

Literature Survey for Design and Analysis of a Multi-Level Algorithmic Technique for Encryption and Decryption

Mr. Hirdesh Sharma^{1&2}, Dr. Gaurav Aggarwal³ and Dr. Sachin Kumar⁴

¹Assistant Professor, CSE Department, Lloyd Institute of Engg. & Tech., Greater Noida, India

²Research Scholar, Jagannath University, Bahadurgarh (Jhajjar), Haryana, India, ORCID iD: 0000-0002-1278-4135
EmailID:- hirdesharma@gmail.com

³Professor & Dean, Dept. of CSE, Jagannath University, Bahadurgarh (Jhajjar), Haryana, India,
ORCID iD: 0000-0002-6836-9352
EmailId:- gauravaggarw@gmail.com

⁴Associate Professor, Dept. of MCA, Noida Institute of Engg. & Tech., Greater Noida, India,
ORCID iD: 0000-0002-1136-8009
EmailId:- sachinks.78@gmail.com

Abstract—Cryptography is the discipline, which epitomizes standards, means, and techniques for the change of information to conceal its data content, forestall its undetected alteration as well as forestall its unapproved use. In cryptography, encryption is the most well-known approach to evolving information (insinuated as plaintext) using a computation (called figure) to make it jumbled to anyone beside those having phenomenal data, commonly implied as a key and unscrambling is the technique engaged with changing (suggested as code text) using an estimation into its interesting design (called plaintext). In spite of the fact that encryption safeguards the information, beneficiaries should have the right unscrambling or interpreting apparatuses to get to the first subtleties. Information classification becomes similarly significant alongside innovative headway. Encryption and Decryption methods are the fundamental part of data security. Albeit in the current framework, a multi-faceted plan was working however the current plan was not giving the security to little information.

Index Terms— Encryption, Decryption, Cryptography, private-key, public-key, RSA, AES, Multilevel Encryption.

I. INTRODUCTION

With the quick improvement of Internet innovation, the Internet has become famous for an enormous scope. While concentrating on the way of behaving of clients on various person to person communication destinations, there is a test: the failure to productively scramble data related with clients across informal communities [2]. A client has individual social records on various informal organizations and the way of behaving on these interpersonal organizations might be unique. It is difficult to successfully distinguish whether the records are from a similar client. Consequently, the client related data across informal organizations can't be additionally scrambled and can undoubtedly be uncovered, which carries burden and mischief to the informal community

clients. The recognizable proof and encryption of the client related data across informal communities is the way to taking care of these issues. Lately, this utilization of the tumultuous standard has gotten increasingly more consideration and numerous researchers are concentrating on it and applying it to picture encryption, voice encryption and numerous different perspectives.

The staggered encryption calculation for client related data across interpersonal organizations gets the client related data through the cross-informal community client affiliation model and afterward utilizes brain network-based staggered turbulent encryption calculation in view of the affiliation data to acknowledge staggered encryption of client related data across informal organizations. With the fast improvement of Internet innovation, the Internet has become famous for a huge scope. While concentrating on the way of behaving of clients on various interpersonal interaction locales, there is a test: the powerlessness to productively scramble data related with clients across informal communities [2]. A client has individual social records on various informal organizations and the way of behaving on these interpersonal organizations might be unique. It is difficult to really distinguish whether the records are from a similar client. Consequently the client related data across interpersonal organizations can't be additionally scrambled and can without much of a stretch be revealed, which carries bother and mischief to the informal community clients. The recognizable proof and encryption of the client related data across informal communities is the way to tackling these issues. Customary encryption calculations, for example, SMM encryption calculation, RSA encryption calculation and Skipjack encryption calculation have the impediments of slow speed, high constraint and unfortunate homomorphism. To address the inadequacies in the above calculations, this paper proposes a staggered encryption calculation.

Cryptography is a strategy for encoding and decoding text by impeding secret information in an unlimited manner to the gatecrasher [3], [4], [5]. Different cryptography systems have been made, for example, the replacement calculation, which relies upon superseding one letter with another, and can be all around arranged by the kind of encryption key into regular and digressed encipher [6][7]. The general advancement of the encipher estimation. For most extreme insurance and strong security with high limit, new techniques for concealing information were recommended by the specialists in view of DNA [8], [9].

