JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 2906 - 2910
https://publishoa.com
ISSN: 1309-3452

Proposed Model for Cryptographic Security Goals using Analytical Hierarchical Process

Ravi Ranjan Choudhary[a], Rajeev Kumar[b], Lokendra Singh Umrao[c*,] Divya Singh[d]
[a,b,c,d]*Department of Computer Science and Engineering, Institute of Engineering and Technology, Dr. Rammanohar Lohia Avadh University, Ayodhya, India*

*Corresponding author Email: lokendrasingh@rmlau.ac.in

ABSTRACT
The quick progress of this technology becomes vital in upcoming years. Cryptography is where security engineering meets mathematics. It gives us the tools that most modern security protocolsrely on. It is perhaps the most important enabling technology for securing distributed systems,yet it is surprisingly difficult to do correctly. Any form of data on a network is private to an individual, and attackers can access it while sharing it with the intended receiver. The demand for availability, confidentiality, Integrity and non-repudiation required for handling is increased. This paper discussed brief about cryptographic methodology and a new model for enhancing cryptographic goals that can be used to secure applications.

Index Terms: Security engineering, Cryptographic methodology, AHP

I Introduction

The internet and its apps now pervade every aspect of our life. To protect the security of our data, we must use cryptographic technology. Network security safeguards system resources [6]. It is in charge of protecting data sent from one computer to another via the internet. In Greek, kryptos logos means "hidden word." Cryptography is the study of securing data. It involves encrypting and decrypting data using mathematical techniques. It's an effort to secure processing. Cryptography is a newer technology for data security [8]. Cryptography now protects data in technology applications. For some applications, data security is vital. Personal information is required for e-commerce, e-banking, email, medical databases, and many more services [10]. Consider a sender named Alice who intends to deliver a data message to a recipient named Bob. Alice uses an unsafe channel. Whether a phone line, a computer network, or something else, Hackers may intercept and read sensitive data in transmissions. They can also update or modify the message as it is being conveyed, oblivious to Bob. This survey compares and contrasts several encryption algorithms with many examples. In online banking, shopping, stock trading, and bill payment, security is crucial to secure sensitive information [7-9]. Our data sent over the internet is not safe. Encryption algorithms protect data sent over the internet. Encryption protectsdata from malicious attacks.

II Proposed Model for Enhancing Cryptography goals

Cryptography has various types and procedures. These systems are easily exposed and insecure. Many assessment indicators, such as resolution efficiency, ease of operation, result integrity, andresolution behaviour, exist to judge and select an identity resolution server with good security performance [12]. We can use the AHP method to create a hierarchical assessment model to determine the security performance evaluation score of the resolution data security [11].

2.1 AHP Model

A complex multi-objective decision-making problem is treated as a system, with each objective broken down into many objectives or criteria, and each level broken down into sub-indicators, resulting in a hierarchical single ranking and total ranking based on qualitative indicators. AHP uses behaviour science to quantify decision makers' empirical judgments [3]. It is ideal for situations where the objective structure is complex and data is lacking. It is a common mathematical tool in systems research. AHP can analyse complicated and ambiguous correlations and test decision makers' judgement and comparison. It is frequently used in social, economic, and management domains. It can be used to graduate employment issues, for example. Graduates and employers each have their own selection criteria [5]. A pleasant living environment, a good firm reputation, a good working environment and greater prospects for future development are relevant characteristics for graduates. For example, huge cities and climate conditions [4] are molecular factors for a pleasant living environment. When a graduateis faced with multiple options, the AHP technique can help quantify the criteria. The quantitativevalue of each optional company is weighted, and the decision is based on the ranking. Figure 1 shows a 3-level evaluation model built on the preceding model concept.

This figure 1 is based on theoretical assumptions and mathematical techniques in order to provide insight into the decision model's efficiency. The evaluation's main goal is to determine the overall weights of the alternatives for each option. The decision maker (in this study effort, the authors are decision makers) chooses the best option based on the weights in the decision model. We were unable to construct every model of cryptography system that is theoretically evaluated with a step an in this work.

