Journal of Engineering and Applied Sciences 13 (15): 5971-5975, 2018
ISSN: 1816-949X

Administering Substantial Security for Data Using Bits-Conversion, Stuffing and Shuffling Algorithm (Bits-CSS)

[1]C. Thangamalar and [2]K. Ravikumar
[1]Research and Development Centre, Bharathiar University, 641046 Coimbatore, India
[2]Department of Computer Science, Tamil University, Thanjavur, India

Abstract: The expeditious internet development nowadays emerges with constant speed. Conventional methods used for detection and defending of attacks from malicious software should be more efficient and have to handle emerging attackers and their new methodologies used for hacking data. Data transmission prone to be hacked by the intruders shall be secured using cryptography techniques. In our proposed study, we provide security using conversion of images or text into binary digits (bits). Then it undergoes three level measure by converting data into bits, stuffing up spaces in between bits and amend the whole set of binary data as 8 bit and ensures that should be divisible by 8 if not then the remaining digits will be added. Store all the converted and stuffed data in a notepad by shuffling binary digits format of data as metadata in it. Thus, this algorithm provides substantial security for data.

Key words: Data transmission, detecting and defending attacks, hacking data, binary digits (bits), binary conversion, shuffling

INTRODUCTION

The issues around statistics confidentiality and privacy are beneath more recognition than ever earlier than as ubiquitous internet get access to exposes crucial corporate information and personal facts to new safety threats (Oberheide *et al*., 2008). On one hand, information sharing across distinct parties and for special functions is important for many programs which includes native security, medical studies and environmental protection. The availability of “huge facts” technology makes it viable to speedy examine massive facts sets and is for this reason in addition pushing the large collection of records (Rozas *et al*., 2009). On the other hand, the combination of more than one datasets might also allow parties retaining these datasets to deduce sensitive information.

Pervasive statistics amassing from a couple of records sources and devices along with smart telephones and clever strength meters in addition exacerbates this tension. Techniques for first-class-grained and context-primarilybased get entry to control are crucial for achieving information confidentiality and privacy (Wang *et al*., 2010). Depending on the particular use of records, e.g., operational functions or analytical purposes, information anonymity strategies may additionally be implemented.

An essential challenge on this context is represented by way of the insider risk this is and records misuses with the aid of people who have get permission to facts for carrying on their organizational features and thus own the essential authorizations to access proprietary or touchy information (Salah *et al*., 2013). Safety towards insider requires now not simplest fine-grained and context-based get right of entry to manage but additionally anomaly detection systems, able to discover uncommon patterns of information get entry to and statistics consumer surveillance systems, capable of reveal user moves and behavior in cyber area B as an instance whether a statistics person is lively on social networks.

It is aware that the adoption of anomaly detection and surveillance systems entails records consumer privacy problems and consequently a task is how to reconcile records safety with statistics consumer privacy. It’s much important to factor out that when dealing with facts privacy, one has to distinguish between records topics that is the users to whom the facts is associated and data users this is the users having access to the information. Privacy of both classes of consumer is important, despite the fact that only few techniques were proposed for information consumer privacy.

Data safety is not but constrained to information confidentiality and privacy. As statistics is regularly used for critical choice making, facts trustworthiness is a crucial requirement. Information wishes to be protected from

Corresponding Author: C. Thangamalar, Research and Development Centre, Bharathiar University, 641046 Coimbatore, India

unauthorized adjustments (Huang *et al*., 2011). Its rovenance need to be available and licensed. Records ought to be accurate whole and up-do-date. Comprehensive data trustworthiness answers are difficult to achieve as they want to combine unique techniques such as virtual signatures, semantic integrity, statistics exceptional techniques as properly taking into account information semantics. Observe also that assuring data trustworthiness may also require a tight manage on data control methods which has privacy implications.

Literature review: The anti-attack software program has been popularized but the virus software has not been successfully curbed and on the opposite the virus infection fee has been rising. In view of the hindrance of conventional virus detection strategies, many students have put forward the techniques of virus detection primarily based on cloud computing. The development of foreign related technology is extra mature. A new idea turned into put forward first of all the robust dispensed parallel processing capability of cloud computing become used to transplant the work of virus detection and evaluation into the cloud computing to hold on, the evaluation and testing of the executable files have been finished in the cloud (Blasing *et al*., 2010).

Intel organization further improved the approach, a whole version of cloud virus detection changed into proposed, it delivered an archive characteristic to keep the virus malware related features bin the report (Yan and Wu, 2009).

Xu *et al.* (2010) used the cloud computing generation to make up for the shortcomings of the conventional virus detection strategies and extended the generation to the navy network and was given good consequences.