TABLE I. APPLICATION AREAS OF CRYPTOGRAPHY

Application Issue	Symmetric Encryption	Asymmetric Encryption
web based business		✓
Simple of key administration		✓
Signature non-renouncement		✓
Usefulness		✓
Significant level security	✓	✓
Quick, productive calculation handling	✓	
Key size	✓	
Challenge-reaction	✓	
Single-client security	✓	
Plate encryption	✓	
Shared confirmation	✓	
Reasonableness	✓	

II. OBJECTIVE OF THE REVIEW

The exploration work zeroed in on fostering another Encryption conspire in light of symmetric guideline. The course of the proposed calculation has seven rounds. The cycle start from Round 1. each round has its own portrayal and claims working standards means to say on which (bit, character, line...) round will work. The proposed calculation are underneath with stream diagram and its means.

- Round 1 on bits.
- Round 2 on character.
- Round 3 on paragraph.
- Round 4 on lines.
- Round 5 on words.
- Round 6 on character.
- Round 7 on bits.

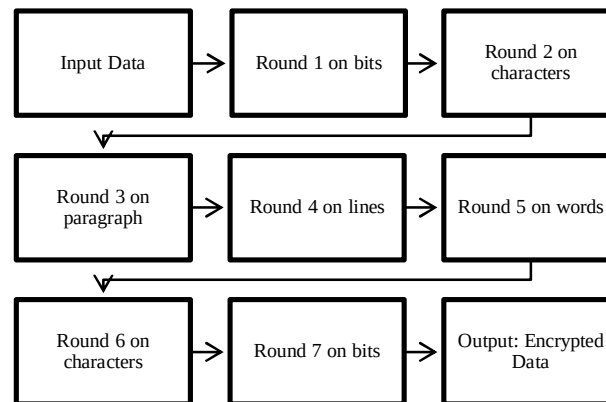


Figure 2. Flowchart of proposed algorithm

III. RELATED WORK

In the writing overview, I have gone through a few papers and got heaps of help and backing from these papers. This one is the base paper from which I got the plan to additionally further develop it to some other level that is by giving greater security to the information. For this I have gone through various papers to aggregate the thoughts by the assistance of which I can move further. The subtleties of various papers from which I took help are depicted underneath.

Consolidating the methodology of RSA and AES is being utilized for both symmetric and hilter kilter encryption is certainly not another methodology. Security is generally a superb issue for buy scientists and experimenters. There are a few executions done by scientists involving cross breed approach as well as staggered cryptography approach. Security in 2016 incorporates different stages to be applied on the information in particular RSA, DES, half breed calculation. The keys that were utilized in the last advance were string modulus, private, public and whole number key [11].

Another methodology was consolidating a symmetric and public key strategy in 2012 hair where utilized for encryption was utilized for key trade. It likewise comprises of pseudo arbitrary number age unit for key age process and GCD figuring unit in the RSA calculation [11].

Staggered encryption is found in 3DS, AES gives cryptographic affirmation of message honesty. Multiphase or staggered encryption procedure utilizes plain instant message to scramble in single or multi level(k times) encryption with the equivalent or different keys. Brings about better security to averall system.[12]

This paper presents a show appraisal of picked symmetric encryption estimations. The picked computations are AES [13], DES, 3-DES, RC6, Blowfish and RC2. A couple centers can be shut from the propagation results. First; there is no huge differentiation when the results are shown either in hexadecimal base encoding or in base 64 encoding. Additionally; by virtue of changing bundle size, it was contemplated that Blowfish has favored execution over other ordinary encryption computations used, followed by RC6. Third; because of changing data type, for instance, picture as opposed to message, it was seen that RC2, RC6 and Blowfish has obstacle

throughout various computations with respect to time use. Moreover, we see that 3DES really has low execution stood out from estimation DES.

In [17] an examination of security exertion level has been proposed for a web programming language to look at four Web programs. This study consider of assessing the presentations of encryption process at the composing PC programs language's substance with the Web programs. This is followed by guiding tests reenactment to get the best encryption computation versus Web program. As of now to learn about Cryptographic File System I went through the paper [18] A Cryptographic File System for UNIX by Matt Blaze. It communicates: yet cryptographic methodologies are expecting an unyieldingly critical part in present day handling structure security, client level gadgets for scrambling record data are off-kilter and experience the evil impacts of different intrinsic shortcomings that. The cryptographer File System (CFS) drives encipher organizations in to the report structure itself.

