I.J. Intelligent Systems and Applications, **2012, 10, 25-34**
Published Online September 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijisa.2012.10.03

Anti-Spam Software for Detecting Information Attacks

Saadat Nazirova
Institute of Information Technology of Azerbaijan National Academy of Sciences, 9, F.Agayev Street, Baku, Azerbaijan, Az1141,
Email: sbunyadova@gmail.com

Abstract— In this paper the development of anti-spam software detecting information attacks is offered. For this purpose it is considered spam filtration system with the multilayered, multivalent architecture, coordinating all ISP's in the country. All users and ISPs of this system involved in spam filtration process. After spam filtering process, saved spam templates are analyzed and classified. This parameterizing of spam templates give possibility to define the thematic dependence from geographical. For example, what subjects prevail in spam messages sent from the certain countries? Analyzing origins of spam templates from spam-base, it is possible to define and solve the organized social networks of spammers. Thus, the offered system will be capable to reveal purposeful information attacks if those occur.

Index Terms— E-mail Spam, Unsolicited Bulk Messages, Filtering, Information Attack, Human Rights, Multilayer Architecture

I. Introduction

Over the past two decades, information technologies have radically changed the ways of saving and transmitting information. E-mail is one of the most widely used types of such kind of service. It is not just a way to deliver messages; it is communication, information distribution and management of various processes in the business. The main advantage of e-mail is its accessibility. Send an e-mail is much cheaper than usual; it allows you to send messages to multiple recipients at no additional cost. E-mail has many advantages, but because of these advantages there are major risks associated with its use. Access to e-mail becomes a disadvantage when spammers begin to use email to send spam [1].

Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email [2].

By spam reports of MacAfee In 2011, the average global spam rate was 2 trillion per day [3]. The growth of spam volume has led to the development of anti-spam industry. Nevertheless, despite the abundance of software products, some anti-spam products are ineffective or do not know how to defend against new types of spam as they appear. It is very difficult to choose software solutions with a high percentage of spam filtering and a low percentage of false positives among the existing ones. False-positive e-mail is a necessary e-mail, classified as spam by the spam filter. Of course, it is easy to achieve 100 percent spam blocking, but in this case, the risk of increasing false positives is escalating. Losing one legitimate e-mail is worse than getting one hundred spam messages.

The rest of the paper is organized as follows. Section 2 presents related works. Section 3 describes the architecture of the offered anti-spam system. The proposed algorithm for realization of anti spam system is presented step by step in Section 4. Functionalities of the offered software are described in Section 5. Conclusion is given in Section 6.

II. Related Works

There are a lot of theoretical and practical ways to despite spam. Though the first spam was sent in 1978 it began to be written about it as a problem in scientific literature only from 1982. The first paper where this problem is considered is the Peter J. Denning's article [4]. The first mathematical apparatus applied to spam filtering systems is the Bayes' algorithm, which was used first by Sahami et.al in 1996 and then by other researchers [5-8]. After this attempt there were such mathematical approaches as Kolmogorov complexity, Markov chain, PageRank and Hidden Markov Model which are met in papers Spracklin L.M., et al. [9], Paolo B., et al [10], and José Gordillo, et al. [11]. But the latest three years are full with scientific papers offering data mining techniques against spam problem, as spam grows day by day, and become more intellectual. Igor Santos and et al. offered in their paper [12] a spam filtering system that use semantics in spam filtering by representing e-mails with Information Retrieval model: the enhanced Topic-based Vector Space Model (eTVSM). In Cheng Hua Li's work [13] it is showed effectiveness of using hybrid similarity measure feature representation methods and refined neural network

algorithms in spam filtering. Juan Carlos Gomez and et al. offer in they work [14] classification of email using document classifier based on text content features. This technique Principal Component Analysis Document Reconstruction reaches a better performance than the popular Support Vector Machine classifier. Another novel approach to spam filtering based on the minimum description length principle and confidence factors is presented in Tiago A. Almeida and et al. paper [15].

The use of semantics in spam filtering by introducing a preprocessing step of Word Sense Disambiguation (WSD) is explored in Carlos Laorden and et al. paper [16] and showed that the proposed method can detect the internal semantics of spam messages presented. In Francisco Salcedo-Campos and et al. paper [17], a novel spam-filtering technique based solely on the information present in headers is introduced. By Noemi Perez-Diaz's and et al. approach [18], headers of email are considered as the result of a dynamic process that generates characters. They applied SDAI methodology to compare eight different well-known content-based spam filtering techniques using several established accuracy measures.

The observed characters are treated as signals and parameterized in accordance with standard signal pre-processing techniques by extracting relevant parameters from the header.

In addition there are a lot of software solutions based on above mentioned mathematical approaches. In this paper it is offered anti-spam software which is differ from others on two features.

At first in the offered anti-spam solution the spam filtration process takes into account multiple subjective assessments of users, institutions, even governments belonging to this or that correspondence delivered to this spam category. Top level filtering is based on user requests of the lower level. In this case, Universal Declaration of Human Rights (Article 19) [19] for access information is not violated. The proposed system is very flexible since it accepts all user opinions in formulating and implementing its policies to prevent spam with no restrictions. Nevertheless whatever the policy of spam combat is, it must be based solely on the basic norms and principles of human rights. Thus, the first thing to consider is the user relationship with any correspondence. Additionally, the situation is further complicated by the fact that the user opinion is not stable and permanent. It varies depending on the user mood and a number of other subjective circumstances. Therefore, at some points, any static approach to unwanted e-mail filtering may violate norms and principles of human rights. In this context, the dynamic approach to combating spam, which could take into account the fickle attitude of the users as it appears during the process of an e-mail viewing, is presented. In the current individual and corporate anti-spam systems the filter are trained, as a rule, on a limited number of messages sent only to a specific user or a specific provider [20, 21, 22, 23]. Consequently, the qualitative spam filtering is not provided, and the problem of collaborative filtering with the involvement of individual users and internet service providers still remains unsolved. The quality of the filtration can be improved through the use of complex hierarchical and multi-user filtration systems, ensuring the full-scale participation of users in the detection process of errors of filtration and corresponding filter settings at each level [24].

