International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

PROTECTION OF VIRTUAL CURRENCY USING SERVICE INTEGRATED MECHANISM IN ECOMMERCE APPLICATION

POLISETTY PRIYANKA[1], MALAPATI NARESH [2]
1 PG Scholar, Dept. of Computer Science and Engineering, Newton's Institute of Engineering
2 Associate Professor, Head. of. Dept. of Computer Science and Engineering, Newton's Institute of Engineering,

ABSTRACT

Online Social Networks and Virtual Currency will place a prominent role in the real world applications, now a day these mechanisms are going to integrate with financial activities those system are using real and virtual currency. This OSN mechanism will provide the platform to promote their products and it was working as a purchasing instrument. However, this scenario related to financial operation. The existing system uses different platforms to perform a single event so this increases the cost to perform a transaction. Also, there are many fake users and sellers who perform some malicious events within the system. In this Project, we will develop a single platform which can perform e-commerce, financial transactions and social networking services, i.e., I will integrate multiple services into a single platform. Initially, we are concentrating on some issues like fake product selling and fake transaction to save the virtual currency. But in this scenario the first challenge was data classification, to overcome this challenge we are using Random forest statically classifier mechanism for obtaining perfect data classification set. By using this we develop a list of fake product sellers based on reviews given by the users/customer, and block such malicious users from performing such malicious events in future. I also restrict the user actions in order to prevent the user from performing any malicious/in authorized events within the system

KEYWORDS: Virtual currency, Random Forest

INTRODUCTION

Online social network associations (OSNs) that consolidate virtual cash serves a drawing in stage for various business works out, where on the online, natural headway is among the foremost unique ones. Specifically, a customer, who is typically addressed by her OSN account, can get repay as virtual cash by sharing on the online progression activities addressed by business components. She would then have the choice to use such reward in various ways, as an example, electronic shopping, moving it to other individuals, and despite exchanging it for authentic cash. Such virtual-money enabled online headway model engages titanic exertion, offers direct financial lifts to finish customers, and in as far as possible the co-activities between business substances and financial foundations. Subsequently, this model has shown unprecedented assurance and expanded enormous normality rapidly. In any case, it faces a significant chance: aggressors can control incalculable records, either by enlisting new records or exchanging off existing records, to seem into the web headway events for virtual cash. Such dangerous activities will during a general sense undermine the sufficiency of the progression works out, rapidly voiding the reasonability of the headway theory from business components and within the meantime hurting ONSs' reputation. Furthermore, a big volume of virtual cash, when compelled by aggressors, could similarly transform into a possible test against virtual money rule.

Secure Computing:-

Computer security (Also referred to as cyber security or IT Security) is information security that can be applied to computers and networks or both collectively called computer networks. Even protection from unplanned events and natural disasters comes under computer security or else, the term security or the computer security can be defined as the techniques that ensuring the data stored that can not be read or accessed by any individuals without authorization. Majorly, whenever we talk about computer security measures it involves in encoding and passwords. encoding in other words can be defined as nothing but the translation of data from a human readable into a human non understandable form which means it needs a deciphering mechanism to understand and decode.

Working Conditions and Basic Needs within the Secure Computing:

If you do not take basic steps to guard your work computer, you set it and every one the knowledge thereon in danger. You will potentially compromise the operation of other computers on your organization's network, or maybe the functioning of the network as an entire.

Physical Security:

Technical measures like login passwords, anti-virus are essential. (More about those below) However, a secure physical space is that the first and more important line of defense.

Is the place you retain your workplace computer secure enough to stop theft or access thereto while you're away? While the safety Department provides coverage across the center, it only takes seconds to steal a computer, particularly a transportable device sort of a laptop or a PDA. A computer should be secured like all other valuable possession once you aren't present.

Human threats aren't the sole concern. Computers are often compromised by environmental mishaps (e.g., water, coffee) or physical trauma. Confirm the physical location of your computer takes account of these risks also.

Access Passwords:

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

The University's networks and shared information systems are protected partially by login credentials (user-IDs and passwords). Access passwords also are an important protection for private computers in most circumstances. Offices are usually open and shared spaces, so physical access to computers can't be completely controlled.