CFS gives a straightforward component to safeguard information written to plates and shipped off arranged record servers. In spite of the fact that involvement in CFS and with client communication is as yet restricted to the exploration climate, execution on present day workstations gives off an impression of being inside a reach that permits its standard use, regardless of the undeniable inadequacies of a client level NFS-server-based execution. The client document framework interface gives off an impression of being the ideal locations to safeguard record information. Think about the other options. Scrambling at the application layer (the customary methodology) is awkward. Scrambling the organization in circulated document frameworks, while valuable overall against network-based assault, doesn't safeguard the genuine media and along these lines actually requires trust in the server not to uncover record information.

Presently to find out about how the message is Encrypted and Decrypted I gone through a few papers however the one which I viewed as reasonable for my examination work is the one given by Arpad Incze that is [19] The Basics of Text Encryption and Decryption. That's what he says: People mean various things when they talk about cryptography. Youngsters play with toy codes and mystery dialects. Nonetheless, these have essentially nothing to do with genuine security and solid encryption. Solid encryption is the sort of encryption that can be utilized to safeguard data of genuine worth against coordinated crooks, worldwide partnerships, and significant legislatures. Solid encryption used to be just military business; nonetheless, in the data society it has become one of the focal devices for keeping up with protection and secrecy.

In a paper [22] on A Current Perspective on Encryption Algorithms by Dr Lawrie Brown he present a perspective on the current status of play in the field of encryption estimations, explicitly on private key square codes which are by and large used for mass data and association encryption. With the new call by the US NIST for entries to characterize an Advanced Encryption Standard to ultimately supplant the DES, there has been expanded action in this field. I will momentarily depict a portion of the known competitors, including the neighborhood LOKI97 calculation.

With developing attention to, and worries about, PC and interchanges security, there is expanding fuse of cryptographic calculations into such frameworks. This paper presents a concise outline of the present status of cryptographic calculations, with an accentuation on private key square codes. It is incited somewhat by the US NIST (National Institute of Standards and Technology) call for passages of contender computations for an Advanced Encryption Standard, due in the not so distant future.

In a paper [23] on Efficient and High-Performance Parallel Hardware Architectures for the AES-GCM by Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh they get further developed building blocks for the AES-GCM to propose compelling and unrivaled execution structures. For the AES, through reasoning entrance minimizations for the inversion in GF [24], the locale of the S-boxes have been reduced. They have moreover evaluated and pondered the introduction of different S-boxes using an ASIC 65-nm CMOS advancement. Besides, through exhaustive searches for the data plans, they have performed propagation based power derivations for different S-boxes to show up at more precise results stood out from the quantifiable methods. They have in like manner proposed predominant execution and powerful plans for the GCM. For the context oriented examination of $q^{1/4}$ 8 equivalent plans in GHASHH, they have played out a gear complexity decline technique for the hash sub key exponentiations, having their arranging complexities immaculate.

This paper expresses that guidance set augmentations for further developing programming executions of symmetric-key calculations have been proposed. Existing writing regarding the matter of improving the exhibition of symmetric-key calculations was talked about, trailed by itemized portrayals of the designated processor and the designated cryptographic calculations. Depictions of the custom guidelines were given alongside the utilitarian units that carry out the basic legitimate and number-crunching tasks. The outcomes show that the proposed directions affect the program code size for the designated calculations as a whole, getting the amount of code bytes by up to a piece of 31.2. The implementation time for all estimations was in like manner

better, with showed open up by components of up to 32.8. The bearing set augmentations required just a 63% expansion in the thinking use of the LEON2 processor on the picked FPGA [25] gadget while diminishing the best clock rehash by around 10%. All of the assigned computations demonstrated a development in T/An extent, extending by a variable of up to 25.81. It was likewise exhibited that segment situated executions of AES are better than column arranged executions of AES for all assessment measurements while utilizing the proposed guidance set augmentations. At last, it was shown that the output for triple DES, IDEA, and AES were roughly a comparable when accelerated through direction set increases, taking into consideration calculation nimbleness that is straightforward to the client as one calculation might be effectively supplanted by one more calculation with insignificant execution corruption.