The second point is that the proposed anti-spam software is also spam analyzer to detect information attacks. Also classifying spam messages it will be possible to establish thematic dependence from geographical (for example, what subjects prevail in the spam-messages sent from the certain countries). It is applied classification of textual spam emails using text mining techniques offered by author in article [25]. Application of text mining methods to an e-mail can raise efficiency of a filtration of spam. Methods of text clustering and classifying successfully applied to spam problem form last decade. A filtration of e-mail onto legitimate and spam with the help of clustering analysis are considered in the papers [26-32]. But proposed system is not filter messages into spam and not spam, and still to divide spam messages into thematically similar groups and to analyze them, in order to define the social networks of spammers [33].

III. Architecture of the Offered Anti-Spam System

The proposed system has a hierarchical multi-layer structure consisting of three levels: governmental, corporate and personal [24, 34]. Each level, in its turn, has a policy of spam struggle, which is defined by a set of features contained in spam-mails on the servers of service providers of this level. The end users and service providers are at the system nodes. Service providers, corporate mail servers and client computers are the vertical components of the proposed hierarchical system. Requests for the filtration of unwanted correspondence are sent from lower level nodes to the top level nodes.

Each level of multi-level hierarchical system has server nodes, which accumulates spam-mail base coming from the lower level nodes or from the usual nodes of the same level. Filtering unwanted correspondences can be generated at any of these levels; however the proposed method involves filtration, which is realized at the top level - the level of service providers, while the information comes from the lower levels for the processing. Filtering is implemented top-down, and the base of spam templates and rules is provided from the bottom upward. The base of spam templates is proposed to form user reports about the spam within the received e-mail.

The system will filter the message for the user node k_{j_i} only and only if the message is recognized as a

spam by sufficient number of nodes attached to the server node j_i. Numerous spam templates of i level at a time t equal to the intersection of the set of spam templates j_i at a time t. That is, this set consists of the spam templates, which at that time are delegated as an unwanted message by the all users of that level. The presented system allows the possibility to withdraw back (restore) the post, previously marked as spam. In this case, the message $s_{k_{ji}}{}^{z}(t)$, reported by the user k_{j_i} as a spam at a time t, is removed from the set of spam templates $U_{j_i}(t)$. Accordingly, the overall base of spam templates $U_i(t+1)$ and anti-spam policy $P_i^s(t+1)$ of $i=0,N$ level changes. The dynamic system algorithm allows to restore the state of a dynamical system in the pace of real time (during the process), using the input information about the current system in discrete time. Despite the fact, that spam filtering in the proposed system is carried out top-down, in fact, it is controlled by the users from the bottom upwards [34].

IV. The Offered Algorithm

For the clarity of the mechanism for implementing the proposed approach, we describe the incremental algorithm of proposed spam filtering system for e-mail exchange (Fig.1).

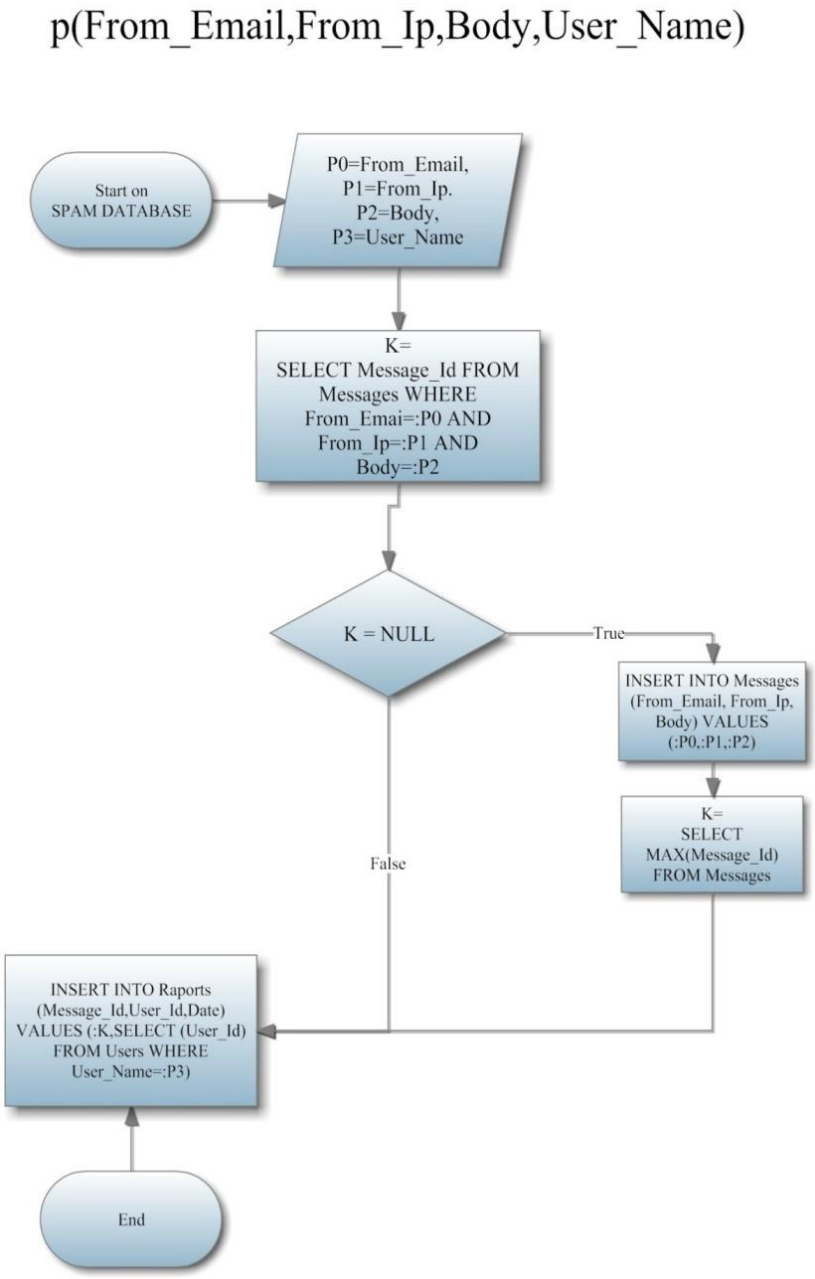

Fig.1: Algorithm of the developed anti-spam software

Step 1. The user checks the e-mail.