Salah *et al.* (2013) proposed a reliable model, the version no longer handiest should detect malicious virus software program, however also could offer effective intercept service for dispensed spam DDOS, the overall performance of the gadget turned into improved (Yi, 2015).

A new kind of MD5 research technique is proposed which progress the performance of virus malware detection. The antivirus malware detection turned into prolonged to the cellular devices and an android software sandbox gadget become proposed, it is able to keep on the dynamic and static detection of the suspicious documents (Deng, 2014).

Compared with the highly mature research abroad, home associated research began late. At present, virus malware regularly makes use of the code confusion era; antivirus software program often can't locate the contents of the file. As a way to effectively minimize the development of such viruses and malicious software, many students have made a quite effective strive.

The malware signature automatic detection gadget AMSDS changed into proposed, it became smaller than the traditional signature database and in virus detection model, users handiest had to installation a lightweight cloud signature collection while the AMSDS couldn' t hit upon the file, it'd be mentioned to the cloud server (Weijie, 2015).

A version cloud SEC of cooperative protection machine turned into proposed, it is able to resist a big quantity of allotted intrusion and could be carried out to cooperative safety services within the cloud.

MATERIALS AND METHODS

Securing data transmission and protecting confidential data: The conceptual point of view, an access manage mechanism typically includes a reference screen that checks that asked accesses via. topics to covered system to carry out certain moves on these items are allowed in keeping with the get right of entry to manage guidelines. The choice taken by way of the access control mechanism is referred to as access manage decision. Of direction, as a way to be powerful access control mechanisms ought to guide fine-grained access control that refers to finely tuning the authorized accesses along distinctive dimensions such as facts item contents, time and area of the access, cause of the get admission to. With the aid of properly proscribing the contexts of the possible accesses you'll reduce flawed statistics accesses and the possibilities for insiders to steal records.

To cope with one of these requirement, extended permission to manipulation manner have been proposed which include time-based permission to manage models, region-based permission to manage system, reason-based access control to manipulate fashions and attribute-primarily based get entry to manage fashions that limit statistics accesses with recognize to time periods, places, reason of statistics usage and user identity attributes, respectively.

Despite the fact that the place of access to manage has been broadly investigated, there are many open research directions, consisting of a way to reconcile access manage with privacy and how to design access control way and mechanisms for social networks and cell systems. Many advanced access manage fashions require that data, together with the area of the user requiring get admission to or user identity attributes, be provided to the get admission to manipulate reveal.

The purchase of such records may additionally result in privacy breaches and the use of cloud for handling the records and enforcing access to manipulate regulations on the facts further will increase the risks for statistics users of being goal of phishing attacks. The undertaking is the way to carry out access to manipulate even as on the identical time maintaining the privacy of the person personal and context records.

Social networks and cell devices acquire a huge form of statistics about individuals consequently access manage mechanisms are to control with which parties this facts is shared. Additionally these days user owned systems are increasingly more getting used for process-related duties and as a consequence keep agency personal facts. The primary difficulty is that, not like traditional company environments wherein directors and different specialized staff are in rate of deploying access control to manipulate guidelines in social networks and mobile devices give up-users are in rate of deploying their own personal get right of entry to manipulate policies.

The primary venture is a way to make certain that devices storing agency exclusive information enforce the organization get right of entry to manage regulations and to make certain that un-depended on programs are not able to get right of entry to this facts. It's more important and vital to factor out that get admission to manipulate by myself may not be enough to guard records against insider danger as an insider may additionally have a valid permission for sure information accesses.

We provide confidential data protecting them from attackers and hackers. Therefore, it is critical to be able decide whether an access even although is granted through the access control to manage mechanism is "anomalous" with appreciate to statistics accesses standard of the activity characteristic of the statistics consumer and/or the standard statistics get entry to patterns. As an example, consider a user that has the permission to read an entire desk in a database and assume that for his/her task function, the user best needs to access some entries an afternoon and does so, at some point of working hours. With appreciate to such access control pattern and it is executed after workplace hours and ensuing in the down load of the entire desk could honestly be anomalous and desires to be flagged.

Internal structure with the maximum critical aspect is the community service part which takes at the challenge of reading suspicious files. The center of the community carrier is to determine whether or not the submitted suspicious documents are virus malware or regular files. unique from the current evaluation techniques, the cloud computing dispensed parallel surroundings is used inside the architecture, each submitted record is detected and analyzed through a fixed of detection engine with a view to determine whether or not the record is malicious files.

