Optimization Pursuit: To optimize and enhance the efficacy of Online Voting System by referring various latest techniques

Er. Daljeet Singh[1], Karanvir Singh[2], Khushpreet Kaur[3], Jaskaran Singh[4]
[1]Guru Nanak Dev Engineering College, Ludhiana
(E-mail: diljitsingh007@gmail.com, karanvir9719@gmail.com)

Abstract— The present scenario of the online voting system uses many different techniques which are useful in maximizing the efficiency of the voting system. But in the prevalent voting system various design issues are leading to a gradual decrease in the working of the system. We are specifying some optimization techniques which when implemented in the current online voting system will increase the efficacy. Techniques such as Http Request Reduction provide a level of optimization required for the optimization of the current online voting system to enhance it further. To sum up, it can be concluded that this paper deals with the much required code optimization and database optimization techniques with relation to the web application of online voting system.

Keywords— *Database optimization techniques, Online voting system enhancement, Online voting system optimization, Web optimization techniques*.

I. INTRODUCTION

Web performance optimization occurs by monitoring and analyzing the performance of your web application and identifying ways to improve it. Web applications are a mixture of server-side and client-side code. Any application can have performance problems on either side and both needs to be optimized. The client side relates to performance as seen within the web browser. This includes initial page load time, downloading all of the resources, JavaScript that runs in the browser, and more techniques for optimization. Election process now a days play a very important role in Indian government. Elections are held to select a perfect candidate for who will lead our nation. In democratic setup people choose their leader by casting their valuable vote. Prevalent Indian voting system is an electronic voting system, under which a voter has to manually go to the voting booth to cast his vote, is a drawback of electronic voting system. So online voting system is a solution for this disadvantage of the Electronic Voting Machine voting paradigm. Using the concept of online voting system any voter can be voting for the candidate from anywhere on the specified Election Day and date. Online voting system security is main concern. In Figure1, laws of optimization are referenced. In online voting process to maintain the strict privacy and uprightness of the vote casted and authentication before the voting process is a considerable issue.

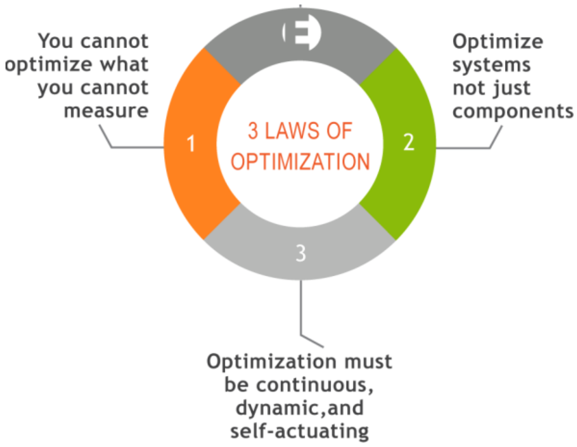
You cannot optimize what you cannot measure
1
3 LAWS OF OPTIMIZATION
2
Optimize systems not just components
3
Optimization must be continuous, dynamic,and self-actuating

Figure 1 : Laws of Optimization

After the voting process, the votes are calculated automatically. Only authorize person can cast their vote. Persons can be authorized by some methods that can be personal identification number (PIN) such as Aadhar card number, secrete message or user identity proof. All authenticated data can be collocated by user. Authentications can be performed by the administrators of the system. The voters and candidates can both request them to either activate or deactivate their user ids. In this online voting system a voter can cast his voter irrespective of his location. He has to register first to participate in the voting process. Registration is mainly done by the system administrator for security reasons. After registration, the voter is earmarked a username which he can use to log in to the system and enjoy the services provided by the system. If invalid/wrong details are submitted, then the citizen is not allowed to vote. Also a Type Analysis mechanism will check for the entry of only the validated data into the system to prevent any attacks.

