IPHV8I3001X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .III
ISSN Online: 2319 – 9253
Print: 2319 – 9245

EFFICIENT SECURITY PROOFS FOR TRUST WORTHY SERVICES IN MOBILE SOCIAL NETWORKS

[#1]Mrs. V S J PALLAPOLU, *Lecturer-BIS,*
Department of Accounting & Finance,
University of Botswana,
Gaborone, Botswana.

[#2]GOLAJAPU VENU MADHAVA RAO,
Research Scholar,
Sri Satya Sai University of Technology and Medical Science, Sehore, Madhya Pradesh.

***Abstract*:** Now a day, Web-based coordinated efforts have turned into a key innovation for a business. Such innovation traverses the communications amongst individuals and administrations over the world. Benefit situated framework gives the administrations to help the different business forms. However, it is constrained to give adaptable collaboration demonstrate required to creating business. For a fruitful business, human must be the piece of the framework. Portable Social Network will be network which enables versatile clients to find and communicate with existing and potential companions. A Trustworthy Service Evaluation (TSE) framework is a framework that empowers clients to share benefit audits in Service arranged versatile social networks (S-MSNs). Each specialist organization ought to freely keep up a TSE for itself that gathers and stores clients' surveys about its administrations without requiring any third confided in expert. In the S-MSNs, to set up the trust relations between the specialist co-ops and the clients is especially essential. We consider a S-MSN made out of static merchants and versatile clients that interconnect entrepreneurially. Every seller is furnished with a remote specialized gadget that has a vast stockpiling space. In this we develop the bTSE(basic TSE) to a Sybil-opposed TSE (SrTSE) which empower the identification of two ordinary Sybil assaults. In SrTSE if a client produces numerous audits toward a merchant in a predefined schedule opening with various nom de plumes, genuine character of that client will be uncovered. Subsequently a Trustworthy Service in Mobile Social Network is presents so clients can get to administrations securely.After recognizable pieces of proof with different punctuations they are sorted all together and reliable administration assessment framework is empowered for the clients to share their surveys of a specific music sheet they are purchasing through their advanced cells or tabs in administration arranged versatile social networks(S-MSN)without any third confided in gathering. Since there are no third trusted gatherings there are many possibilities for Sybil assaults and other adjustment survey assaults which are to be kept away from.

Keywords: *Portable social networks confide in assessment, Sybil assault, and conveyed framework.*

I.INTRODUCTION

In the S-MSNs, specialist organizations offer area based administrations to neighborhood clients and draw in the clients by different publicizing approaches, for instance, sending e-flyers to the adjacent travelers by means of remote connections. With a higher notoriety, a specialist organization is probably going to be picked by the clients. Nonetheless, the S-MSNs are independent and conveyed networks where no third trusted expert required for bootstrapping the trust relations. In this way, for the clients in the S-MSNs, empower the trust assessment of the specialist organizations that is a testing issue. Area based administrations now rise as a basic need of portable clients. It can be coordinated into different sorts of networks to acquire promising applications while their execution has numerous remarkable and autonomous research issues. The blast in online innovation has prompted expanding volume and many-sided quality of information, which animates the expansion of virtual learning groups (VLCs). VLCs are data innovation based cyberspaces in which people and gatherings of geologically scattered learners achieve their objectives of elearning. One of VLCs' motivations is to energize learning sharing so that profitable information inserted in the network can be successfully investigated. The vast majority of the learners take an interest in VLCs with the desires that they can gain and offer important information to suit their requirements. The development of VLCs over the previous decade has empowered research interests by the scholarly world and experts. Dependable administration evaluation[3] (TSE) framework utilized for specialist organization or any third trusted expert to get of client criticism is called review.Mobile Social networks have given the foundation to various developing applications as of late, e.g., for the suggestion of specialist co-ops or the proposal of documents as administrations. In these applications, trust is a standout amongst the most vital figures basic leadership by a serviceconsumer, requiring the assessment of the dependability of a specialist co-op along the social trust ways from an administration shopper to the specialist organization.