Bits-CSS algorithm implementation: The dynamic Binary digit conversion, stuffing and shuffling algorithm helps in substantial security over data while transmission. Data images and information to be transferred securely will be converted into binary digits that are 0's and 1's. Then the space between bits will be stuffed with alternate 0's and 1's. At last the whole bits will be scrutinized for its divisibility by 8. If the total bits count is not divisible by 8 then the remaining left over number will be stuffed with random bit generator. Once the binary digits match the number of bits it will be stored in the notepad (Fig. 1).

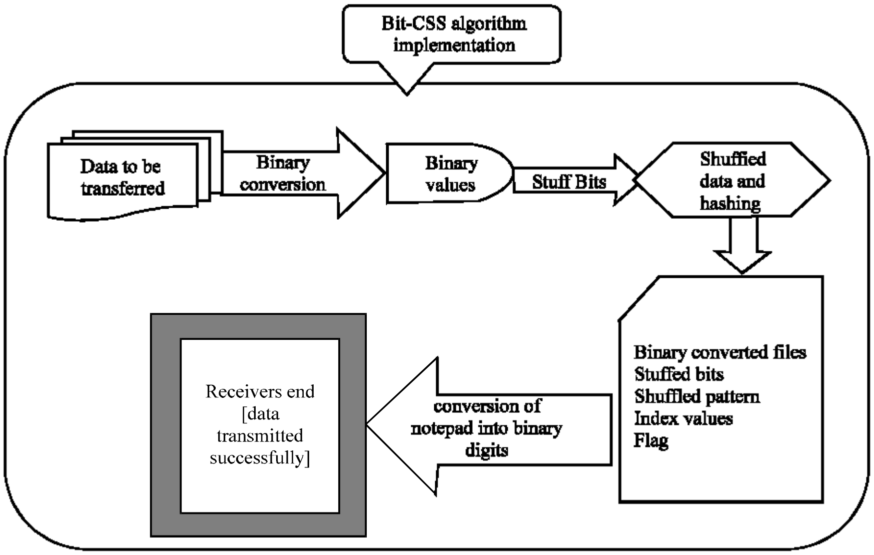
Bit-CSS algorithm implementation
Data to be transferred
Binary conversion
Binary values
Stuff Bits
Shuffled data and hashing
Binary converted files
Stuffed bits
Shuffled pattern
Index values
Flag
conversion of notepad into binary digits
Receivers end [data transmitted successfully]

Fig. 1: Bit-CSS algorithm implementation

The process of conversion into binary and stuffing of left digits to match the binary consistency is completed. After storing these converted bits into a notepad and it will be appended along with the data file. The data file will be sent with strongly secured and encoded binary digits. The disordered and bewildered binary data accumulated in the notepad will be further hashed and shuffled and that details also will be stored in notepad. Thus, when sending such binary converted notepads along with the file helps in the receivers end to be decoded.

The receiver only knows the trick to decode the data file. The algorithm applied is efficient and stubborn by which no intruder can get any valid information from the binary converted data and notepad files. The shuffling pattern, stuffed binary bit details, random binary digit generated and the number of hashing the bits undergone all the details to be hacked and decoded are terribly impossible for the attacker. Thus, we provide substantial security over data transmission.

When decoding the same steps to be followed in the reverse way. Along with each file the binary converted notepad will be appended which contains information such as:

- Binary pattern how data is converted
- The position of bits added in the binary space
- To make it divisible by 8 the random number stuffed
- Number of times hashing in implemented
- Number of times the notepad to be decoded is converted or shuffled
- Finally they have index values and flag to be set for finding the decode secrets involved

As the first step our proposed bits-CSS algorithm will decode the received file by finding the number of notepads appended in the data file. For this, we have to find the notepad binary files and then decode it to notepad values. Then with the above provided information from the decoded notepad the data extraction process begins. The index values will be taken into loop for considering the values and flag will be noted for the binary digits value. If the flag set to be 1 then the bit should be considered as it is else if it is 0 then the bit should be considered opposite.

Then the index value should be noted down for position of bits stuffed inside the data files and have to remove each bit and at last the random number generated for amending the binary values should also be removed. Now at this point, we are left with the binary values which again have one flag which shows what are the bits to be taken directly and what to be reversed its value. Then finally the bits will be reconverted to its original image format or way, we administer substantial security for data files to be transferred.

RESULTS AND DISCUSSION

Experimental and performance analysis: The binary digits to be transmitted along with the stuffed data will have certain consideration over binary value transformation. As the spaces in between are stuffed up the index values should be clearly list up the position. If the index value denotes 5th position then that should be taken as 6th position as the 5th value will be the stuffed up bit value by our algorithm. Thus, decoding of data files will be by calculating number of notepads and then decoding the notepad converted binary values.