II. LITERATURE REVIEW

Jambhulakar, chakole and pradhi [3] proposed a novel security for online voting system by using multiple encryption schemes. Provide security for cast vote when it is submitted from voting poll to voting server. Multiple encryptions to avoid DOS attack. They use cryptography concepts to take pros of digital signature. Encrypting the send forth vote to client server then send to voting server with the help of net. After sending encrypted vote then server side decrypt the vote before counting. On server side decryption of that vote is done before counting. So for this purpose we need a pair of asymmetric keys. To provide security from active intruder who can alter or tamper the casted vote when vote is transferring from voter to voting server, we are using digital signature. When a voter cast his/her vote after that he/she will digitally sign on that by using his/her own private digital signature, and send this to voting server, on voting server side that signature is checked by digital signature verifier of that voter which is publicly known. For this purpose each voter should have a private digital signature and a public digital signature verified. The feasibility of this is not justifiable to the people of a large democratic country. Pashine, ninave and kelapure [4] proposed an android platform for online voting system. They suggested security to the voter and his comfort. They suggested that the voter need not to go to the polling booth. In this application which is partitioned into three panels on the basis of its users as follows: Admin Panel: This panel will be specifically used by members of election commission to administer all the electoral processes including registrations of candidates & voters; and monitor all other actions carried out by them. Candidate Panel: This panel will be specifically used by electoral candidates to interact with the election commission & voters which will help them to work efficiently. Voter Panel: This panel will be specifically used by each individual voter who is eligible for casting his vote i.e. a person ageing 18 years or the above. These are the main users, for whom the application is being developed. Khasawneh [2] proposed an e-voting system for biometric security is providing a two sided solution such as server and user side. After casting the vote system will generate hardcopy for voter and also generate unique number. This unique number and voter name and identification number is secured. All content are stored in special box this box is secured box, this information is used for verifying the vote before stored in final database. This side copy is printed with unique barcode that can be easily readable automatically and scanned then randomly choose one copy, then this copy is tested. Firas I. Hazzaa, Seifedine Kadr [6] They suggested to deal with the design and development of a web-based voting system using fingerprint in order to provide a high performance with high security to the voting system. They are using web technology to make the voting system more practical. The new design is proposed for an election for a university for selecting the president of the university. The proposed EVS allows the voters to scan their fingerprint, which is then matched with an already saved image within a database. K. P. Kaliyamurthie1, R. Udayakumar, D. Parameswari and S. N. Mugunthan [5] Their aim is to make people who have citizenship of India and who are above 18 years and of any sex can give their vote through online without going to any physical polling station. Election Commission Officer (Election Commission Officer who will verify whether registered user and candidates are authentic or not) to participate in online voting. This online voting system is highly secured, and its design is very simple, ease of use and also reliable. Their software is developed and tested to work on Ethernet and allows online voting. It also creates and manages voting and an election detail as all the users must login by user name and password and click on his favorable candidates to register vote. This will increase the voting percentage in India. By applying high security it will reduce false votes. Himanshu Agarwal and G.N.Pandey [7] proposed aadhar id based online voting system for Indian election is proposed for the first time in this paper. The proposed model has a greater security in the sense that voter high security password is confirmed before the vote is accepted in the main database of Election Commission of India. In their system the tallying of the votes will be done automatically, thus saving a huge time and enabling Election Commissioner of India to announce the result within a very short period. This system is much secure and efficient than the traditional voting system. Manipulation of votes and delay of results can be avoided easily. A unique AADHAAR identity is the center point of our proposed model. It leads to the easier verification of both voters and candidates. But the registration of the voter should be completed only after the verification of all documents by the field officer. The field officer also verifies AADHAAR Identity Number from the main AADHAAR card database. After completing verification, the registration of the voter should be complete and the voter will get auto generated email which has all these information of the voter with the system generated password. The Voter can use this password for login and he/she can also change the system generated old password.

III. SCOPE OF STUDY

The scope of study consists of research about various web optimization techniques which can be employed to make the website content and databases more efficient and optimized. Website optimization is also sometimes used to describe the practice of improving the discoverability of a website for search engines, with the ultimate goal of improving search result rankings for key search terms. The scope will be in relevance with the web based solutions and implementations. The scope is delimited by the areas of different techniques which are to be employed in the web application code and databases.

IV. OBJECTIVES

Various objectives of optimization and enhancement of the security for the online voting system can be articulated as follows:

1. Study about the current research for optimization of existing voting system.
2. Enhancement of security of the existing voting system by implementing current research oriented techniques.
3. To develop a secure user interaction system to be used for voting system.
4. To develop a secure user interaction system to be used for voting system.

V. Fundamentals Of Proposed System For Web Optimization

Here we are using various techniques and tools to optimize the web application security and accessibility for the existing voting system paradigm. These include usage of various Input validations along with a suitable typing analysis system to make sure only required inputs are fed into the system and no other unrequired inputs are submitted. Various Optimization for web applications are also articulated in the Figure 2.