IPHV8I3001X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .III
ISSN Online: 2319 – 9253
Print: 2319 – 9245

Nonetheless, there are normally numerous social trust ways between two members who are obscure to each other. Furthermore, some social data, for example, social connections amongst members and the proposal parts of members, has critical impact on trust assessment yet has been ignored in existing investigations of online social networks. Besides, it is a testing issue to seek the ideal social trust way that can yield the most dependable assessment result and fulfill an administration customer's trust assessment criteria in light of social data. Which enables Business experts to dissect clients' discussions on social networking locales, and as a result, gives constant notices about their items and administrations likewise. In the above circumstances, trust is a standout amongst the most vital variables for members' basic leadership, requiring methodologies and instruments for assessing the reliability between members who ;are obscure to each other. For instance, if a social network comprises of bunches of purchasers and merchants, it can be utilized by a purchaser to locate the most reliable/respectable dealer who offers the item favored by the purchaser. In social networks, every hub speaks to a member and each connection between members relates to this present reality associations or online cooperations between them (e.g., A→ B and A → C in Fig. 1). One member can give a trust an incentive to another in light of the immediate associations between them. For instance, a trust rating can be given by a member to another in view of the nature of the motion pictures prescribed by the last at FilmTrust3. As every member generally cooperates with numerous different members various trust way. For instance, in Fig. 1, A&M are in a roundabout way connected by two ways, A → B → E → M and A → D → M. On the off chance that a trust way interfaces two nonadjacent members (i.e., there is no immediate connection between them), [6] the source member can assess the dependability of the objective one in light of the trust data of the objective on of the trust based data. This procedure is called [5] trust engendering and the way with trust data connecting

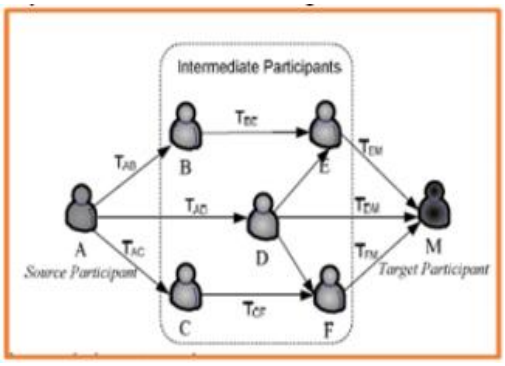


Fig.ure 1: A social network

The source member and the objective one is known as a social trust way For instance, in Fig. 1, if A will be a purchaser and M is a vender, A can assess the dependability of M utilizing the social trust ways from A to M. We allude to An as the source member and M as the objective member. This paper portrays another follow based reenactment innovation that catches conditions between social network messages seen in full-framework reproduction of multithreaded applications. Bruckman (2002) found that the learning capability of the Internet innovation can originate from associates and senior citizens. Jin (2002) gave a theoretical structure to the improvement of a model arrangement of the virtual group based intuitive learning condition. Wachter et al. (2000) brought up that an improved learning condition is conceivable just in the event that one goes past unimportant online course conveyance and makes a group of learners and other related asset gatherings. Wasko and Faraj (2005) found that learning sharing has been an inspiration for investment in virtual groups. What's more, many online or specialist based models and programming have been proposed to bolster association, dialog, and coordinated effort in VLCs (Taurisson and Tchounikine, 2004; Zhang and Tanniru, 2005; Matusov, Hayes, and Pluta, 2005; Avouris, et al., 2004). Earlier reviews have given confirmation that exhibits the significance of information trade in improving learningperformance. They additionally have required the consideration of giving components to bolster learning partaking in VLC situations. Nonetheless, learning partaking in some VLCs has not satisfied desires. Two obstructions anticipating proficient and successful information sharing are: (1) the trouble in discovering quality information, and (2) the trouble in finding dependable learning colleagues to collaborate with. The target and commitment of this exploration is applying shared (P2P) based social networks with trust management instruments to overcome the previously mentioned obstructions. Keeping in mind the end goal to enable learners to discover quality substance and reliable associates, we give peer-positioning components and characterize peers in view of their substance's quality. We have upgraded the ordinary catchphrase seek with a watchword thesaurus look and a semantic inquiry to enhance the execution of substance disclosure. We have additionally improved customary online gathering dialogs by finding reliable partners who are all the more ready to share. to their loved ones [Haythornthwaite 2005]. The marvelous development of social network clients as of late has not gone unnoticed. Governments and undertakings have begun misusing the potential utilization of social networks as stages for conveying and enhancing their administrations [Jaeger et al. 2007; Zappen et al. 2008]. In any case, there have been reports in the media of numerous episodes of breaking