Step 2. Received e-mail is checked for spamness element.

Step 3. Legitimate correspondence comes into the folder "inbox".

Step 4. Correspondence marked as a spam, is delegated to the server for subsequent processing.

Step 5. The server analyzes the e-mail and identifies the spamness index, which is characterized by a total number of delegation operations of the given e-mail.

Step 6. The e-mail is checked for the spam templates correspondence by the database.

Step 7. If no match is found, the e-mail is added into the database, and initial spamness index is assigned to it.

Step 8. If a match is found, the spamness index is compared with the total number of users.

Step 9. If the e-mail spamness index is less than the user number, the index is adjusted to unit.

Basing on this algorithm, the software was developed in Borland C language, in Delphi environment. The developed system is based on the client-server technology basis. Absolute Database was selected as a database.

Spamness of incoming e-mail is checked as in Fig 2.

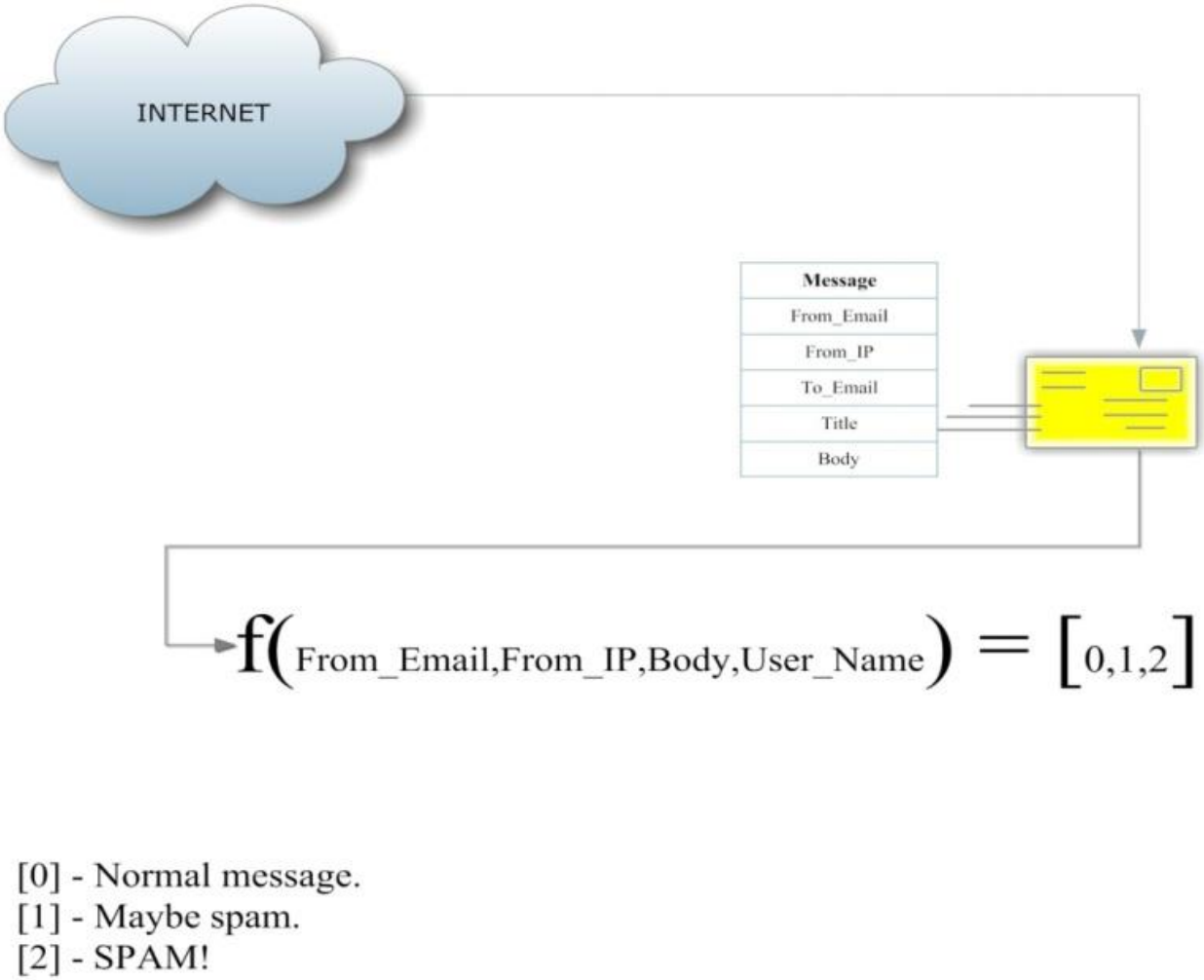

Fig 2: Checking each incoming message for spamness

The function

$$f(From\_Email, From\_IP, Body, User\_Name)$$

takes the value 0, if the e-mail is legitimate, it takes the value 1 - if the e-mail is doubtful, it takes the value 2 - if it is a spam. Afterward, query is held by the Fig. 3, on the report number for that spam-mails, and the resulting report number is compared with the user number included to the same group.

