JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

NETWORK INTRUSION DETECTION USING REGISTER TAG DISABLE FUNCTION SECURITY MODEL (RTDFSM) APPROACH

Dr A.Senthil kumar[1],

[1]Assistant Professor, Department of Computer Science, Tamil University, Thanjavur-613010,

erodesenthilkumar@gmail.com

Abstract

To determine a framework model which describes the registration purpose, assigning Tag-IDs and Disable functional mode thereby providing scalability issues that is specified as a novel approach for intrusion avoidance in the social networks. This research work suggests a model framework namely Register Tag Disable Function Security Model (RTDFSM), which provides "Data sharing" as the first motive to support the network technologies and provides "Data Security" that supports data sharing along with security benefits by assigning tag identification numbers (tag-ids), and Disable function process in order to detect the intrusions by fixing the data size and its time series to share process. A recent survey depicts that Facebook has at least 1.71 billion active users per month. In addition the survey has estimated that 400 million photos per day are being uploaded. The reason behind is the users adaptive behaviour of sharing. The security parameters are fixed and this model has achieved 70% level scalability in case of data storage and the time series maintenance processes when compared to other network security algorithms. The time series is analysed with the suitable 'disable function' say 'Df' when all the assigned tag and data is enabled for 'protected download' option. The increase in number of the function grows to a considerable percentage ranging from 10%, 20% upto 58% at the later stage. Computer networks are the fundamental platform for online transactions and sharing of information worldwide. Without Social Networks (SNs) such as Facebook, Twitter or Instagram, the real internet applications seem to be considered idle only for data processing and not for data sharing. The research work is a novel model named as "Register Tag Disable Function Security Model (RTDFSM)" that will enable user authenticity for every data sharing process in the network communication either in wired or in wireless media.

Keywords

Register Tag Disable Function, Disable Function, Fit Size, Time Series, Social networks.

1. Introduction

Security breaching is an incident in recent days due to communication media advancements and lack of awareness to handle a data in particular, social networks. The creation of an idea with its emotional thoughts are flavoured in photographs, images, pictures, audio and video data or any other mode of specification is subject to vulnerable with respect to its authentication measures. This research work suggests a novel model described as "Register Tag Disable Function Security Model (RTDFSM)" which will allocate a registration process for every user who wishes to share their data initially. The model frames a separate 'Tag-Info' notation which denotes a unique number which will be assigned randomly for every user. The exact data with respect to its size and time of every sharing is calculated by a disable function say 'f' which will compare the sender and receiver authentication with respect every login process and sharing communication in the networks. Any vulnerable identity within the analysing of disable function is subject to be quarantined and the model set back the sender thereby claiming new authentication procedures. The first phase shows the registration process of every user since the novelty in analysing every user is a mandatory method. For every problem specification the system architecture is essential and this model also frames an architecture involving every user and their process though an input output specifications. The security model finally achieves 70% level of scalability by comparing other network security algorithms dynamically and stands a novel model for detecting the intrusions. The model is framed by analysing previous literature research papers and a new novel method is described in this research paper.

2. Literature Review

In the article cited 'Privacy preserving photo sharing on a secure JPEG [1]" the authors described the JPEG framework which is fabricated on protected JPEG framework that incorporates various tools to protect photo privacy. There are various tools to ensure the image privacy such as filtering, encryption, scrambling. In this proposed work, general crawling is described to secure a metadata and cryptographic principles are depicted for any communicated data within network users. The problem specifies an architecture server based on data uploading process with its host thereby mentioning their geographic locations and the automatic identification of data enrolled and uploaded are analysed in the JPEG file format itself. Some of image manipulating methods are utilized in this approach. The next literature paper named as "Collaborative Face Recognition for Improved Face Annotation in Personal Photo Collection [2]" by their authors has provided a distributed method in order to perform certain idenficational and verificational measures in the data with respect to a centralized model. The model undergoes a video surveillance based technique that queries a face image as the photo i.e data and compares other relevant photographic images with new facial recognition methods. Lastly, the difference in the data extraction is identified by various amounts of annotations with different collections. In the next method, the conditional random field models [3] with label specifications respect to web oriented applications are analysed with the machine learning approach and data produced with respect to images are measured.