protection of people through social networks [Gross and Acquisti 2005]. Given the open way of Web-based social networks and their present level of prominence, clients are progressively worried about protection, a critical thought for them. To adjust the open way of social networks and shield the security worries of clients, it is critical to fabricate confide in groups, which we characterize as groups that make a situation where individuals can share theirs considerations, sentiments, and encounters in a transparent path without worries about protection and dread of being judged. These people group are based on realness, open sharing, as mindedness and common regard. We fight that social trust gives a perfect establishment to building trust groups. In this way, trust turns into an imperative part of social networks and online groups. Trust has been considered in many controls including humanism [Helbing 1994; Mollering 2002; Molm et al. 2000], brain research [Rotter 1967; Cook et al. 2005], financial aspects [Granovetter 1985; Huang 2007], and software engineering [Maheswaran et al. 2007; Hughes et al. 2005]. Each of these orders has characterized and considered trust from alternate points of view, and their definitions may not be specifically material to social networks. When all is said in done, trust is a measure of certainty that a substance or elements will carry on in a normal way. In this article, we audit the definitions and estimations of trust from the crystal of various controls, with an attention on social networks. The most vital resource of any general public or a social network is its social capital [Nahapiet and Ghoshal 1998; Moibus and Quoc-Anh 2004]. We consider the extravagance of the connections between individuals in the social network as its social capital. With regards to social networks, trust is gotten from social capital, which we call social trust.

II.RELATED WORK

Mobile social networks expand social networks in the by enabling versatile clients to find and interface with existing and potential companions. Regardless of their guarantee to empower energizing applications, genuine security and protection concerns have obstructed wide reception of these networks [1].

A. Secure Friend Discovery

A vital capacity offered by portable social networks is that to enable versatile clients to find and connect with companions. Assume you are sitting tight for your flight in an air terminal and your cell phone finds your's companion is in the following path and you can chat with eye to eye. Or, on the other hand you visit another place and your cell phone discovers somebody in your region has comparative characteristics as you so you can interface with. Assume you are sitting tight for your flight in an airplane terminal and your cell phone finds your's companion is in the following passageway and you can chat with vis-à-vis. Or, then again you visit another place and your cell phone discovers somebody in your region has comparative properties as you so you can connect with. One approach to address the protection and security issues is to exploit a confided in focal server, which gathers data from individual clients, figures and disperses the nearness comes about on request. Server-basedsolution is not appropriate for portable social networks for the accompanying reasons. In the first place, clients in a portable social network might not have guide access to a PC or the Internet.

B. Dynamic Privacy-Preserving Key

Management For vehicle client's protection conservation to enhance key refresh proficiency of area based administrations (LBSs) in vehicular advertisement - hoc networks (VANETs), we propose a dynamic security saving key administration conspire, called DIKE. We partition session into a few availabilities so t each schedule opening holds an alternate key, when no vehicle client leaves from the administration session. In this additionally coordinate a novel dynamic edge procedure in conventional V-2-V and V-2-I interchanges to accomplish session key's in reverse mystery. Execution assessments for broad reenactments show the proficiency and adequacy of the proposed DIKE conspire for relaxed refresh postponement and quick key refresh proportion. In this paper, we accomplish vehicle client's security Preservation and to enhance the key refresh effectiveness. In this a Dynamic security saving Key administration plot, called DIKE, for the LBSs in VANETs. With this plan, every client can utilize a pseudo-id to cover its genuine character amid an administration session. To start with, present a protection saving verification (PPA) system, which can get from a productive gathering Signature.However, every vehicle client can hold different nom de plumes; can't keep a traded off yet unrevoked vehicle client to do twofold enrollment in a similar session. That is the reason we isolate a session into a few schedule openings, and each availability can hold an alternate session key. At the point when no vehicle leaves from the administration session, each joined client use forward-mystery system to self-sufficiently refresh new session key to diminish key refresh delay. To accomplish in reverse mystery, we coordinate a novel dynamic limit method in customary V-2-V and V-2-I interchanges.