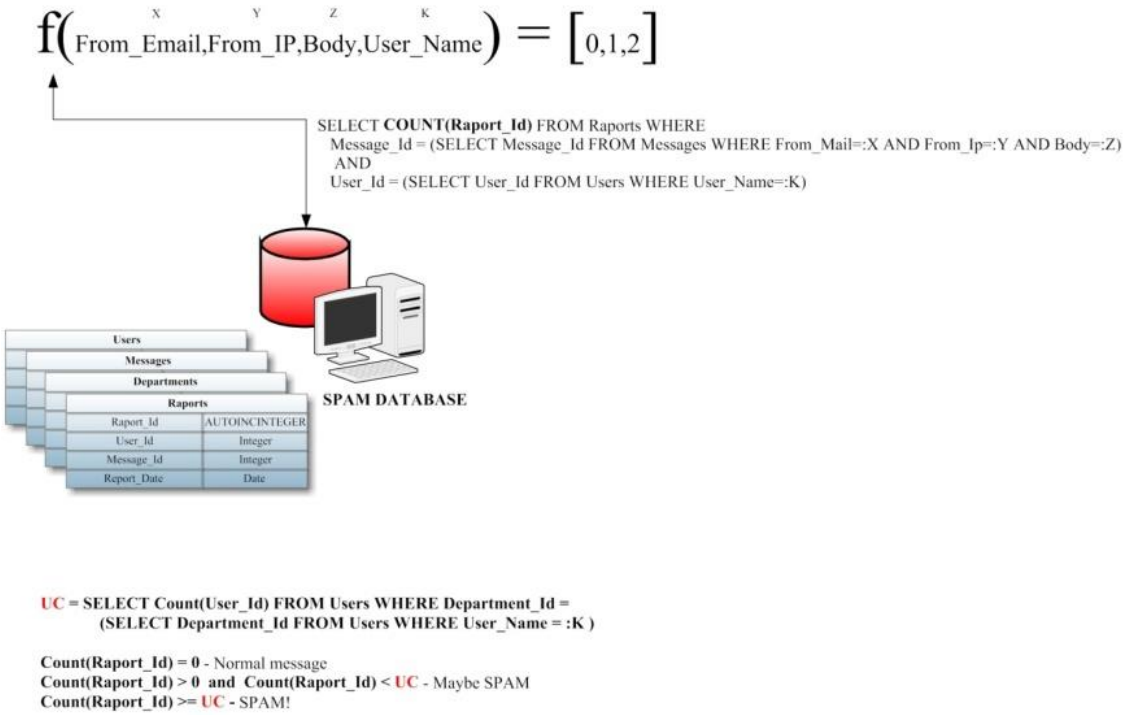

Fig. 3: Schema of the query for the number of reports and comparison with the number of users

The database includes User Database tables, which stores information about the users, and Spam Database tables, which stores information about spam-mails. Schemes reflecting the functional structures of these tables are shown in Fig. 4 and Fig. 5.