To protect your computer, you ought to consider setting passwords for particularly sensitive applications resident on the pc (e.g., data analysis software), if the software provides that capability.

Prying Eye Protection:

Because we affect all facets of clinical, research, educational and administrative data here on the medical campus, it's important to try to everything possible to attenuate exposure of knowledge to unauthorized individuals.

PROBLEM DESCRIPTION

Attackers may attempt to evade our detection after they know the design of Procured. This represents a general challenge for all detection systems rather than a specific design flaw of the Existing system. Specifically, attackers can instrument their accounts so that their behaviors' are indistinguishable from benign accounts. However, since Procured, detection features characterize elements of malicious accounts that are critical to their success of attacks and stealthiest against other detection systems, the successful evasion may fundamentally constrain attackers' capabilities. For example, attackers can significantly increase the number of active days of malicious accounts. However, it may expose malicious accounts to existing bot-account detection systems that leverage frequent login patterns of malicious accounts. Attackers can also increase the number of friends by adding malicious accounts as friends. Nevertheless, this may qualify the applicability of many detection systems that take advantage of social structures. Attackers can also increase the diversity for recharging sources, the amount of recharging, and the expenditure from bank accounts. However, these solutions directly increase the financial cost for launching the attacks, which could make attacks themselves meaningless. Attackers might also attempt to decrease the percentage of expenditure as gifts, which, however, fundamentally limit the bandwidth to launder the collected virtual currency.

RELATED WORK

We propose a green encoder that relies upon mixed substance game plan features from a significant part of the world's unfathomable powers. In the ABE Diagram in Grand Universe, any game plan can be used as a segment of the contraption, and these properties are not for the most part recorded eventually inside the piece. In a multi-authority ABE plan, no single authority passes on keys to clients. Or maybe, there are various organizations, each responsible for coursing the right keys to a specific plan of features. Preceding our imaginative manifestations, various plans have presented that oblige these sorts of homes, yet not both. Our creation achieves the most significant arrangement with the help of allowing two powers to control the key assignment of a collection of features.

Online social we present another method of encryption for block figures, which we call win or bust encryption. This mode has the fascinating characterizing property that one should unscramble the whole ciphertext before one can decide even one message block. This implies that animal power look against win or bust encryption are eased back somewhere near a factor equivalent to the quantity of squares in the ciphertext. We give a particular method of actualizing win big or bust encryption utilizing a "bundle transform≒ as a pre-handling step to a conventional encryption mode. A bundle change followed by standard codebook encryption additionally has the fascinating property that it is effectively executed in equal. Win big or bust encryption can likewise give insurance against picked plaintext and related-message assaults.

PROPOSED MECHANISM

In this project, we are concentrating on some issues like fake product selling and fake transaction to save the virtual currency but in this scenario, the first challenge was data classification to overcome this challenge. I used Random forest mechanism for perfect data classification for fake product selling. We are design review based mechanism to identify the fake sellers and we are concentrating on unauthorized apps usage to save the virtual currency by using authentication protocol mechanism to avoid unauthorized user access. Increasing the scalability to user in these, we are implemented monopoly ecommerce layer to avoiding the gateway payments issue. We proved experiment theoretically and practically.

Social Network

In this module, the Social Network has to login by using valid user name and password. After login successful he can do some operations such as View all Buyers and authorize, View all Ecommerce Users and authorize, View all Products, View all Purchased Products Based On Ecommerce Site, View all Money Laundering Account, View all Phishing Attackers, View all Exploit Vulnerability

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Ecommerce User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like View Profile, Add Category, Add Products, View All Products, View All Products Purchase Request, View all Purchased Products with total bill, View all Money Laundering Account, View all Phishing Attackers, View all Exploit Vulnerability.

Buyers

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like Manage account, View Your Profile, Search Friends, View Friend Request and Response, View My Friends, Search Products, View all Purchased Products with total bill.