A. Features

1. Input validation [8]: Much work can be done with an aim to mitigate the impact of malicious input data without changing the application's source code. Automating the task of generating test vectors for exercising input validation mechanisms is also a topic explored in various existing systems.

2. Attack detection and prevention [8]: Different techniques have been proposed to detect the occurrence of SQL injection attacks in HTTP traffic. Some Intrusion detection systems are configured with a number of 'signatures' that support the detection of web-based attacks. These systems match patterns that are associated with known exploits against HTTP traffic obtained while monitoring web applications. Unfortunately, it is very difficult to keep the set of signatures up-to-date as new signatures must be developed when new attacks or modifications to previously known attacks are discovered. Anomaly-based intrusion detection systems also establish models describing the normal behavior of the monitored system and rely on these models to identify anomalous activity that may be associated to intrusions. The main advantage of anomaly detection systems compared to signature-based intrusion detection is that they can identify unknown attacks. While anomaly-based detection systems have the potential to protect web applications effectively against SQL injection attacks, they suffer from a large number of false positives. In contrast to anomaly-based detection systems, our approach employs static analysis using Type Analysis to achieve a larger coverage of protected parameters to the web application.

3. Vulnerability analysis [7, 8]: Static analysis as a tool for finding security-critical bugs in software has also received a great deal of attention. There are some projects where the goal of the analysis is to check whether a sanitization routine is applied before data reaches a sensitive sink. Several static analysis approaches have been proposed for various languages. Unfortunately, due to the inherently dynamic nature of scripting languages, static analysis tools are often imprecise. While our prototype static analyzer is simple and imprecise, our evaluation results are nevertheless encouraging.

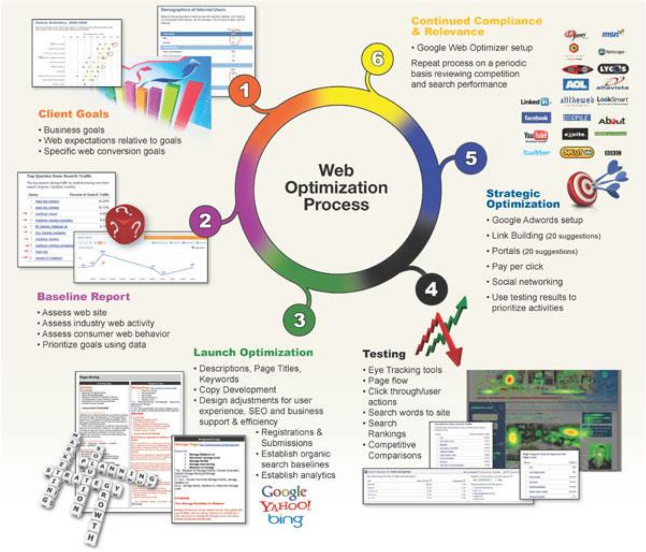
Web Optimization Process
1
Client Goals
• Business goals
• Web expectations relative to goals
• Specific web conversion goals
2
Baseline Report
• Assess web site
• Assess industry web activity
• Assess consumer web behavior
• Prioritize goals using data
3
Launch Optimization
• Descriptions, Page Titles, Keywords
• Copy Development
• Design adjustments for user experience, SEO and business support & efficiency
• Registrations & Submissions
• Establish organic search baselines
• Establish analytics
Google
YAHOO!
bing
4
Testing
• Eye Tracking tools
• Page flow
• Click through/user actions
• Search words to site
• Search Rankings
• Competitive Comparisons
5
Strategic Optimization
• Google Adwords setup
• Link Building (20 suggestions)
• Portals (20 suggestions)
• Pay per click
• Social networking
• Use testing results to prioritize activities
6
Continued Compliance & Relevance
• Google Web Optimizer setup
Repeat process on a periodic basis reviewing competition and search performance
msn
LYCOS
AOL
altavista
LinkedIn
alltheweb
LookSmart
facebook
About
YouTube
excite
twitter
MARKETING
PLANNING
STRATEGY
POSITION
GROWTH

Figure 2 : Optimization process

4. Input Sanitation through typo analysis [7]: Sanitation procedures, or sanitizers, focus on enforcing a particular security policy, such as preventing the injection of malicious code into an HTML document. While rigorous input validation can provide a security benefit as a side-effect, sanitizers should provide a strong assurance of protection against particular classes of attacks.