In a paper [26] on Research on power data encryption calculation in view of composite tumultuous framework in wavelet change area by Li Xiaoming and Yun Zhao. They proposed an information encryption calculation in view of composite disorder and wavelet change hypothesis. The strategy built the composite turbulent framework utilizing two one-layered tumultuous planning, which has great cryptography qualities, and completed time-recurrence change on plaintext in light of 2D wavelet change [27] hypothesis, while the wavelet coefficients of plaintext are mixed with composite tempestuous gathering in wavelet space.

It was displayed in [30] that the security of WAMS [31] faces extraordinary test while fulfilling energy requirements. The focal issue applying security estimations to WAMS [31] is to change the energy usage and the energy supply to the systems. This paper proposed a variety of novel code advancement technique to increment energy utilization effectiveness of various calculations. This paper additionally exhibits that it is incredibly useful to choose and design security calculations in energy-obliged frameworks to work on the security of the framework.

IV. RESEARCH GAP

A perplexing estimation [32] is suggest to encode & unscramble a unencrypted text. The estimation gives the four level of security. The 4 levels for the arrangement of the level of safety expected to encode the communication are:

- Short quantity dependability
- Medium quantity dependability
- Undeniable quantity dependability
- Fundamentally undeniable quantity dependability

In the four degrees of safety, the initial three levels depend on chunk figure & the 4th level depends on torrent figure. Level [32-33] is expected as strategic security and fourth level is planned as essential security. Existing system is good to implement if data is large. If data is small, then no good security can be avail. This was the motivation for my idea of developing a more secure multi-level algorithm of 7 (seven) rounds for small data as well as large data.

V. ANALYSIS OF MULTI-LEVEL ALGORITHMIC TECHNIQUE FOR ENCRYPTION AND DECRYPTION

A. Benefits of Design and Analysis of a Multi-level Algorithmic Technique for Encryption and Decryption

1. A multi-layer data encryption and interpreting plan that uses the investigation of steganography and cryptography is proposed and made.
2. The heads of GA, for instance, assurance, mixture and change are used on at different levels of encoding and unraveling to collect a strong and strong data encryption and unscrambling plan.
3. The accommodating components of RNS, for instance, developments and parallelism alongside a merging measure to embed text inside pictures are similarly used to extra work on the security, force and the throughput of the arrangement.
4. We probably displayed the credibility of the arrangement in getting data on the way an open channel, for instance the Internet.

B. Advantages of Design and Analysis of a Multi-level Algorithmic Technique for Encryption and Decryption

1. The fundamental job of encryption is to shield the protection of cutting edge data set aside on PC systems or sent over the web or some other PC association.
2. In development to security, the gathering of encryption still up in the air by the need to meet consistence rules.

3. A number of affiliations & recognized bodies either recommend or require sensitive data to be mixed to hinder unapproved untouchables or peril performers from getting to the data.
4. For model, the Payment Card Industry Data Security Standard (PCI DSS) anticipates that vendors should encode clients' portion card data when it is both taken care of exceptionally still and sent across open associations.

C. Disadvantages of Design and Analysis of a Multi-level Algorithmic Technique for Encryption and Decryption

1. While encryption is intended to hold unapproved substances back from having the option to comprehend the information they have gained, in certain circumstances, encryption can hold the information's proprietor back from having the option to get to the information also.
2. Key organization is presumably the best trial of building an endeavor encryption technique because the keys to interpret the code text should dwell some spot in the environment, and aggressors routinely have an extremely brilliant considered where to look.
3. There are a ton of endorsed strategies for encryption key organization. Accepting a critical calamity should strike, the most well-known approach to recuperating the keys and adding them to another support server could grow the time that it takes in any case the recovery action.
4. Having a key organization system set up isn't adequate. Chiefs ought to consider a sweeping arrangement for protecting the key organization structure. Consistently, this infers backing it up autonomously from the wide range of various things and taking care of those fortifications with the end goal that simplifies it to recuperate the keys in the event of a tremendous degree catastrophe.