C. The Sybil Attack

The Sybil assault was first presented by Douceur with regards to shared networks. In this, we examine the Sybil assault, which is an unsafe assault in sensor networks. In Sybil assault,

a vindictive hub acts like it was a bigger number of hubs, as by mimicking different hubs or just by guaranteeing false personalities. We propose novel procedures to shield against Sybil assault, and break down their viability legitimately. In this paper, we look at how the Sybil assault can used to assault a few conventions in remote sensor network. So initially consider assaults on conveyed stockpiling a calculation, like the Douceur portrays in the distributed condition. To protect the Sybil assault, we can esteem that every hub character is a personality displayed by the comparing physical hub. There are two sorts to approve a personality we characterize the Sybil assault and build up scientific classification of that assault by recognizing diverse assault sorts. The definition and scientific categorization are vital in comprehension and dissecting the danger that protections of Sybil assault. We exhibit a few novel techniques by which a hub can be checked whether different characters are Sybil personalities.

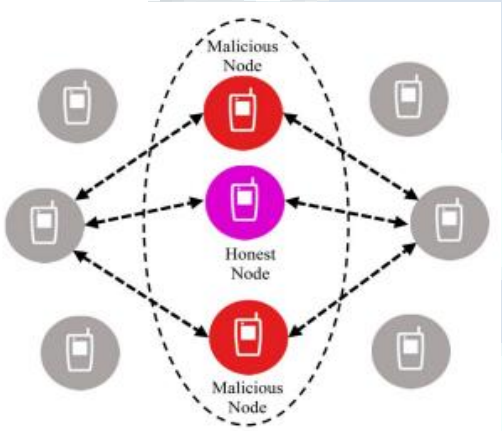


Fig. 2. Example of Sybil attack.

A Sybil assault resembles PC programmer assault on a distributed (P2P) network. It is named by the novel Sybil, which describes therapeutic treatment of a lady with outrageous dissociative character issue. The assault target just notoriety arrangement of the P2P program and furthermore enables the programmer to have an uncalled for preferred standpoint in affecting the notoriety and the score of records put away on the P2P network. A few variables verify that how a Sybil assault can be similarly influences the notoriety framework and that it is so natural to make an element; at long last whether the program acknowledges non-put stock in substances and their information. Approving records can be the most ideal path for managers to keep these sorts of assaults, however this yields the secrecy of clients.

III. INSPIRATION

In this paper, we proposed follow – based reenactment system for TSE. TSE framework is set aside more opportunity for message sending and accepting by client and seller. That framework give mystery key to confirmation both time ask check no then procedure begin in proposed [4] framework utilized follow based reproduction system. Time taken is not exactly as indicated by the current framework. Various messages can be passing frequently.The [10] reliance data is put away alongside bundle information in the network follow. By implementing the requesting limitations in a network test system, the proposed strategy can extraordinarily build the devotion of follow driven assessment with little effect on reenactment speed. . Follow construct recreation works with respect to two part one that executes activity and stores the outcome and another which peruses the log records to follow and adds at that point to new situation. On account of extensive PC outline the execution happens on few hubs and follow are left in log record .In propose framework utilized follow based reproduction method for increment the work quick. Some imperative direct related toward inspiration.

- In this venture proposed follow based recreation to empower client to share benefit survey in administration situated portable social network.
- Trace based reproduction alludes to framework reenactment performed by taking a gander at hint of program execution or framework part access with purposed of execution expectation.
- Trace construct reenactment works with respect to two part one that executes activity and stores the outcome and another which peruses the log records to follow and adds at that point to new situation.
- In the instance of expansive PC plan the execution happens on few hubs and follow are left in log document.

In this segment, we assess the execution of the bTSE through follow based custom recreations. We contrast the bTSE and a NCP (non-helpful) framework, where every client straightforwardly presents its survey to the merchant with no synchronization limitation (utilization of tokens). We utilize the accompanying execution measurements

- SR. It is characterized as the proportion of the quantity of effectively submitted audits to the aggregate number of produced surveys in the network.
- SD. It is characterized as the normal span between the time when an audit is produced and the time when it is effectively gotten by the merchant.