B. *Optimization Techniques for code*

Various optimization techniques [2, 5, 6] are to be implemented in this system which are articulated in the Figure 2 (Optimization process) to make sure the coding part of the system is well optimized and must run efficiently and snag free. And the efficacy of the system can be ensured using these techniques.

1. Http Request Reduction.
2. Deleting unnecessary files.
3. Code minimization.
4. Web caching optimization.
5. Image optimization.
6. Reducing the redirects.

C. *Optimization Techniques for Databases*

A number of database optimization techniques [2, 4, 7, and 8] can be employed to ensure the efficient working of the databases. The optimization methodology is shown in the Figure 3. This shows the proper handling of the optimization process under the effect of monitoring, analyzing and feedback processes. The database statistics are well loaded into the optimizer as shown in the below image. Then a suitable optimal plan is chalked out. Afterwards execution plans are outlined.

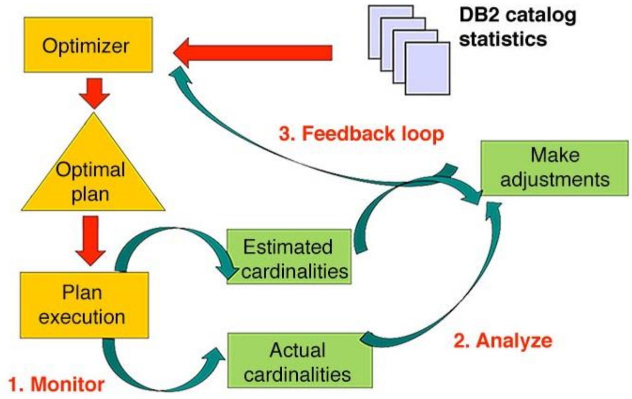

Figure 3 : Optimization Methodology

Various database optimization techniques can be well articulated in the following schemes-

1. Proper Indexing – Proper indexing is a must for increasing the query processing by the database. Excessive indexing and under indexing are both wrong and hugely hamper the performance.

2. Retrieving the relevant data only – Using the commands like LIMIT and * can make sure only relevant data is picked up by the query.

3. Getting rid of the correlated queries – Using just a single query instead of multiple queries can enhance the performance of the databases.

4. Avoiding the temporary tables or their proper use according to the requirement is beneficial.

5. Avoid coding loops – Coding loops can be avoided by using the unique UPDATE or INSERT commands with individual rows.

VI. CONCLUSION

We here intend to conclude that a system with a secure and accessible online voting system can be well optimized and enhanced using the above cited techniques. These techniques can well be implemented in any other web application or even any simple websites so that the system can works efficiently and properly. Various web optimization techniques and database optimization techniques can be enforced to optimize and enhance the security accessible for online voting system.

REFERENCES

[1] Smita Khairnar, Reena Kharat "Survey on Secure Online Voting System" in International Journal of Computer Applications(0975-8887), Volume 134 – No.13.January 2016.

[2] Divya G Nair, Binu. V.P, G. Santhosh Kumar," An Improved E-voting scheme using Secret Sharing based Secure Multi-party Computation", arXiv: 1502.07469v1 [cs.CR] 26 Feb 2015.

[3] Prof. S.M. Jambhulkar, Prof. Jagdish B. Chakole, Prof. Praful. R. Pardhi "A Secure Approach for Web Based Internet Voting System using Multiple Encryption", 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies,2014.

[4] Pranay R. Pashine, Dhiraj P. Ninave, Mahendra R. Kelapure, Sushil L. Raut, Rahul S. Rangari, Kamal O. Hajari," A Remotely Secure E-Voting and Social Governance System Using Android Platform", International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 13 - Mar 2014.

[5] K. P. Kaliyamurthie, R. Udayakumar, D. Parameswari and S. N. Muguthan , "highly secured online voting system over network", 4833 Indian Journal Science and Technology Print ISSN: 0974-6846 Online ISSN: 09745645 Vol 6 (6S) May 2013.

[6] Firas I. Hazzaa, Seifedine Kadry, Oussama Kassem Zein,"Web-Based Voting System Using Fingerprin Design and Implementation",International Journal of Computer Applications In Engineering Sciences ISSN: 2231-4946. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interfaces (Translation Journals style)," IEEE Transl. J. Magn.Jpn., vol. 2, Aug. 1987, pp. 740–741 [Dig. 9th Annu. Conf. Magnetics Japan, p. 301] 1982.

