Diminishing Cyber stalking and Cyber bullying Issues using a Hashing Approach and Rail Fence Technique

Narander Kumar[1] and Priyanka Chaudhary[2]

Dept. of Computer Science
B. B. A. University (A central University) Lucknow, India

Abstract: With the advancement of technology, number of individuals who can get to and utilize technology, cyber stalking is a crime expanding in common over the cloud. Cyber Stalking is an example of pattern after some time in which a stalker looks to access, or control over a martyr. Such activities range from the favorable to the noxious and may bring about enthusiastic misery or damage to the victim. The foremost goal of this paper to upgrade the security, diminishing issues of cyber stalking. In this paper, we have proposed an algorithm which is established using bcrypt hashing and rail fence transposition method for password security.

Keywords:; Cyber Security; Cyber Stalking; Bcrypt Hashing Algorithm; Rail fence Technique, Cyber Criminals

1. Introduction

With the advancement of the utilization of the Internet, cyber security has become a major involvement toward clients and organizations alike. While communication advances have without a doubt emphatically changed the way we impart, it additionally gives cyber criminals strategies and systems to be utilized for illegitimate purposes, for example, distribution of obnoxious and undermining materials [1], spamming, phishing, cyber bullying, infections, provocation and cyber stalking [2]. Cyber stalking is a confounded and unavoidable issue, which influences and focuses on an enormous number of people [3], and dissimilar to numerous different cybercrimes, cyber stalking does not happen in a solitary event [4], rather casualties encounter rehashed, precise and various assaults. Cyber stalking has been distinguished as a developing social issue [5], and a worldwide issue [6], to a degree in which it is conceived that very nearly 20% of individuals at one phase of their lives will turn into a casualty of cyber stalking, where the ladies will more probably turn into a casualty than men [7,8]. Maple et al. have characterized cyber stalking as a "course of activities that include more than one occurrence executed through or using electronic implies that cause misery, dread or alert". There is confirmation that cyber stalking will increment in both recurrence and power [9]. While cyber criminals, for example, cyber stalkers use a variety of advancements, devices and strategies like talk rooms, notice loads up, newsgroups, instant message (IM), short message benefit (SMS), interactive media informing administration (MMS), and trojans, email is a standout amongst the most generally utilized techniques for cyber stalking [10, 11]. A cyberstalker can send messages, SMS, IM, MMS, and talk to undermine, disgrace, intimidate, or upset email communication by flooding a martyr's email inbox with undesirable mail [12,13] anyplace whenever unidentifiedly or pseudonymously without dread of indictment. This makes another test for law requirement and in the advanced forensic examination. Anonymity in communication is one of the principle issues misused by cyber criminals [14]. Along these lines, cyber stalkers could without much of a camouflage themselves by spoofing email, and making a diverse alias for the most part of free web mail suppliers. So also online portals are used to spoof SMS [15], and diverse unknown visitors IDs are effectively made. The act of cyber bullying or cyber stalking is not constrained to children or young people, the practice is perceived by a similar importance when it is finished by grownups moreover. The complexity in age group alludes to this online abuse as cyber stalking when

submitted by grownups towards grownups. The regular procedure utilized by cyber stalkers or cyber bullies is an expert out in the opening stages, long range informal communication destinations or online information locales and are proposed to threaten an objective's pay, notoriety, protection, security or business. Direct may include inducing others to irritate the objective and attempting to impact a martyr online collaboration

Cyber security is an extensive problem for business associations and people alike. The Internet has progressively turned into a stage for online predators, wherein one gathering in a relationship looks to control, abuse, exfloit, or hurt the other party by molestation. Cyber stalking is the merging of stalking and the internet wherein over a time frame the stalker gain access and control to a martyr. Cyber bullying is the rehashed, purposeful and frequently mysterious act done to hurt someone else through instant messages from a mobile phone, email, person to person communication sites, talk rooms, and prompt informing. It can be submitted by a solitary individual or a posse of individuals. Anybody can turn into an objective of cyber stalking. Cyber bullying more often than not alludes to children or youths being the victim or targets—all the more particularly understudies of open or non-public schools are the martyr. At the point when cyber bullying incorporates watching somebody quickly, taking after and focusing on individuals' online exercises, it is called as cyber stalking.