VI. IDEAS TO IMPLEMENT RESEARCH ACTIVITIES ACCORDING TO MULTI-LEVEL ALGORITHMIC TECHNIQUE FOR ENCRYPTION AND DECRYPTION

The craving of mystery has driven individuals to involve information cryptography for successful and secure information transmission by applying progressed techniques for cryptography. Simultaneously rival organizations have contributed a ton of assets to break into these encryptions, take insider facts and gain a high ground. This is to give the clients adaptable, effective and secure strategy for information encryption-decoding. Information cryptography implies scrambling and unscrambling information utilizing a chose apparatus or technique, encoding the information implies annihilating the information to make it difficult to be perceived or utilized by some other unapproved party [34], [35].

Flexibility suggests the limit of the input encipher decoding encipher technique to use different range of the private instructor, different range of unencrypted text chunk, including clear clutter capacities with regards to key age [35], ability to change the hash limits. Procedure strength suggests making the hacking framework incomprehensible or incredibly testing to trusted by another client, while strategy productivity implies limiting the encryption, decoding times however much as could be expected. Encoded information, otherwise called ciphertext, seems mixed or muddled to an outsider individual or element getting to without consent and without knowing the PK and the tasks utilized for encryption. Information encryption standard (DES) is probably the easiest technique for information encryption-decoding.

VII. CONCLUSION

It is proposed another complex encryption and decoding plan (calculation) for an enormous information as well as little information. This examination work endeavors to show the security force of another Multi-level encryption routine through its capacity to scramble basic instant messages into a totally indistinguishable configuration. Here in our work we expanded the quantity of rounds to perform encryption. This brought about making encryption more grounded, which thus brought about higher security of bigger text as well.

REFERENCES

- [1] N. Sharma, Prabhjot, & H. Kaur. (2017). A Review of Information Security using Cryptography Technique. International Journal of Advanced Research in Computer Science, vol. 8, no. Special Issue, pp. 323-326.
- [2] B. Preneel. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. London: Springer.
- [3] Marshall Ball, Dana Dachman-Soled, & Mukul Kulkarni. (2020). New techniques for zero-knowledge: Leveraging inefficient provers to reduce assumptions, interaction, and trust. Daniele Micciancio and Thomas Ristenpart, editors, CRYPTO2020, PartIII, volume 12172 of LNCS, pages 674–703. Springer, Heidelberg.
- [4] Shohei Egashira, Yuyu Wang, & Keisuke Tanaka. (2019). Fine-grained cryptography revisited. StevenD. Galbraith and Shihō Moriai, editors, ASIACRYPT2019, PartIII, volume 11923 of LNCS, pages 637–666. Springer, Heidelberg.