The other method mentioning the title "The statistics of photo Sharing on social networks and propose a three realms Model [4]" identifies the real estimation of relationship existence in the images with respect to physical identity, visual sensor identity and the co-occurrence norms specified between images. In addition to this research work the next paper entitled, "The contextual information in the social realm and cophoto relationship to do automatic fr Stone[5]", has narrated the pairwise conditional random field model with measures the optimal joint label specifications over the image data. Further the work assumes the conditional density maximization principle also within the data images and provides certain samples that are analysed based on some statistical and baseline principles.Improving the accuracy of face annotation by effectively making use of multiple FR engines available in an OSN. Their collaborative FR framework consists of two major parts: selection of FR engines and merging (or fusion) of multiple FR results. The selection of FR engines aims at determining a set of personalized FR engines that are suitable for recognizing query face images belonging to a particular member of the OSN. For this purpose, they exploit both social network context in an OSN and social context in personal photo collections.

These literature review papers has suggested that authentication based on image property can be analysed through suitable model specifications but the research gap identification is how the exact data is analysed in an individual manner than the grouping images is not specified. Hence this research model, "Register Tag Disable Function Security Model (RTDFSM)" narrates that unique data identification and assignment to them is possible thereby enriching security and detecting the intrusions accordingly. The next section depicts the architecture model framing the necessary constraints which will enable the structural method flow of data between the techniques.

3. Architectural Pitch

This section specifies the necessary model constraints in the diagrammatic representations stating the registration process which will enable every user to initially specify their log-in credentials for every transaction in the network. The user's authentications are stored in a specific database for revocations during implementation stage.

3.1. Registration Process

The Registration module contains User id and Password for new users. Here all the users whom are termed as the clients are registered one after another to undergo the process. The Registration module contains User id and Password [7] for new users. Here all the users whom are termed as the clients are registered one after another to undergo the process. The exact login identifications and passwords are noted specifically and their personal mobile numbers, email ids and other important contact information's are mentioned.

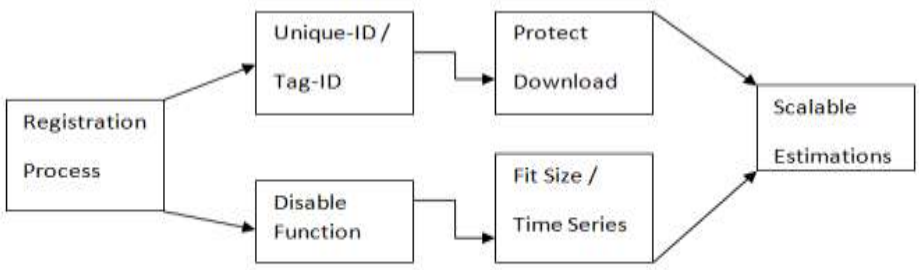

Figure 1 : Register Tag Disable Function Security Model (RTDFSM)

3.2. Unique-ID / Tag – ID Assignments

After the authentication process which is initiated from the registration process is completed, the unique-id or tag-id assignment to every individual user in the network is executed for every transaction with respect to the size of the data as well as the time of execution between the users. Alike the data file or the communication which means the data sharing file remains same in size it is assignment be a tag identification number(tag-id)[9] which is otherwise named as the unique-id is allocated and the process is repeated for every users who wishes to share their own data(photo) in the network. This process is repeated for every user who participates in the network until the end user hosts their own transaction which ends by his/her side. Meanwhile, the disable function says,

$$Df = rp(ur1/tg1+ur2/tg2 \ldots.. urn/tgn) <= NW \quad \text{--- equation 1}$$

Where 'Df' refers the 'Disable function', 'rp' refers – registration process, 'ur1' refers the user registered or numbered 1, 'ur2' refers the user registered numbered 2, 'urn' refers the end user or the last user in the network which must be authenticated or participated in the network say, 'NW'. Furthermore, the user one in the network is assigned by a specific authentic tag say, 'tg1' 'tg2' and 'tgn' respectively for all the nodes that are installed physically.