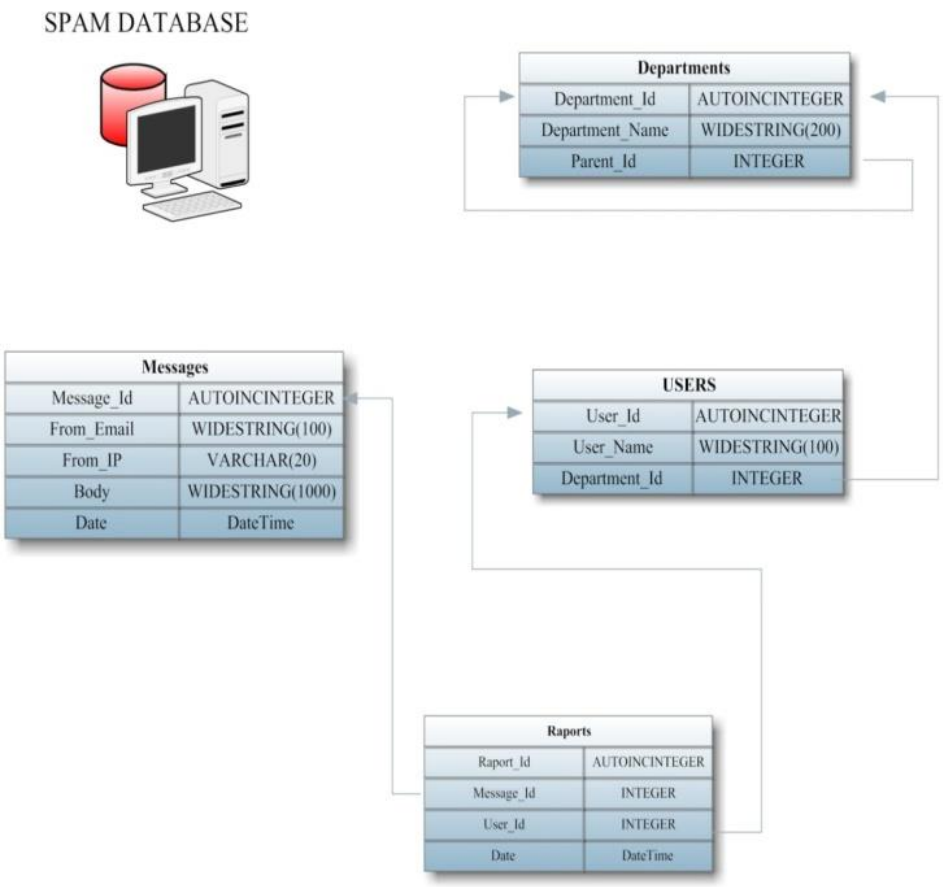

Fig. 4: Spam Database Tables

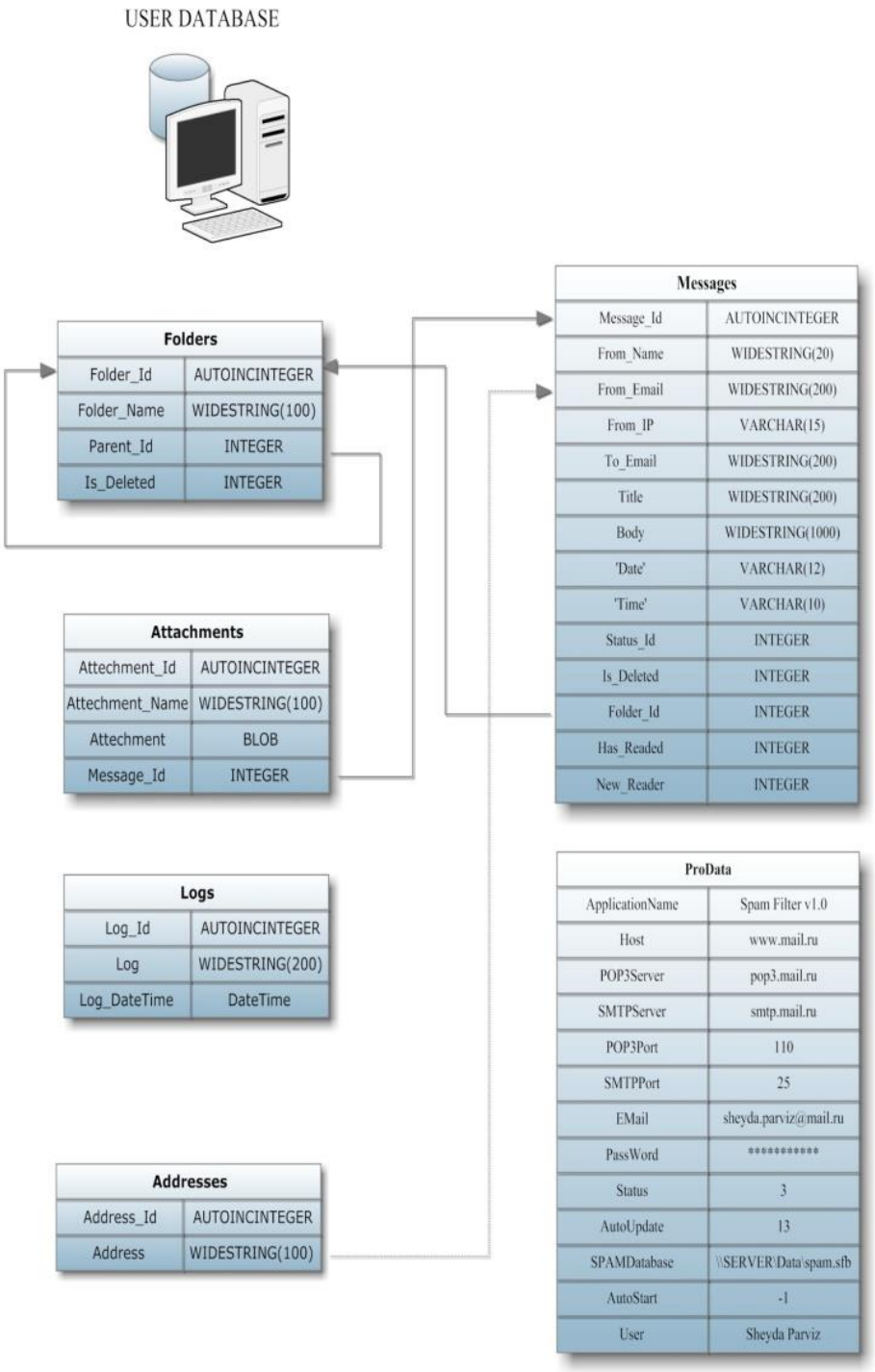

Fig. 5: User Database Tables

V. Functionalities of the Offered Anti-Spam Software

Developed anti-spam software consists of two modules: the client - for users, and the server - for the administrator. Computer requirements to install the two modules are minimal and simple enough to be executed. The interface and functional capabilities of the modules differ from each other significantly.

While installing a client module in the machines, the users register their e-mail and add the path to the database located on the server. This module is functioning as a normal e-mail client while sending and receiving messages (Fig. 6). In the system the user can sort his mails, delete e-mails, search, start a blacklist of spammers, configure the system, etc. When you receive a new e-mail the user marks the spam-mails, and the relevant information is recorded in the database on the server.