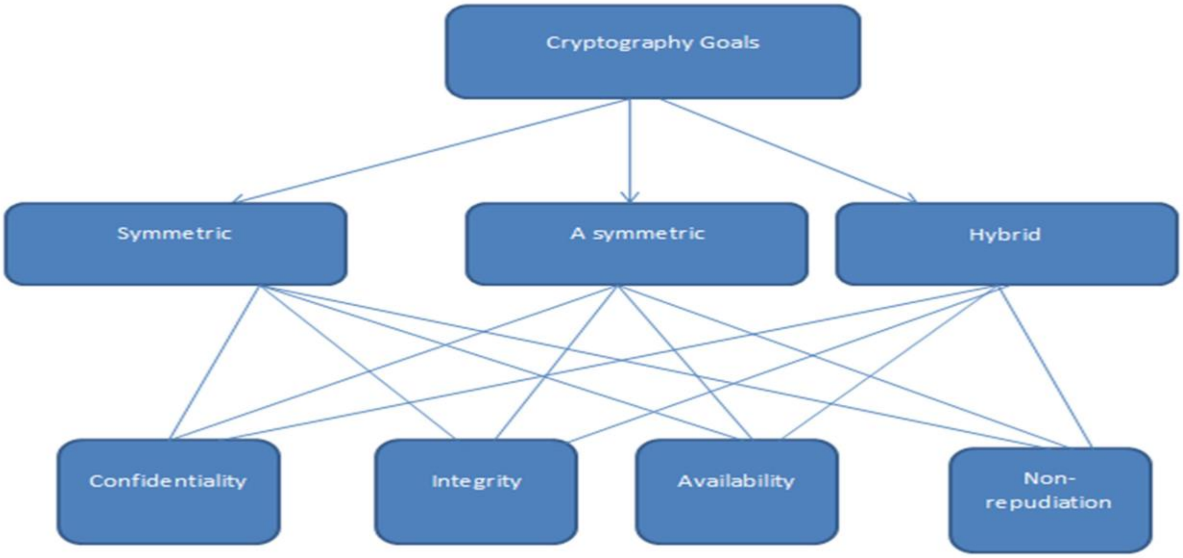

Fig 1: Evaluation Model

Step procedure, so we'll show you a symmetric model with each option and a set of rules for evaluating it. The pairwise comparison matrix 1 of 3 indicators $\{Fi, i = 1\sim3\}$was created after processing the data of the relevant study with arithmetic average, as shown in table 1 below. The following is the row and column order of the three indicators $\{Fi,$ $i = 1\sim3\}$: Confidentiality, Integrity, and Availability are the three pillars of our security.

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix},$$

$$W = \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix}, \text{ and } \quad w_i = \frac{\sum_{i=1}^{n} a'_{ij}}{n} \quad \text{for i} = 1, 2, \ldots, \text{n}$$

Equation (1)

Table 1: Weightage Allocation table

Symmetric Method	Confidentiality	Availability	Integrity
Confidentiality	1	3.5	6.7
Availability	2.5	1	3.9
Integrity	4.7	3.6	1
Total Weight	8.2	8.1	11.6

Table 2 compares a set of criteria to the goal. Technical and managerial components still dominate the overall confidentiality security policy views, accounting for 0.1219 of the local weight, followed by availability and integrity aspects at 0.4320 and 0.5775. It is vital to remember that the priority of symmetric criterion may vary depending on the situation.

Table 2: Evaluation step 3

Symmetric	Confidentiality	Availability	Integrity	
Confidentiality	0.1219	0.4320	0.5775	1.1314
Availability	0.304	0.1234	0.0862	0.7634
Integrity	0.5731	0.4444	0.9997	1.1037
	0.999	0.9998	0.997	

Table 3 and (B) show the relative weights of the three alternatives (confidentiality, integrity, and availability). In terms of average weight, both matrices (table 2 and 3, 3 (b)) have low average weight measurements, but this is acceptable because the entire measure is less than the maximumpoint.

Table 3: Evaluation step 4

Symmetric	Confidentiality	Availability	Integrity
Confidentiality	0.1077	0.3818	0.5104
Availability	0.3982	0.1616	0..4401
Integrity	0.5192	0..4026	0.0781
Average weight	1.025	0.946	1.0286

Table 3 (b): Evaluation step 5				
Symmetric	Confidentiality	Availability	Integrity	
Confidentiality	0.1050	0.4035	0.4962	1
Availability	0.3884	0.17082	0.41573	0.9749
Integrity	0.3884	0.17082	0.41573	1.010

Following are the key findings based on these results. In comparison to confidentiality and availability, decision makers give the highest weight (0.5039) to integrity. Confidentiality accounts for 0.4962, whereas availability accounts for 0.4264.

Table 5: Evaluation step 6					
Symmetric	Confidentiality	Availability	Integrity		
Confidentiality	0.1050	0.4035	0.4962	1	0.4962
Availability	0.3983	0.1752	0.4264	1	0.4264
Integrity	0.5039	0.4212	0.07516	1	0.5039
	1	1	1		

As a result, tables 5 and 6 indicate the relative relevance of cryptographic factors and indicators. The overall weights are computed by multiplying the weight of the criteria or sub-criteria by the parent perspective's important weight. The entire maturity assessment may be carried out afterthe weights of the cryptography factors, their indications in the assessment process, and the total

index values (0.4962, 0.4264, 5.39) can be determined by calculation. Table 5 is used to examinethe situation, and tables 5 shows the entire comprehensive index value. Figure 2 shows the comprehensive comparative goals of cryptography systems, highlighting the highest priority integrity goals in terms of confidentiality and availability.