Different encode technique, cryptographic convention and cryptography technique are utilized to secure password and information exchange. In the event that putting away password in a plain content or is traded off through simple encryption strategy, then there is the potential outcome of unscrambling of the password and stolen. To protect and secure information and secret key SHA256, SHA512, RipeMD, and WHIRLPOOL are cryptographic hash strategies can be utilized. Hashing password is a better strategy , then encryption of password because in one way approach – we can't recover a plain content regarding from its hash [16] suggest the plain password that assembles a hash can't be recovered from its hash value. Hashing is delicate to the dictionary assault. Dictionary assault is a strategy for recuperating secret key from known password. So it is conceivable to split hash secret key by utilizing pre-figured hash esteem or utilizing hash word reference. Hashing method is extremely deterministic as they deliver same hash regarding for same information content. Crude hashes are more ever helpless against rainbow tables, a strategy for adjusting a requirement for pre - calculation of hashes and the clearly huge amount of capacity is important to keep a whole word reference of hashes [16].

2. Review of Work

Simran kaur recommends an approach, malware detection of clone and achieve better outcomes and the approach adopted is an implementation of a clone detection approach is such as ‘String Pattern Back Propagation [17]. Rajesh Panda is planned with a specific end goal of various types of determinants such as ‘online transaction’ intentions’ of shoppers. This also tries to take in how the determinants of online shopping in India are different from the global context [18]. M.L. Mazurek et al., depict our information accumulation methodology, especially the numerous insurances we took to reduce uncertainty to clients. We then break down how guessable the gathered passwords would be, amid an offline assault by subjecting them to a state-of-the-art password splitting algorithm [19]. P. G. Kelley et al. dissect 12,000 passwords gathered under seven arrangement approaches through an online study. We build up a valuable distributed technique for computing how valuably a few heuristic password assumption algorithm surmise passwords. Utilizing this strategy, we examine (a) the resistance of passwords made under various conditions to speculating; (b) the execution of speculating calculations under various preparing sets; (c) the relationship between passwords expressly made under a given piece approach and different passwords that happen to meet the same necessities; and (d) the relationship between guess ability, as measured by the password splitting technique, and entropy gauges. Our discoveries advance comprehension of both secret key structure strategies and measurements for evaluating

password security that is described in [20]. P. Kevin Dyer, describe the primary far reaching assessment of an extensive arrangement of DPI frameworks from the perspective of protocol misidentification assaults, in which enemies on the systematic endeavor to drive the DPI to mislabel connections. This approach utilizes different types of cryptographic primitive known as format, transforming encryption technique which augments conventional symmetric encryption technique with the ability to change the cipher text into an arrangement of our choosing text [21]. M. Dürmuth, assess the security of PBKDF2 against password speculating assaults utilizing state-of-the-art parallel processing models, with the objective to discover the parameters for the PBKDF2 that will ensure against today's assaults. Specifically, they grew quick usage of the PBKDF2 on FPGA-cluster and GPU-clusters [22]. R. Mordinyi examines the difficulties of forming related model perspectives amid the building of CPPSs to accomplish a mechatronic view on the designing antiques. Taking into account true cases, they examine (a) the qualities and constraints of best-practice approaches in CPPS building and (b) how software engineering commitments can give the establishment to viably tending to the test of forming building model components to give a mechatronic view. From this investigation, they infer research issues for future work [23]. A Web based research project is designed for wireless mobile network security and protection structure that is fixated on the ideas of omnipresent social insurance administrations gave to the patients in rustic or remote territories from inaccessible healing centers. With this framework system, a doctor can safely get to and convey the patient data from a cell phone overhaul the patient in-arrangement disconnected on the cell phone and synchronize the information with the server at a later time [24]. An approach in advancement is discussed in [25], towards outlining effective security messages concentrating on passwords rules. This underlying review showed the absence of enticing components in the present secret key rules may prompt unmotivated conduct of delivering great passwords. This paper additionally incorporates introductory results acquired from the pilot study, which uncover promising results supporting the use of influence techniques to enhance the present state data security compliance. An agenda is defined in [26] for a Facebook Watchdog application pursuing the expect to identify the aforementioned dangers to enhance the circumstance. The danger signs are dictated by picture investigation, online networking examination, and text mining procedures with a specific end goal to bring issues to light about continuous assaults and to give help to further action. An approach is defined with three dictionaries based secret key [27] recovery technique that utilizes both MPI and CUDA. In this approach the hashed estimations of known words are registered and contrasted and hash estimations of obscure client passwords. The algorithm contrasted in GPU memory use and how the information was separated and disseminated among the MPI hubs and GPU gadgets. An isolated word reference technique split the dictionary of potential passwords over the GPUs and replicated the secret key database to each GPU. A separated password database technique splits the secret key database and replicated the potential passwords. A minimal memory approach has split the password database and consecutively handled to the individual passwords on the GPUs. An approach is discussed in [28] in which contrast PTP and some normal secret word arrangements. On account of this, a few imperfections of PTP are resolved. A change of PTP is proposed to alleviate its fault. The change is actualized by joining PTP with a password approach. The exploratory results demonstrate that the new form of PTP is superior to the first form in both security and usability. An approach is defined they investigate the passwords of the understudies from the Faculty of Tourism and contrast outcomes. They gathered the information by method for an online survey, performed among undergrad and graduate understudies. In spite of our endeavors to teach the clients about the significance of the incessant secret key change, a huge percent of clients did not change their passwords taking after the addresses. [29] A survey is proposed one of which got password security data and an activity to fortify it. This study recommends compelling ways that trainer or employer can enhance