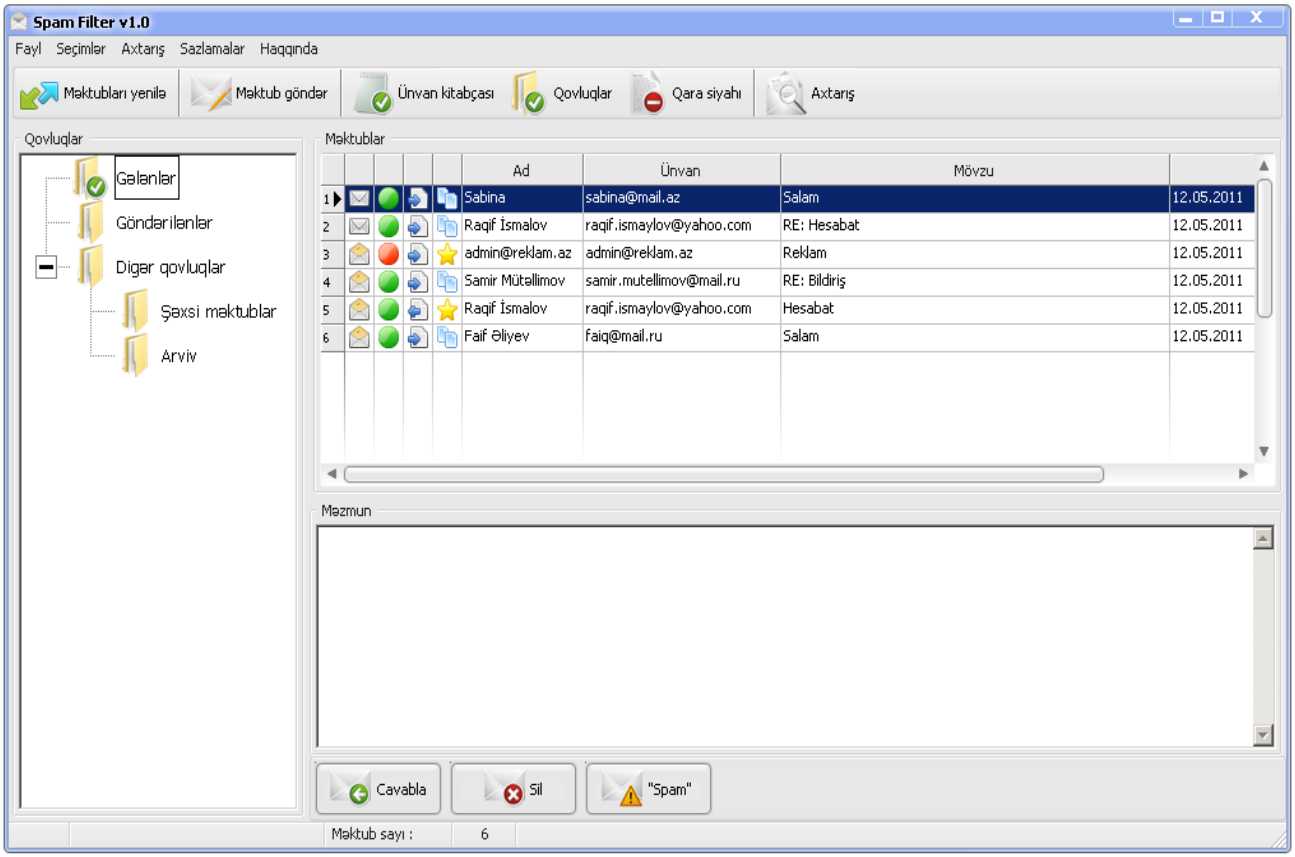

Fig. 6: User interface of the developed anti-spam software

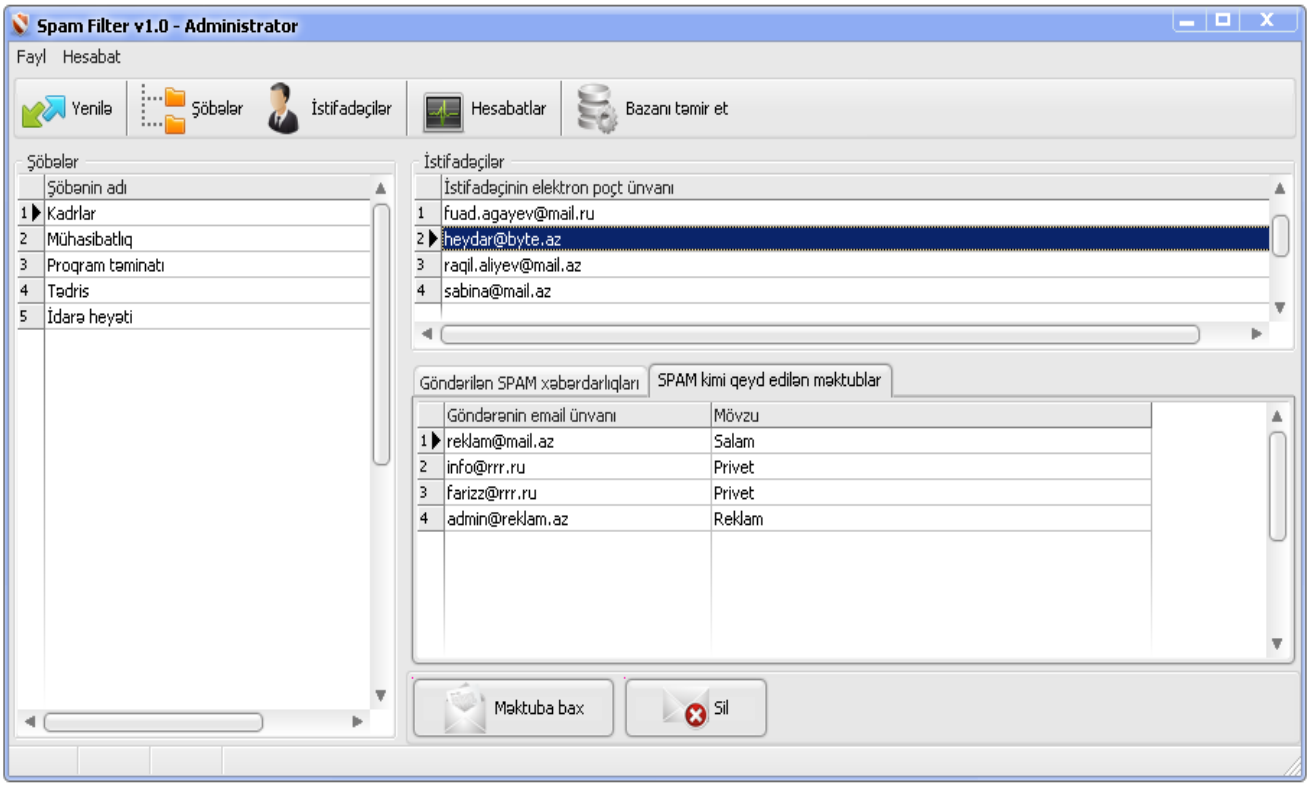

Fig. 7: Administration panel of the developed anti-spam software

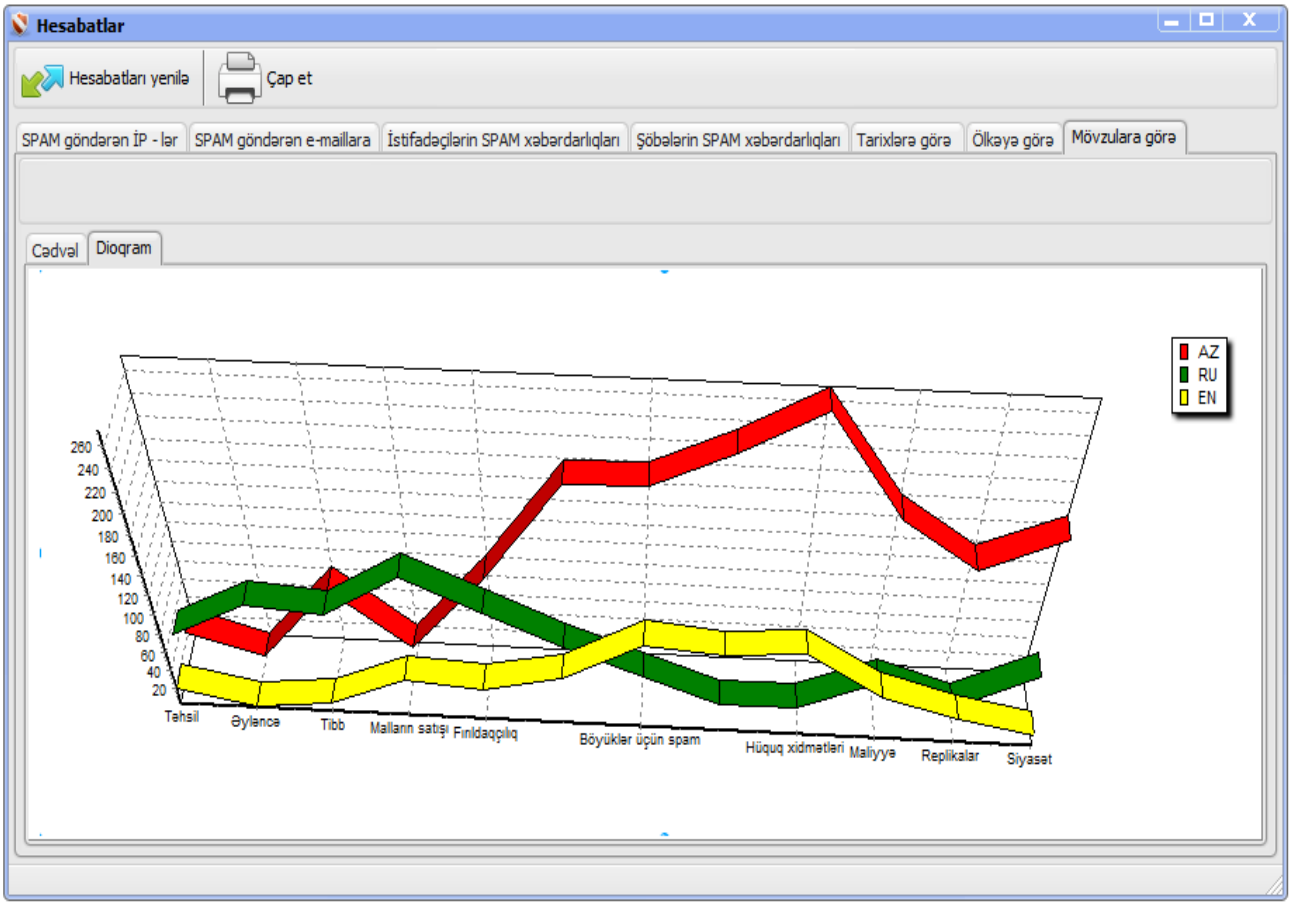

Fig. 8: Exported reports

Functional features of the server module are more; besides the spam filtering it is an analyzer of the information stored in the database. The server component is installed on the server node and controlled by e-mail administrator of the organization. After installing the server component the administrator access the server and adds information about sections and employees (Fig. 7).

The administrator is permitted to export and print the following reports in tabular and diagrammatic form (Fig. 8):

- By IP-addresses of spammers - what IP-addresses more or less spam comes from.
- By e-mail addresses of spammers - what e-mail addresses more or less spam comes from.
- By the user reports - which users receive more or less spam.
- By the reports of individual departments or groups of users - which users receive more or less spam.
- By the dates – in what periods of time more or less spam comes.
- By the countries - which countries more or less spam comes from.

Classifying and parameterizing spam templates, it will also be possible to define the thematic identity by the geographical one (for example, what topics dominate within the spam messages sent from certain countries). Thus, the system is able to identify the targeted information attacks, if any occur. Analyzing the sources of spam messages that are in the database of spam templates, it will be possible to determine and reveal the organized spam groups.

VI. Conclusion