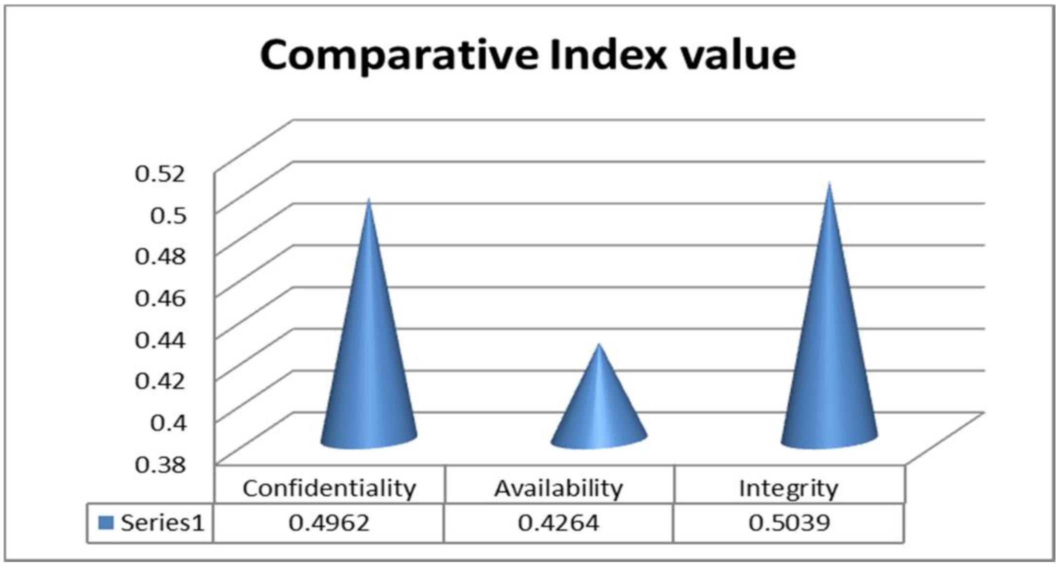

Fig 2: Comparative ValuesIV Conclusion

The AHP approach can help meet cryptography security goals (confidentiality, Integrity and availability). Further research into existing cryptosystems and current information assurance approaches may help increase security in general. The research finding that the AHP approach can be used to prioritise defence in-depth measures is verified. AHP-based decision-making can help increase crypto security. Using AHP to select and apply in-depth measures could be a beneficial technique. Future AHP research, particularly in security, may help us better understand how to design for data security.

References

Al-Harbi, K. (2001) Application of the AHP in Project Management. InternationalJournal of Project Management, 19, 19-27.

Utugizaki, M., Udagawa, M., Shinohara, M. and Osawa, K. (2007) Consistency Index for the Whole Decision Making. Proceedings of DEA Symposium 2007, Osaka University, Osaka, 102-105.

Geoff, C. (2004) The Analytic Hierarchy Process (AHP). Pearson Education, Upper Saddle River.

Cooper, C.R. and Schindler, P.S. (2008) Business Research Methods. 10th Edition,McGraw-Hill, Boston.

National Commission for the Protection of Human Subjects (1979) Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research. Department of Health and Welfare, Washington DC.

Bhatia, P., & Sumbaly, R. (2014). Framework for wireless network security using quantum cryptography. arXiv preprint arXiv:1412.2495.

Tayal, S., Gupta, N., Gupta, P., Goyal, D., & Goyal, M. (2017). A Review paper on Network Security and Cryptography. Advances in Computational Sciences and Technology, 10(5), 763- 770.

Panda, M. (2014). Security in wireless sensor networks using cryptographic techniques. American Journal of Engineering Research (AJER), 3(01), 50-56.

Shyam Nandan Kumar, "Technique for Security of Multimedia using Neural Network," Paper id-IJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05, pp.1-7. Sep-2014

Daemen, J., and Rijmen, V. "Rijndael: AES-The Advanced Encryption Standard, Springer, Heidelberg, March 2001.

Ritu Pahal, Vikas Kumar,"Efficient implementation of AES", International journal of advanced research in computer science and software engineering, volume3, issue 7,july2013.

N.Lalitha,P.Manimegalai,V.P.Muthu kumar, M. Santha,"Efficient data hiding by using AES and advance Hill cipher algorithm ", International journal of research in computer applications and Robotics, volume 2, issue 1 ,January 2014.