- [5] Paulo S. L. M. Barreto. (2017). The WHIRLPOOL Hash Function.
- [6] Saarinen, M-J; Aumasson, & J-P. (2015). The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC). IETF. doi:10.17487/RFC7693. RFC 7693. Retrieved 4.
- [7] J. Dittman, P. Wohlmacher and K. Nahrstedt, 2001 "Using Cryptographic and Watermarking Algorithms" IEEE Multimedia, vol. 8, no. 3, PP. 54-65.
- [8] Lo, C. C., and J. ChenY, 1999 "Secure Communication Mechanism for GSM Networks" IEEE Trans. Consumer Electronics, vol. 45, PP. 1074-1080.
- [9] Musbahj. Aqel, A. S.Abdul-Ahad, R. S.Qahwaji, 2009 "Multidimensional encryption algorithm for computer networks" Department of Electronic Image and Media Communication School of Informatics, Bradford University, Richmond Road, Bradford BD7 1DP, U.K.
- [10] B. Schneier, 1996 "Applied Cryptography", 2nd ed. New York: Wiley.
- [11] Kefa Rabah, 2005 "Theory and Implementation of Data Encryption Standard: A Review" Information Technology Journal 4(4): 307-325.
- [12] http://en.wikipedia.org/wiki/Stream_cipher [accessed 21 June 2012].
- [13] http://en.wikipedia.org/wiki/Block_cipher [accessed 21 June 2012].
- [14] C. Brenton and H. Cameron 2003, "Networking Security", Sybex.
- [15] C. Peikari and S. Fogie 2003 "Maximum Wireless Security", SAMS Publishing.
- [16] Charles P. Pfleeger and Shari L. Pfleeger, 2012 "Security in computing" Prentice Hall PTR Upper Saddle River, NJ, USA. [online] available at: <http://www.crypto.com/papers/>. [accessed 20 August 2012].
- [17] Diao Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, 2010 "Performance Evaluation of Symmetric Encryption Algorithms" International Journal of Network Security, Vol.10, No.3, PP.216-222, May 2010.
- [18] Eli Biham, Helena Handschuh, 2007 "seminar on symmetric cryptography", Dagstuhl seminar 07021
- [19] Federal Information Processing Standards (FIPS), Publication 197, "Advanced Encryption Standard" November 2001, [online] available at: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf> [accessed 17 August 2012].
- [20] Ruangchaijatupon, P. Krishnamurthy, 2001 "Encryption and Power Consumption in Wireless LANs-N," The Third IEEE Workshop on Wireless LANs - September 27-28, 2001- Newton, Massachusetts.
- [21] S. Hirani, 2003 "Energy Consumption of Encryption Schemes in Wireless Devices Thesis" university of Pittsburgh.
- [22] Nadeem, Aamer, 2005 "A performance Comparison of Data Encryption Algorithms" IEEE Information and Communication Technologies, 2005. ICICT 2005. First International Conference, 2006-02-27, PP.84-89.
- [23] S.Z.S. Idrus, S.A. Aljunid, S.M.Asi, 2008 "Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, PP-20-25.
- [24] Matt Blaze, 1993 "A Cryptographic File System for Unix". First ACM Conference on Communications and Computing Security, Fairfax, VA, November 1993.
- [25] Arpad Incze "The basic of text encryption and decryption".
- [26] Tim Grembowski "Comparative Analysis of the Hardware Implementations of Hash Functions SHA-1 and SHA-512" Electrical and Computer Engineering, George Mason University, 4400 University Drive.
- [27] Federal Information Processing Standards Publication (FIPS) 180-4, "Secure Hash Standard" March 2012, [online] available at: <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf> [accessed 20 August 2012].
- [28] Dr Lawrie Brown, 1998 "A Current Perspective on Encryption Algorithms" School of Computer Science, Australian Defense Force Academy, Canberra, Australia AUUG98.
- [29] Sean O'Melia and Adam J. Elbirt, 2010 "Enhancing the Performance of Symmetric-Key Cryptography via Instruction Set Extensions" IEEE Transactions On Very Large Scale Integration (Vlsi) Systems, Vol. 18, No. 11, November 2010.
- [30] J. Elbirt, W. Yip, B. Chetwynd, and C. Paar, 2001 "An FPGA-based performance evaluation of the AES block cipher candidate algorithm finalists" IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 9, no. 4, pp. 545-557.
- [31] Li Xiaoming and Yun Zhao, 2011 "Research on Power Information Encryption Algorithm Based on Composite Chaotic System in Wavelet Transform Domain" ELSEVIER, Procedia Engineering 15 (2011) 2118 - 2122.
- [32] Kevin Sean Chan and Faramarz Fekri, 2004 "A Block Cipher Cryptosystem Using Wavelet Transforms Over Finite Fields" IEEE Transactions On Signal Processing, Vol. 52, No. 10, October 2004.
- [33] Carl Landwehr, Dan Boneh, John C. Mitchell, Steven M. Bellovin, Susan Landau and Michael E. Lesk, 2012. "Privacy and Cyber security: The Next 100 Years" Vol. 100, Proceedings of the IEEE.
- [34] Chung-Ming Ou, 2008 "Design of Block Cipher by Simple Chaotic Functions" IEEE Computational Intelligence Magazine May 2008.
- [35] Meikang Qiu, Wenzhong Gao, Min Chen, Jian-Wei Niu and Lei Zhang, 2011 "Energy Efficient Security Algorithm for Power Grid Wide Area Monitoring System" IEEE Transactions On Smart Grid, Vol. 2, No. 4, December 2011.
- [36] J. Ree, V. Centeno, J.Thorp and A. Phadka, 2010 "Synchronized phasor measurement applications in power systems" IEEE Trans. Smart Grid, vol. 1, no. 1, PP. 20-27.
- [37] Daniel A. Menasce, 2003 "Security Performance" IEEE Internet Computing, June 2003