doi.org/10.1155/2017/1378128.

[8]. V. Shukla, N. Srivastava , A. Chaturvedi, A bit commitment signcryption protocol for wireless transport layer security (wtls), IEEE international conference on electrical computer and electronics engineering, 2016, 83-86, DOI: 10.1109/UPCON.2016.7894629

[9]. M. Trnka, T. Cerny, N. Stickney, Survey of authentication and authorization for the internet of things, Security and communication networks, volume 2018, 2018, 1-17, DOI: https://doi.org/10.1155/2018/4351603.

[10]. M. Alhaidary, S.K.M.D. M. Rahman, M. Zakariah, M.S. Hossain, A. Alamri, M.D. S.M. Haque, B. B. Gupta, Vulnerability analysis for the authentication protocols in trusted computing platforms and a proposed enhancement of the OffPAD Protocol, IEEE access, volume 6, 2018, 6071 -6081, DOI: 10.1109/ACCESS.2017.2789301.

[11]. A. Chaturvedi, V. Shukla, Tripartite key agreement protocol using conjugacy problem in braid groups, International journal of computer applications, volume 31, number 1, 1-4, 2011, DOI: 10.5120/3786-5201

[12]. M.A.Alia, A.A.Tamimi, Q.N.A. Al-Allaf, Cryptography based authentication methods, Proceedings of the world congress on engineering and computer science, 2014, 199-204, available at http://www.iaeng.org/publication/WCECS2014/WCECS2014_pp199-204.pdf.

[13]. B.Poettering, D.Stebila, Double authentication preventing signatures, European symposium on research in computer security (part of the lecture notes in computer science book series, (LNCS, volume 8712)), 2014, 436-453, DOI: https://doi.org/10.1007/978-3-319-11203-9_25 .

[14]. C.Paar, J.Pelzl, Understanding cryptography-a textbook for students and practitioners, ISBN 978-3-642-04101-3, 2010.

[15]. B.Schneier, Applied cryptography, protocols, algorithms and source code in C, second edition, Wiley, ISBN 978-1-119-09672-6, 1995.

[16]. D.R.Stinson, Cryptography-theory and practice, third edition, Chapman & Hall, CRC, ISBN 978-1-58488-508-5, 2006.

[17]. V. Shukla, A. Chaturvedi, N. Srivastava, Authentication aspects of dynamic routing protocols: associated problem & proposed solution, International journal of recent technology and engineering, volume 8, issue 2, 2019, 412-419, DOI: 10.35940/ijrte.B1503.078219

[18]. Cryptool portal, Cryptography for everybody, available at https://www.cryptool.org/en/download-ct1-en/215.

[19]. V. Shukla, A. Mishra, S. Agarwal, A new one time password generation method for financial transactions with randomness analysis, Innovations in electrical and electronic engineering (part of the lecture notes in electrical engineering book series (LNEE, volume 661)), 2020, 713-720, DOI: https://doi.org/10.1007/978-981-15-4692-1_54

[20]. M. K. Lee, J. B. Kim, M. K. Franklin, Enhancing the security of personal identification numbers with three dimensional displays, Mobile information systems, volume 2016, article ID 8019830, 2016, 1-9, DOI: https://doi.org/10.1155/2016/8019830

[21]. P.Wang, Y.Kim, V.Kher, T.Kwon, Strengthening password-based authentication protocols against online dictionary attacks, International conference on applied cryptography and network security (part of the lecture notes in computer science book series, (volume 3531)), 2005, 17-32, DOI: https://doi.org/10.1007/11496137_2.

[22]. S.Chakrabarti, M.Singhal, Password-based authentication: preventing dictionary attacks, Computer (IEEE computer society), volume 40, issue 6, 2007, 68-74, DOI: 10.1109/MC.2007.216.

[23]. S.J.Abond, M.A.Al-Fayoumi, M.Al-Fayoumi, H.S.Jabbar, An efficient RSA public key encryption scheme, Fifth international conference on information technology: new generations, 2008, 127-130, DOI: 10.1109/ITNG.2008.199.

[24]. Crypto-IT, Kerckhoff's principle, available at http://www.crypto-it.net/eng/theory/kerckhoffs.html.

[25]. H.C-Gibbs, W.Mu, D.Boneh, B.Ford, Ensuring high-quality randomness in cryptographic key generation, ACM SIGSAC conference on computer & communications security, 2013, 685-696, DOI: 10.1145/2508859.2516680.