consistent with secret word rules. Specifically, preparing projects ought to mean to improve IS security adapting evaluation. The examination model proposed in this study has additionally been appearing to be a valuable model for clarifying IS security behavioral intentions [30]. The proposed exploration is a way to deal with upgrade the current Graphical Password strategies and oppose against assaults like Shoulder Surfing. This framework can be enhanced to give a more extensive password space if more server variables are included. A Study on the strength of the framework against Sniffing can be recommended for further study [31]. Tamilarasi R et al. scheduled an approach using Three-Tier method for providing improvised information secureness and protection along with high level of data security, verification, and confidentiality and avert information leakage utilizing segmentation and CSA. [32]

From an existing review of the work we have find some vulnerabilities Salt guarantees that intruders can't use a specific assault like as a lookup table and rainbow tables to break huge amount of hashes quickly, however, it doesn't keep them from running dictionary or brute-force attacks on each and every hash independently.

2.1 Brute Force Attack At the moment that a brute force assault to every conceivable arrangement of characters up to a given length. This sort of attack is computationally extreme, and is all things considered the base master concerning as hashes broke per processor time, nonetheless they will constantly thus execute the password.

2.2 Salt Collision Salt collision arises when two passwords encoded using with associated same salt value. For creating dictionary attack an interloper can be assembled by ciphered passwords through the salt and hash every last candidate secret word from a dictionary just per salt. The result speedup can be resolved as Number of secret word Number of Different salt. In the case that salts are delivered with an arbitrary number generator the acknowledged number of different salts for n password passages with s salts is

$$\mathrm{EV}(n,s)=\sum_{i=0}^{n-1}\left(\frac{s-1}{s}\right)^{i}=s-(s-1)^{n}\,s^{1-n}$$

3. Proposed Method

In this technique we have proposed security algorithm for password using Bcrypt algorithm and Rail fence technique.

3.1 Bcrypt Algorithm

BCRYPT is a key derivation method for passwords created by Niels Provos and David Mazières, depend on the Blowfish cipher, and displayed at USENIX. At the same time coordinating a salt that gives security appreciation to a rainbow table assaults, CRYPT is a versatile capacity after some time the emphasis cycle could be extended to make it slower, subsequently it stays impervious to brute force attack even with growing computational force. The Bcrypt algorithm is the default password hash technique for BSD and various diverse frameworks. The prefix value such as "$2a$" or "2y" that is utilized for hash string, i.e. set of character in a shadow password i.e. secret key file exhibits that hash string i.e. set of characters a Bcrypt hash specifically in a crypt format. Whatever remains of the hash string incorporates the cost parameter, a 128-bit salt and the 192 bit hash esteem. Blowfish is renowned among block cipher for its costly key setup stage. It begins off with sub-keys in a standard state, then uses this state to implement a block encryption utilizing part of the key, and uses the outcomes of that encryption to boost a portion of the sub-keys. At that point, it utilizes this changed state to scramble another part of the key and uses the outcome to change a greater amount of the sub-keys. It continues in this form, utilizing a logically changed state to hash the key and change bits of state until all sub keys have been set. Provos and Mazières built up another key setup method for Blowfish, naming the subsequent cipher "Eksblowfish". The key setup starts with altered types of the standard Blowfish key setup, in which both the salt and password have utilized to set all sub-keys. There are various rounds in which the standard Blowfish method has been