Summarizing above-listed, we can note that the offered anti-spam software solution has the following features:

- It is a unique anti-spam filter based on a personalized server solution, that takes into account the human right for access information (Article 19);
- It is an analyzer, of spam messages accumulated in the database, which is capable to detect information attacks directed through the spam weapons.

Acknowledgements

I would like to give my sincere thanks to Dr. Rasim Alguliev and Dr. Ramiz Aliguliyev for their support, would also like to thank the anonymous reviewers for their valuable comments and suggestions.

References

[1] A. Taranov, O. Slepov, Email security, http://www.nextmail.ru/hist/security.phtml?t=2 (in russian)

[2] Wikipedia, Spam. http://en.wikipedia.org/wiki/Spam_email

[3] McAfee Threats Report: Fourth Quarter 2011, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2011.pdf

[4] J. P. Denning, ACM president's letter: electronic junk. Communications of the ACM, Vol. 25, No. 3, March 1982, pp. 163-165.

[5] M. Sahami, Learning limited dependence Bayesian classifiers. Proceedings of the second International conference on knowledge discovery and Data mining, Menlo Park, CA, 1996, pp. 334-338.

[6] M. Sahami, S. Dumais, D. Heckerman, et al., A Bayesian approach to filtering junk email. AAAI Workshop on Learning for Text Categorization, 1998, AAAI Technical Report WS-98-05.

[7] J. R. Hall, How to avoid unwanted email. Communications of the ACM, Vol. 41, no.3, March 1998, pp. 88-95.

[8] E. Gabber, M. Jakobsson, Y. Matias, et al., Curbing junk e-mail via secure classification. Proceedings of the second International conference on financial cryptography, March 23-25, 1998, pp. 198-213.