Identifying spontaneous substance and in this way the spammers who make it is a long-standing test that influences all people on every everyday . The informal community application ongoing development has given new difficulties just as promising circumstances inside the spam location occasion. Roused by the Tagged.com1 informal community, we create techniques to recognize spammers in advancing

multi-social interpersonal organizations. We model an informal community as a period stepped multi-social chart where vertices address clients, and edges address various exercises between them. to distinguish spammer accounts, our methodology utilizes primary highlights, grouping displaying, and aggregate thinking. We influence social succession data utilizing k-gram highlights and probabilistic demonstrating with a combination of Markov models. Moreover, a class of probabilistic graphical models which are profoundly versatile. Here, they utilized Graph lab Create TMand Probabilistic Soft Logic (PSL)2 to model and tentatively assess our answers on web scale information from Tagged.com. Our examinations exhibit the adequacy of our methodology, and show that models which consolidate the multi-social nature of the informal community fundamentally acquire prescient execution over individuals that don't.

CONCLUSION

This work presents a novel system, CESDM to automatically detect and block the malicious accounts that participate in online platforms. Here, we introduce a single online platform to perform multiple events at single instance of time. Our model consists of banking/financial transaction platform, e-commerce platform and online social networking site. By this project, we have been successful at blocking the malicious accounts within the system, this makes our platform much authenticated and secured platform by blocking malicious sellers enables us to provide a trustful platform to end-user which sells quality products. By blocking malicious end users we can decrease the un necessary traffic within the system which results in less load on servers..

REFREENCES

[1]Y. Wang and S. D. Mainwaring, "Human-currency interaction: learning from virtual currency use in china," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2008, pp. 25–28.

[2]X. Hu, J. Tang, and H. Liu, "Online social spammer detection," in Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence. AAAI, 2014, pp. 59–65.

[3]"Leveraging knowledge across media for spammer detection in microblogging," in Proceedings of the 37th international ACM SIGIR conference on Research & development in information retrieval. ACM, 2014, pp. 547–556.

[4]Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia, "Detecting automation of twitter accounts: Are you a human, bot, or cyborg?" IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6, pp. 811–824, 2012.

[5]Z. Chu, S. Gianvecchio, A. Koehl, H. Wang, and S. Jajodia, "Blog or block: Detecting blog bots through behavioral biometrics," Computer Networks, vol. 57, no. 3, pp. 634–646, 2013.

[6]S. Fakhraei, J. Foulds, M. Shashanka, and L. Getoor, "Collective spammer detection in evolving multi-relational social networks," in Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2015, pp. 1769– 1778.

[7]Y.-R. Chen and H.-H.Chen, "Opinion spammer detection in web forum," in Proceedings of the 38th International ACM SIGIR Conference on Research and Development in Information Retrieval. ACM, 2015, pp. 759–762.

[8]F. Wu, J. Shu, Y. Huang, and Z. Yuan, "Social spammer and spam message co-detection in microblogging with social context regularization," in Proceedings of the 24th ACM International on Conference on Information and Knowledge Management. ACM, 2015, pp. 1601–1610.

[9]Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A. H. Wang, "Twitter spammer detection using data stream clustering," Information Sciences, vol. 260, pp. 64–73, 2014.

[10]H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detecting and characterizing social spam campaigns," in Proceedings of the 10th ACM SIGCOMM conference on Internet measurement. ACM, 2010, pp. 35–47.

[11]S. Lee and J. Kim, "Warningbird: Detecting suspicious urls in twitter stream." in NDSS, vol. 12, 2012, pp. 1–13.

[12]A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud

detection system: A survey," Journal of Network and Computer Applications, vol. 68, pp. 90 – 113, 2016.

[13]J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," Computers & Security, vol. 57, pp. 47 – 66, 2016.

[14]D. Olszewski, "Fraud detection using self-organizing map visualizing the user profiles," Knowledge-Based Systems, vol. 70, pp. 324 – 334, 2014.

[15]L. Breiman, "Random forests," Machine learning, vol. 45, no. 1, pp. 5–32, 2001.

[16]S. RColorBrewer and M. A. Liaw, "Package randomforest," 2012.

POLISETTY PRIYANKA is a Master candidate in Dept. of computer Science and Engineering at Newton's Institute of Engineering, Macherla.

MALAPATI NARESH is a Associate Professor & Head Department of Computer Science & Engineering at Newton's Institute of Engineering, Macherla.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362