tested utilizing, on the other, hand the salt and the password as the key, each step beginning with the sub-keys state from the previous step. Crypto-hypothetically, this is no more active than the standard Blowfish key schedule, yet the quantity of rekeying rounds is configurable; this procedure can consequently be made arbitrary slow that is has provided service to brute force attack upon the hash or salt. BCRYPT is right now becomes the most secure standard for password hashing. It's derived from the Blowfish block cipher which, to generate the hash, uses lookup tables which are initiated in memory, i.e. specific amount of memory ought to be utilized for space requirement before a hash could be produced. This should be possible with CPU, however, when utilizing the force of GPU it will end up being significantly bulkier because of memory limitations. Bcrypt has utilized around for a long time, in the form of a cipher which is used around for more than 2 decades.It's been all around confirmed and tried and subsequently considered the standard for password hashing. There is really one shortcoming, FPGA processing units. At the point when bcrypt was initially built up its principle danger was custom ASICs particularly worked to assault hash method. Nowadays, those ASICs would be GPUs which are cheap to buy and are perfect for multithreaded procedures, for example, password brute forcing. FPGAs (Field Programmable Gate Arrays) is like GPUs, however, the memory management is altogether different. On these chips brute forcing bcrypt should be possible more efficient than on GPUs, however, you have a sufficiently long password it will, in any case, is unfeasible. The emphasis number is a power of two, which is a contribution to the calculation. The number is encoded in the textual outcomes

The general work process for record enlistment and validation in a hash-based record framework is as per the following:

- The user sign up an account.
- Hashed their pass code and after that entered in the database. At that time the plain-message pass code ever kept on the hard drive.
- At that point when the front end user login, the hash of the secret key, they entered and checked against the hash of their genuine secret key
- On the off chance that the hashes coordinate, the client is allowed access. If not, the client is told they entered invalid login accreditations.
- Phase 3 and 4 rehash each time somebody tries to login to their air conditioning tally.
- In phase 4, never tell the client on the off chance that it was the username or secret word they got off-base. Continuously show a non specific message like "Invalid username or password." This keeps aggressors from listing substantial user names without knowing their passwords.

3.2 Rail Fence Technique

The Rail Fence Technique is most simple transposition method. This procedure includes composing plain content as a grouping of analysis and understanding it row by row to create the encoded content. An illustration is demonstrated as follows. The plain content is HELLO and the figure content is HLOEL.

Plain text	H	E	L	L	O
Cipher text	H		L		O
		E		L	

.

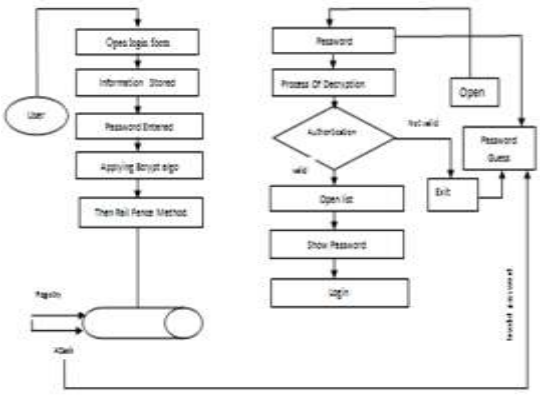

Fig. 1. Flow Chart of Proposed Algorithm

In Proposed model is characterized in fig 1.User opens the login page. Store client data in list and data incorporates the client name, password, and the vital data with a password. We apply Bcrypt hashing method. Subsequent to applying Bcrypt hashing we utilize rail fence method. The release will be saved in windows registry. The Client can open his list by entering a substantial password. Apply unscrambling and it will verify the client and offer access to the list.

4. Implementation

We designed our proposed algorithm using with NetBean IDE 8.0 software. The below figures defines the implementation of the proposed algorithm by using different numbers of text data values and sizes of a wide range.

Fig. 2. Login Page

Fig. 3. Bcrypt hashing Algorithm

Fig. 4. Rail Fence Technique

5. Result and Discussion

From the outcome indicated database password security utilizing hashing and salting design gives a more grounded security with the end goal that the first password has never put away. Regardless of the possibility that the password store is traded off, just the hashes get to be distinctly open. The mystery word length is not put away and can't be assessed, making secret word splitting that much harder. There is no requirement for a secret as none is utilized to hash the password. For multi-client conveyed applications, the secret word hash can be utilized for verification. While using encryption, password should be conveyed or the password must be imparted to play out the verification toward the front.