[9] L.M. Spracklin, L.V. Saxton, Filtering spam using Kolmogorov complexity estimates. 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), Vol. 1, 2007, pp.321-328. (in russian)

[10] P. Boldi, M. Santini, S. Vigna, PageRank as a function of the damping factor. Proceedings of the 14th International conference on World Wide Web, May 10-14, 2005, pp. 557-566.

[11] J. Gordillo, E. Conde, An HMM for detecting spam mail. Expert systems with applications, Vol. 33, no. 3, October 2007, pp. 667-682.

[12] I. Santos, C. Laorden, B. Sanz, et al., Enhanced Topic-based Vector Space Model for semantics-aware spam filtering. Expert Systems with applications, no.39 (2012), 2012, pp. 437-444.

[13] C. H. Li, J. X. Huang, Spam filtering using semantic similarity approach and adaptive BPNN. Neurocomputing, no. 92 (2012), 2012, pp. 88-97.

[14] J. C. Gomez, M.-F. Moens, PCA document reconstruction for email classification. Computational Statistics and Data Analysis, no. 56 (2012), 2012, pp. 741-751.

[15] A. A. Tiago, A. Yamakami, Facing the spammers: A very effective approach to avoid junk e-mails. Expert Systems with Applications, no. 39 (2012), 2012, pp. 6557-6561.

[16] C. Laorden, I. Santos, B. Sanz, et al., Word sense disambiguation for spam filtering. Electronic Commerce Research and Applications, December 2011, pp. 1-3.

[17] F. Salcedo-Campos, J. Dнaz-Verdejo, P. Garcнa-Teodoro, Segmental parameterization and statistical modeling of e-mail headers for spam detection. Information Sciences, no. 195(2012), 2012, pp. 45-61.

[18] N. Perez-Diaz, D. Ruano-Ordos, F. Fdez-Riverola, et al., SDAI: An integral evaluation methodology for content-based spam filtering models. Expert Systems with Applications, 2012, pp. 1-14.

[19] Universal Declaration of human rights, Article 19 http://www.un.org/en/documents/udhr/index.shtml #a19

[20] P. A. Baranov, Review of anti-spam and E-mail viruses. Computer Systems, no.1, 2004, pp. 44-50. (in russian)

[21] B.Y. Sirkov, "Killers" and "consumers" or the fight against spam. Technology and Communications, no. 4, 2004, pp. 102-105. (in russian)

[22] R. Anderson , Get rid of spam. Networks and communication systems, no. 11(117), 2004, pp. 94-104 (in russian)

[23] L. Pelletier, J. Almhana, V. Choulakian, Adaptiv Filtering of SPAM. Proceedings of the Second Annual Conference on Communication Networks and Services Research. IEEE, 2004. pp. 530-537.

[24] R. M. Alguliyev, S. H. Nazirova, Multilayer and Multiagent Automated E-mail Filtration System. Telecommunications and Radioengeneering, Vol.67, no.12, Begell House, 2008, pp. 1089-1095.

[25] R.M. Alguliyev, R.M. Aliguliyev, Classification of Textual E-Mail Spam Using Data Mining Techniques. Applied Computational Intelligence and Soft Computing Vol. 2011, Article ID 416308, 8 pg.

[26] C. James, H. Ray, Tightening the net: A review of current and next generation spam filtering tools. Computers and security, no. 25, 2006, pp. 566-578.

[27] H. Wen-Feng, Ch. Te-Min, An incremental cluster-based approach to spam filtering. Expert Systems with applications, no. 34, 2008, pp. 1599-1608.

[28] M. L. Sang, S. K. Dong, S. P. Jong, Spam Detection Using Feature Selection and Parameters Optimization. IEEE International Conference on Complex Intelligent and Software Intensive Systems, 2010, pp. 883-888.

[29] F. S. Mehrnoush, B. Hamid, Spam detection using dynamic weighted voting based on clustering. Second International Symposium on Intelligent Information Technology Application IEEE, no. 2, 2008, pp. 122-126

[30] S. Minoru, Sh. Hiroyuki, Spam detection using text clustering. IEEE Proceedings of the 2005 International Conference on Cyberwords, 2005, pp. 316-319.

[31] C. Paulo, L. Clotilde, S. Pedro, et al., Symbiotic Data Mining for Personalized Spam Filtering. IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 2009, pp. 149-156.

[32] Kh. Ahmed, An Overview of Content-Based Spam Filtering Techniques. Informatica, no. 31, 2007, pp. 269-277.

[33] S. Nazirova, Mechanism of classification of text spam messages collected in spam pattern bases. PCI 2010 Third International Conference on Problems of Cybernetics and Informatics, N2, 2010, pp. 206-209.

[34] R. M. Alguliyev, S. H. Nazirova, Mechanism of formation and realisation of anti-spam policy. Telecommunications, Moscow, Vol. 12, 2009, pp. 6-1. (in Russian)

Saadat Nazirova was born on June 03, 1979 in Azerbaijan. She received the B.Sc. and M.Sc. degrees from Applied Mathematics and Cybernetics department of Azerbaijan State University, in 2000 and 2002, respectively.

From 2006 she is PHD student at the Institute of Information Technology of Azerbaijan National Academy of Sciences. She has published over 10 refereed journal and conference papers in the areas of email filtering systems. Her representative published articles lists as follow: Classification of Textual E-mail Spam Using Data Mining Techniques (USA: Applied Computational Intelligence and Soft Computing, 2011), Two Approaches on Implementation of CBR and CRM Technologies to the Spam Filtering Problem (USA: Journal of Information Security, 2012), Survey on Spam filtering techniques (USA: Communications and Networks, 2011), etc. Moreover, she is an expert in implementation of ISO 27000, 20000 standards and development of Information Security Management Systems. Her research interests include text classification, data mining, CBR and CRM technologies. Especially, her researches about the methods of filtering electronic junk mail.

How to cite this paper: Saadat Nazirova,"Anti-Spam Software for Detecting Information Attacks", International Journal of Intelligent Systems and Applications(IJISA), vol.4, no.10, pp.25-34, 2012. DOI: 10.5815/ijisa.2012.10.03