3.3. Disable function

The disable function say 'Df' in its context are executed until the node completes its initial transaction say file sharing or photo sharing or any application that are initiated in the system. This process is executed for all nodes and the function checks for manipulating the file size and the time of transaction initiated for a node say 'n1'. The second node say 'n2' is also noted for its own tag number and the process of completing it for every transaction in the beginning of the node till the end of the node is assigned for the purpose of completing the authentication.

3.4. Protect Download

Upon the execution of the disable function, the protect download option is enabled for matching the constraints that are initially specified in the tag-id. Basically, the tag-id is the unique number assigned to every user for the authentication identity as well as the application identity [11]. For example, the prescribed token say a photo p1, is measured with its size and its time of notification before sharing and the time it is sharing. During this stage, the application itself is assigned with another security option which is specified as the protect download option which will download at the receiver end only if the size of the data i.e image or picture may fit with respect to the timing events which is the time of the image that is shared along with the tag-ids. This process is repeated until the sender truncates its final transaction which assumes in its side. The host or the client involved in these communications are determined by the tag-id's as well as the protect download option also. The following diagram illustrates the uploading data of the client from its memory.

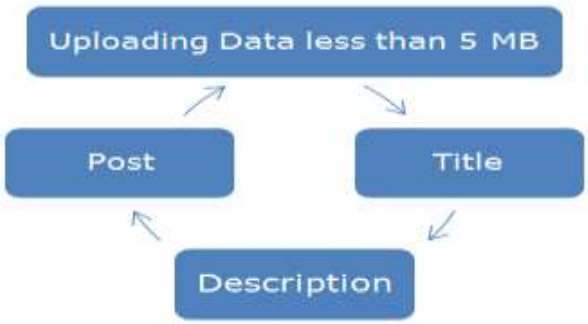

Figure 2 : Data Uploading and its Description

In this diagram, the data size is initially limited to 5 MB as to check the data manipulation process in the beginning stage in order to avoid any complexity involved in the process. Furthermore, the 'post' claimed by the user or the 'title' is the specification of the user who depicts the data initially and the file name of the data. In the other the word 'description' is the full content narrated by the data which is the size of the data as well as the time of uploading the image for sharing before it is communicated. This context is applied in both the ends that are mentioned in the network as the fully transacted data is specified for every notation that can be monitored for many upcoming data.

3.5. Fit Size / Time Series

The important parameter or the test indicator of this 'Register Tag Disable Function Security Model (RTDFSM)' model is the size of the data along matched with the timing constraint. The reason behind this model is the intrusion detection mechanism involved. The cause is data security measures initially executed by the process such as 'Tag-id's', 'Disable function', 'Fit size' and 'Time series'.

Here the 'Fit size' and 'Time series' both test parameters are utilized for analysing the data variant which is identified as the vulnerable data. Further any change in uploading the image, along with the post as well as the title which is the file name derives the description which notifies the total amount of data along with all of its necessary parameters that are mentioned in the specification are identified as the notable tested parameters in this research work.

4. Scalable Estimations

This research work includes the scalable estimation for the purpose of illustrating the noted parameters under testing strategy. The main focus of this research is identifying the vulnerable data and isolating it with respect to assigning tag identification numbers through specifying a new framework as 'Register Tag Disable Function Security Model (RTDFSM)'.The diagram specifies the tag id number initially assigned for every user.

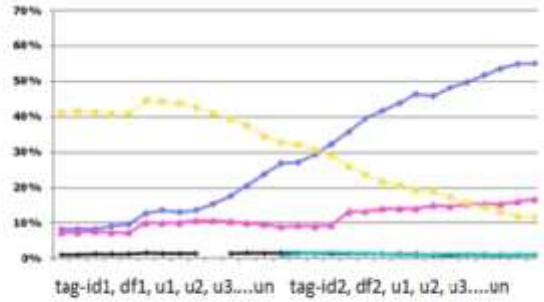

Figure : 3 Parameter Analysis for Register Tag Disable Function Security Model (RTDFSM)

This tested parameter is indicated by the colour lined 'pink'. In the beginning stage, the data communication in the social network is slightly increased. In the next stage, the tag-id specification and the data number of 30% to 40% when summed to achieve 70% is said to be evaluated with respect to its time further. The time series is analysed with the suitable 'disable function' say 'Df' when all the assigned tag and data is enabled for 'protected download' option. The increase in number of the function grows to a considerable percentage ranging from 10%, 20% upto 58% at the later stage. Thus the 'Register Tag Disable Function Security Model (RTDFSM)' has stated a milestone in the domain network security or information security to detect the intrusion of any vulnerable data.