The performance metrics are shows encryption time and throughput time. The encryption time is defined as, the time is taken for generating a cipher text from plain text.

$$Througput = \frac{Size\ of\ Encrypted\ Text\ in\ MB}{Time\ Required\ for\ Encryption\ in\ Seconds}$$

Fig. 5. shows the encryption time of proposed algorithm and Fig. 6. shows the throughput time of the proposed algorithm**.**

6. Conclusion

Security and validness are the two noteworthy areas of the overall system.

These drawbacks are enlightened with the investigation of cryptography. Password stockpiling security is one fundamental piece of data assurance as most structure now these days require an approval system utilizing passwords Regardless, with time, assaults have got the opportunity to be conceivable over the utilizing of dictionary tables and rainbow tables.

Table 1. Execution Time for Proposed Algorithm

Dataset (character)	Proposed Algorithm Execution Time (Microsecond)
Data 1	2589
Data 2	2856
Data 3	3074
Data4	3429
Data5	3763
Data 6	3982

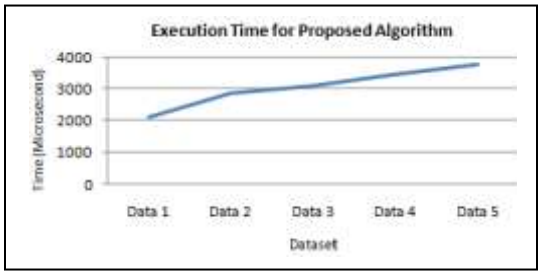

Fig. 5. Execution Time for Proposed Algorithm

In this paper, we endeavored to make solid password management more helpful. While previous technique were inadequate in either transportability for versatile clients or security against brute force attack, we outline accomplishes an adjust of the two by utilizing password reinforcing methods.

Table 2. Throughput of Proposed Algorithm

Dataset (character)	Data (MB)	Execution Time (second))	Throughput
Data 1	.000969	.0025	.3876
Data2	.000996	.00285	.3494
Data 3	.000955	.00307	.3110
Data 4	.000990	.00342	.2894
Data 5	.001098	.00376	.2920