[7] Himanshu Agarwal, G.N.Pandey, "Online Voting System for India Based on AADHAAR ID", Eleventh International Conference on ICT and Knowledge Engineering 2013.

[8] Theodoor Scholte, Davide Balzarotti, William Robertson, Engin Kirda, "Preventing Input Validation Vulnerabilities in Web Applications through Automated Type Analysis".

[9] K. P. Kaliyamurthie, R. Udayakumar, D. Parameswari and S. N. Muguthan , "highly secured online voting system over network", 4833 Indian Journal Science and Technology Print ISSN: 0974-6846 Online ISSN: 0974-5645 Vol 6 (6S) May 2013.

[10] Gianluca Dini "Increasing Security and Availability of an Internet Voting System", Proceedings of the Seventh International Symposium on Computers and Communications (ISCC'02) 1530-1346/02 $17.00 © IEEE 2002.

[11] Xun Yi, EijiOkamoto, "Practical Internet voting system", Journal of Network and Computer Applications 36 378–387 2013.

[12] Alexander. Stakeholders: Who is your system for? IEEE: Computing and Control Engineering, 14(1):22 26, April 2003.

[13] David, C., C. Claude, peau, and D. Ivan. (Multiparty Unconditionally Secure Protocols.), in Proceedings of the twentieth annual ACM symposium on Theory of computing. Chicago, Illinois, United States: ACM, 1988.

[14] A. Rasouli et al. (A Robust and High Speed E-Voting Algorithm Using ElGammel CryptoSystem), in The 2nd

International Conference on Computer and Automation Engineering (ISI Indexed). 2010.

[15] R. Küsters et al. (Clash Attacks on the Verifiability of EVoting Systems), in IEEE Symposium on Security and Privacy (S&P)2012.

[16] Goldreich, Micali and Wigderson (How to play any mental game), in Proceedings of the 19th Annual ACM Symposium on Theory of Computing, pages 218-229, ACM, 1987.

[17] Damgård I, Groth et al. Secure electronic voting, Chapter 6, Kluwer Academic Publishers, 77–99 2011.

[18] Riera A, and Brown P. Bringing confidence to electronic voting, EJEG, vol 2(1) 2014.

[19] Lin Y, and Chlamtac I . Wireless and mobile network architectures, Wiley Publications 0–99 2000.

[20] Baron R J . Mechanisms of human facial recognition, International Journal of Man-Machine Studies, vol 15, 137–178 1981.

[21] Cardinaux F, Sanderson C et al. User authentication via adapted statistical models of face images, IEEE Transactions on Signal Processing, vol 54(1), 361–373 2006.

[22] Lee K-C, Ho J et al. Acquiring linear subspaces for face recognition under variable lighting, IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI), vol 27(5), 684–698 2005.

[23] M. Johns, B. Engelmann, and J. Posegga. Xssds: Server-side detection of cross-site scripting attacks. In Proceedings of the 2008 Annual Computer Security Applications Conference, ACSAC '08, pages 335–344, Washington, DC, USA, 2008.

Daljeet Singh received his b-tech degree in Computer Science and Engineering from Punjab Technical University, Jalandhar, Ludhiana, Punjab, India, in 2008, the M-Tech, degree in computer science and engineering from Punjab Technical University, Jalandhar, Guru Nanak Dev Engineering College, Ludhiana, Punjab, India in year 2012. He is an assistant professor at present, with department of computer science and engineering, in Guru Nanak Dev Engineering College. His research interests under Phd. in computer science and engineering include software engineering, software metrics, UML, object oriented paradigm (e-mail: gndecds@gmail.com).

Karanvir Singh is a research scholar in the Computer Science and Engineering department of the Guru Nanak Dev Engineering College, Ludhiana, Punjab, India. He is in the final year of is B Tech degree. His research interests include web designs and web application optimization. (e-mail: karanvir9719@gmail.com)

Jaskaran Singh is a research scholar in the Computer Science and Engineering department of the Guru Nanak Dev Engineering College, Ludhiana, Punjab, India. He is in the final year of is B Tech degree. Her research interests include web development. (e-mail: jass181997@gmail.com)

Khushpreet Kaur is a research scholar in the Computer Science and Engineering department of the Guru Nanak Dev Engineering College, Ludhiana, Punjab, India. She is in the final year of is B Tech degree. Her research interests include web designs. (e-mail: sidhukhushi22@gmail.com)