5. Conclusion

The research work analysed the vulnerable data intrusions in the network communications by proposing a novel model namely 'Register Tag Disable Function Security Model (RTDFSM) '. The work narrates the review literature by suggesting certain supportive research papers which initiates this model to identify the network intrusions. The model depicts the importance of network security theme through proposing certain security test parameters like 'tag-id- tag identification number' a unique number assigned to every node in the network which narrates the importance of isolating the intrusion behaviour in the social networks. Furthermore, the assignments of nodes are registered initially with various login procedures as usual and it is assigned by tag identification numbers with respect to its time series. Within the time series classifications a novel manipulating function called as 'disposable function' is assigned to every nodes enrooted in the network to measure the vulnerabilities. If any of the node violates the disable function are considered to be vulnerable subjectively. Moreover 'protection enabled' option is assigned to every sharing data along with memory size i.e fit size classifications. This model further analyses that any change in size of the data with respect to its time is also categorized as vulnerable and has detected the intrusion occurrence in the network. Finally all the test resulting parameters are suggested for network intrusion detections are tested based on its value inputted with respect to the disposable function. All the intrusions are detected with respect to the tag-identifications in the initial stage and later the scalability process of the suggested parameters are improved upto 70% level with respect to the usual network algorithms. Hence this model is suggested as novel framework to identify intrusion detection in network.

6. References

[1]. Randy Baden, Adam Bender, Neil Spring, Bobby Bhattacharjee, and Daniel Starin. Persona: An online social network with user-defined privacy. August 2009, 135–146, SIGCOMM *Comput. Commun. Rev., 39(4)*. Available from: https://www.researchgate.net.

[2]. Nathan Bronson, Zach Amsden, George Cabrera, Prasad Chakka, Peter Dimov, Hui Ding, Jack Ferris, Anthony Giardullo, Sachin Kulkarni, Harry Li, et al. Tao: Facebook's distributed data store for the social graph. 2013 , pages 49–60, *In Presented as part of the 10TH USENIX Annual Technical Conference (USENIX ATC 13)* . Available from: https://www.usenix.org.

[3]. Sonja Buchegger, DorisSchi¨oberg, Le-HungVu, and AnwitamanDatta. Peerson: P2p social networking: Early experiences and insights. 2009, pages 46– 52, *In Proceedings of the Second ACM EuroSys Workshop on Social Network Systems, SNS '09, New York, NY, USA,. ACM.* Available from: https://dl.acm.org/doi/10.1145/1578002.1578010.

[4]. L. A. Cutillo, R. Molva, and T. Strufe. Safebook: A privacy-preserving online social network leveraging on real-life trust. Dec 2009, 94–101, *IEEE Communications Magazine, 47(12)*. Available from: https:// www.semanticscholar.org.

[5]. AzarEftekhar, ChrisFullwood, and NeilMorris. Capturing personality from Facebook photos and photo-related activities: How much exposure do you need? 2014, 37: 162 – 170, Computers *in Human Behaviour*. Available from: https://www.researchgate.net.

[6]. PhilipW.L.Fong. Relationship-based access control: Protection model and policy language. ACM, 2011, pages 191–202, In *CODASPY'11.* Available from: https://citeseerx.ist.psu.edu.

[7]. Allison Lewko and Brent Waters. Decentralizing attribute-based encryption. 2011, pages 568–588, *In Proceedings of the 30th Annual International Conference on Theory and Applications of Cryptographic Techniques: Advances in Cryptology, EUROCRYPT'11, Berlin, Heidelberg, and Springer-Verlag.* Available from: https://eprint.iacr.org.

[8] KaitaiLiang, JosephK.Liu, RongxingLu, and DuncanS.Wong. Privacy concerns for photo sharing in online social networks. 2015, 58– 63, *IEEE Internet Computing.* Available from: https://ieeexplore.ieee.org/document/6894476.