[26]. A.H.Lone, A.Khalique, Generalized RSA using 2k prime numbers with secure key generation, Security and communication networks, volume 9, issue 17, 2016, 4443-4450, DOI: https://doi.org/10.1002/sec.1619.

[27]. K. Marton, A. Suciu, I. Ignat, Randomness in digital cryptography: a survey, Romanian journal of information science and technology, volume 13, number 3, 2010, 219-240, available at: http://romjist.ro/content/pdf/kmarton.pdf

[28]. A.Chaturvedi, N.Srivastava, V.Shukla, S.P.Tripathi, M.K.Misra, A secure zero knowledge authentication protocol for wireless (mobile) ad-hoc networks, International journal of computer applications, volume 128, number 2, 2015, 36-39, DOI: 10.5120/ijca2015906437

[29]. A.Chaturvedi, N.Srivastava, V.Shukla, A secure wireless communication protocol using Diffie-Hellman key exchange, International journal of computer applications, volume 126, number 5, 2015, 35-38, DOI: 10.5120/ijca2015906060

[30]. V. Shukla, A. Chaturvedi, N. Srivastava, A new one time password mechanism for client-server applications, Journal of discrete mathematical sciences and cryptography, volume 22, issue 8, 2019, 1393-1406, DOI: 10.1080/09720529.2019.1692447

[31]. T. Lakshmanan, M. Muthusamy, A novel secure hash algorithm for public key digital signature schemes, The international Arab journal of information technology, volume 9, number 3, 2012, 262-267, available at: http://iajit.org/PDF/vol.9,no.3/2728-10.pdf

[32]. W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, G. Wang, Digital signature scheme for information non-repudiation in blockchain: a state of the art review, Eurasip journal on wireless communications and networking, volume 2020, article number 56, 2020, 1-15, DOI: https://doi.org/10.1186/s13638-020-01665-w

[33]. R.F.Schaefer, A.Khisti, H.V.Poor, Secure broadcasting using independent secret keys, IEEE transactions on communications, volume 66, issue 2, 2017, 644-661, DOI: 10.1109/TCOMM.2017.2764892.

[34]. V.Shukla, A.Chaturvedi, N.Srivastava, A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography, Communications on applied electronics, volume 3, number 3, 2015, 16-21, DOI: 10.5120/cae2015651903

[35]. M.K. Misra, A. Chaturvedi, S.P. Tripathi, V. Shukla, A unique key sharing protocol among three users using non-commutative group for electronic health record system, Journal of discrete mathematical sciences and cryptography, volume 22, issue 8, 2019, 1435–1451, DOI: 10.1080/09720529.2019.1692450

[36]. V. Shukla, A.Mishra, A new sequential coding method for secure data communication, IEEE international conference on computing, power and communication technologies, 2020, 529-533, DOI: 10.1109/GUCON48875.2020.9231252

[37]. M. A. Mughal, X. Luo, A. Ullah, S. Ullah, Z. Mahmood, A light weight digital signature based security scheme for human-centered internet of things, IEEE access, volume 6, 2018, 31630-31643, DOI: 10.1109/ACCESS.2018.2844406

[38]. O. Tayan, M. N. Kabir, Y. M. Alginahi, A hybrid digital-signature and zero-watermarking approach for authentication and protection of sensitive electronic documents, The scientific world journal, volume 2014, article ID 514652, 2014, 1-14, DOI: https://doi.org/10.1155/2014/514652

[39]. U. Somani, K. Lakhani, M. Mundra, Implementing digital signature with RSA encryption algorithm to enhance the data security of cloud in cloud computing, First international conference on parallel, distributed and grid computing, 2010, 211-216, DOI: 10.1109/PDGC.2010.5679895

[40]. P. Subpratatsavee, P. Kuacharoen, An implementation of a paper based authentication using HC2D barcode and digital signature, Computer information systems and industrial management (part of the lecture notes in computer science book series (LNCS, volume 8838)), 2015, 592-601, DOI: https://doi.org/10.1007/978-3-662-45237-0_54

[41]. A. Dhivakar, D. Ravichandran, V. Dakha, Security and data compression in cloud computing using blobseer technique, Special conference issue, International journal of advanced networking and applications, 2015, 201-203, available at https://www.ijana.in/Special%20Issue/C36.pdf

[42]. M. Singh, V. Chaudhary, Loseless image compression having compression ratio higher than JPEG, Special conference issue, International journal of advanced networking and applications, 2015,135-139, available at https://www.ijana.in/Special%20Issue/C23.pdf