The index values infused will be looped to decode the position of binary values from the converted binary digits (Fig. 2). Then the flag values will be checked for its direct or inversed data. Then the shuffled and hashed data will be decoded after that the extra values are removed from the stuffed bits. As the last procedure the processed binary values will be decoded and its original data transmitted will be generated.

The image and notepad conversion into binary values and shuffling them while sending through network will be an advanced technique and cannot be predicted by the attackers. Thus, we have substantial security provided for data transmitted which can never be hacked even if it is hacked the obtained information will be of no use without the decoding pattern algorithm. Thus, we have achieved efficient security provided.

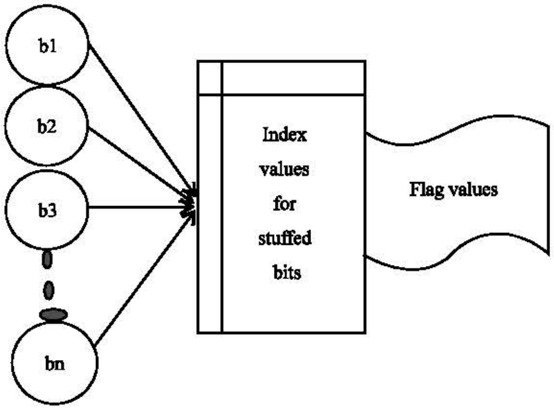

Fig. 2: Binary digits with index and flag values

CONCLUSION

In our study, we propose Bit-CSS that is binary digit-conversion, stuffing and shuffling algorithm to avert attacks or hacks over data transmission through web. By these three step process, we achieve unpredictable efficiency over security provided for data transmission. The reversal of process will not be that easy to be made by the intruders without proper algorithm implementation for it. Binary conversion and stuffing of extra bits to confuse attackers makes data hardly impregnable. We achieve strong and robust data transmission over internet for both image and text data.

REFERENCES

Blasing, T., L. Batyuk, A.D. Schmidt, S.A. Camtepe and S. Albayrak, 2010. An android application sandbox system for suspicious software detection. Proceedings of the 5th International Conference on Malicious and unwanted software (MALWARE'10), October 19-20, 2010, IEEE, Nancy, France, ISBN: 978-1-4244-9353-1, pp: 55-62.

Deng, P., 2014. Research on computer virus and its defense technology in network environment. Silicon Valley, 7: 83-84.

Huang, N.F., C.N. Kao and R.T. Liu, 2011. A novel software-based MD5 checksum lookup scheme for anti-virus systems. Proceedings of the 7th International Conference on Wireless Communications and Mobile Computing (IWCMC'11), July 4-8, 2011, IEEE, Istanbul, Turkey, ISBN:978-1-4244-9539-9, pp: 207-212.

Oberheide, J., E. Cooke and F. Jahanian, 2008. CloudAV: N-version antivirus in the network cloud. Proceedings of the 17th Symposium on USENIX Security, July 28-August 1, 2008, USENIX Association Berkeley, San Jose, California, USA., pp: 91-106.

Rozas, C., H. Khosravi, D.K. Sunder and Y. Bulygin, 2009. Enhanced detection of malware. Intl. Technol. J., 13: 6-15.

Salah, K., J.M.A. Calero, S. Zeadally, S. Al-Mulla and M. Alzaabi, 2013. Using cloud computing to implement a security overlay network. IEEE. Secur. Privacy, 11: 44-53.

Wang, X., T.L. Huang and Z.J. Ren, 2010. Notice of retraction research on the anti-virus system of military network based on cloud security. Proceedings of the International Conference on Intelligent Computing and Integrated Systems (ICISS'10), October 22-24, 2010, IEEE, Guilin, China, ISBN: 978-1-4244-6834-8, pp: 656-659.

Weijie, L., 2015. Study on the implementation path of network security technology in the background of cloud computing. Netw. Secur. Technol. Appl., 2015: 48-48.

Xu, J., J. Yan, L. He, P. Su and D. Feng, 2010. Cloudsec: A cloud architecture for composing collaborative security services. Proceedings of the IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom'10), November 30-December 3, 2010, IEEE, Indianapolis, Indiana, USA., ISBN: 978-1-4244-9405-7l, pp: 703-711.

Yan, W. and E. Wu, 2009. Toward Automatic Discovery of Malware Signature for Anti-Virus Cloud Computing. In: Complex Sciences, Zhou, J. (Ed.). Springer, Berlin, Germany, ISBN:978-3-642-02465-8, pp: 724.

Yi, W., 2015. Research on computer network security defense technology. Network Secur. Technol. Appl., 2015: 59-59.