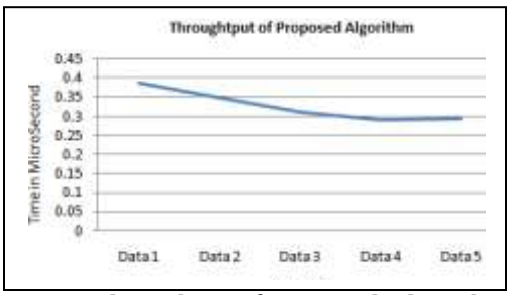

Fig. 6. Throughput of Proposed Algorithm

References

1. O. D. Vel, A. Anderson, M. Corney, G. Mohay. Mining E-mail Content for Author Identification Forensics. In: Proc ACM Sigmod Record, 2001. p. 55–64.
2. K. Reynolds, A. Kontostathis, L. Edwards. Using Machine Learning to Detect Cyberbullying. In: Proc IEEE ICMLA, 2011. p. 241–244
3. M. Baer. Cyberstalking and the Internet Landscape We Have Constructed. Virginia Journal of Law & Technology 2010;153-227.
4. J. L. Truman. Examining intimate partner stalking and use of technology in stalking victimization. PhD thesis. University of Central Florida Orlando, Florida, 2010.
5. B. L. Ellison, Y. Akdeniz. Cyber-stalking: the Regulation of Harassment on the Internet. Criminal Law Review 2001;29–48.
6. A. Maxwell. Cyberstalking. Technical Report 7, Auckland University, 2001.
7. D. A. Jurgens, P. D. Turney, K. J. Holyoak. SemEval-2012 Task 2: Measuring Degrees of Relational Similarity. In: Proc of the First Joint Conference on Lexical and Computational Semantics, 2012. p. 356–364.
8. C. Maple, E. Short, A. Brwon, C. Bryden, and M. Salter. Cyberstalking in the UK: Analysis and Recommendations. International Journal of Distributed Systems and Technologies, 2012; 34–51.
9. N. Parsons-pollard, L. J. Moriarty. Cyberstalking: Utilizing What We do Know Victims and Offenders 2009; 435–441.
10. L. Roberts. Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: An Analysis on Cyber Stalking. International Journal of Cyber Criminology 2008; 271–285
11. A. Maxwell, Cyberstalking. Technical Report 7, Auckland University, 2001.
12. C. Southworth, J. Finn, S. Dawson, C. Fraser, and S. Tucker. Intimate partner violence, technology, and stalking. Violence against women 2007;842–856.
13. L. L. Sheridan, T. D. Grant. Is cyberstalking different? Psychology. Crime & Law, 2007;627–640.
14. R. Hadjidj, M. Debbabi, H. Lounis, F. Iqbal, A. Szporer, and D. Benredjem. Towards an integrated e-mail forensic 2009;124–137.
15. A. Bose and K. G. Shin. On mobile viruses exploiting messaging and Bluetooth services. In: Proc 2006 Securecomm and Workshops, IEEE, 2006 p. 1–10.
16. P. Sriramya, R. A. Karthika. Providing Password Security by Salted Password Hashing Using Bcrypt Algorithm. ARPN Journal of Engineering and Applied Sciences 2015;5551-5556.
17. Simarleen Kaur, Arvinder Kaur. Detection of Malware of Code Clone using String Pattern Back Propagation Neural Network Algorithm. Indian Journal of Science and Technology 2016;1-9.
18. Rajesh Panda, Biranchi Narayan Swar. Electronic Retailing: A Review of Determinants of 'Online Shopping Intentions' in India. Indian Journal of Science and Technology 2016;1-6
19. M.L. Mazurek et al.. Measuring Password Guessability for an Entire University. In: Proc. 2013 ACM Conf Computer and Communications Security (CCS 13), 2013. p.173–186.
20. P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas,L. Bauer, N. Christin, L. F. Cranor, and J. Lopez. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In; IEEE Symposium on Security and Privacy, 2012. p. 523– 537.
21. Dyer, Kevin P., Scott E. Coull, Thomas Ristenpart, and Thomas Shrimp- ton. Protocol misidentification made easy with

format-transforming encryp- tion. In: Proc ACM SIGSAC conference on Computer communications security, 2013. P. 61-72.
22. M. Dürmuth, T. Güneysu, M. Kasper, C. Paar, T. Yalçin, and R. Zimmermann. Evaluation of Standardized Password-Based Key Derivation against Parallel Processing Platforms. In Computer Security – ESORICS 2012; 716–733.
23. R. Mordinyi, S. Biffl. Versioning in Cyber-physical Production System Engineering - Best-Practice and Research Agenda. In: Proc IEEE/ACM 1st International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS), 2015. p. 44-47.
24. W. D. Yu, R. Gummadikayala, S. Mudumbi. A web-based wireless mobile system design of security and privacy framework for u-Healthcare. In: Proc 10th International Conference on e-health Networking, Applications and Services HealthCom , 2008. p. 96-101.
25. N. H. Zakaria, N. Katuk. Towards designing effective security messages: Persuasive password guidelines. In: Proc International Conference on Research and Innovation in Information Systems (ICRIIS*)*, 2013. p. 129-134.
26. M. Rybnicek, R. Poisel, S. Tjoa. Facebook Watchdog: A Research Agenda for Detecting Online Grooming and Bullying Activities. In: Proc IEEE International Conference on Systems, Man, and Cybernetics, 2013. p. 2854-2859.
27. D. Apostal, K. Foerster, A. Chatterjee and T. Desell. Password recovery using MPI and CUDA. In: Proc 19th International Conference on High Performance C omputing (HiPC), 2012. p. 1-9.
28. T. T. T. Nguyen, Q. U. Nguyen. An analysis of Persuasive Text Passwords. In: Proc 2nd National Foundation for Science and Technology Development Conference on Information and Computer Science (NICS), 2015. p. 28-33.
29. V. Taneski, M. Heričko, B. Brumen. Impact of security education on password change. In: Proc 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO*)*, 2015. p. 1350-1355.
30. F. Mwagwabi, T. McGill, M. Dixon. Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines. In: Proc 47th Hawaii International Conference on System Sciences, 2014. p. 3188-3197.
31. S. Farmand, O. B. Zakaria. Improving graphical password resistant to shoulder-surfing using 4-way recognition-based sequence reproduction (RBSR4). In: Proc 2nd IEEE International Conference on Information Management and Engineering (ICIME), 2010. p. 644-65
32. Tamilarasi R, Prabu S,. Swarnalatha P. An Approach for Data and Image Security in Public Cloud using Segmentation and Authentication (CSA) Protocol Suite. MAGNT Research Report 2015. 133-141.