Area based administrations as of late rise as a basic need of versatile clients. It can be incorporated into different sorts of networks to acquire promising applications while their execution has numerous extraordinary and free research issues, for example, content conveyance [13], benefit disclosure [14], security, and protection issues [15]. Trust

assessment of specialist co-ops is a key segment to the accomplishment of area based administrations in a disseminated and self-ruling network. Area based administrations require a one of a kind and productive approach to awe the neighborhood clients and acquire their trust so that the specialist organizations can get benefits. Rajan and Hosamani utilized an additional screen sent at the untrusted merchant's site to ensure the respectability of the assessment comes about. Wang and Li [10] proposed a two-dimensional trust rating total way to deal with empower a little arrangement of trust vectors to speak to a vast arrangement of trust evaluations. Ayden and Fekri moved toward the trust administration as a derivation issue and proposed a conviction engendering calculation to productively process the minimal likelihood conveyance capacities speaking to notoriety esteems. Dasand Islam presented a dynamic trust calculation model to adapt to the deliberately changing conduct of vindictive specialists. In this paper, we empower portable clients to present their surveys to a framework kept up by the neighborhood seller, where the audits speak to the assessment comes about toward the administrations of the merchant. We consider the malevolent practices by the seller and the clients including the audit assaults and the Sybil assaults. Rather than utilizing an additional screen gadget on the merchant's site, we investigate client collaboration endeavors and make utilization of productive cryptography-based systems to build SR, lessen SD, and moderate the impact of the pernicious practices.

IV. PROPOSED PRINCIPLES

In the proposed framework, we are requiring specialist co-ops that will keep up the TSE without anyone else's input. In this, we consider the clients that partake in the TSE in a helpful way. So we will concentrate conceivable malignant practices that are directed by the specialist organizations and clients. Due to the proposed framework, there are points of interest that offer the client of the administrations, it recognizes three remarkable audit assaults, i.e., survey connect capacity assault, audit dismissal assault, and survey change assault in the bTSE every client ought to initially enlist in the social network and afterward they can utilize the administrations given by the specialist organization. Additionally each specialist co-op ought to likewise give their qualifications to enlist in a social network. In the wake of utilizing the administrations the client ought to likewise give audits to each administration. So that the clients who needed to utilize that administrations ought to get the thought

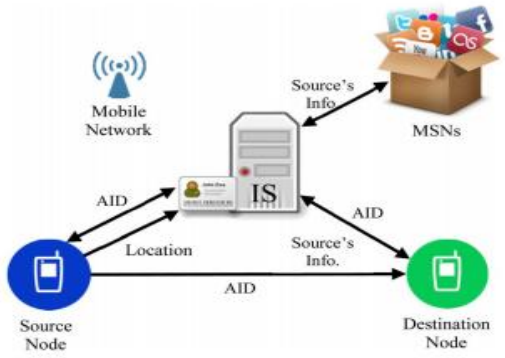


Fig .3. Identity confidentiality in MSNs.

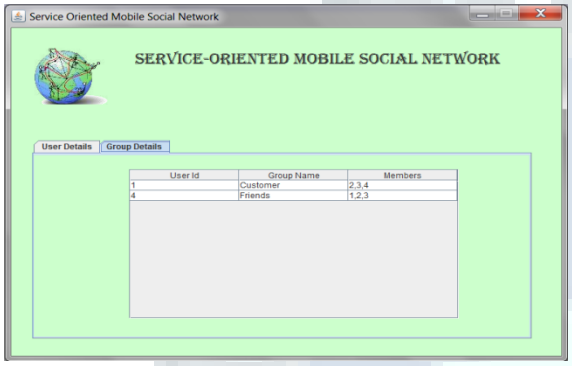
As the framework is dependable so each specialist organization and client ought to give substantial accreditations. The framework utilizes the Ranking procedure for making the positioning simple. Utilizing the TSE, specialist organizations discover that the administration encounters of the clients and that can enhance their administration methodology in time. The gathered surveys can then make accessible to general society, which are upgrades benefit publicizing and accommodating the clients in making savvy benefit determinations. They are vital instruments for specialist organizations who focus on the worldwide market. In this, we move the TSE into the S-MSN settings. Every client ought to right off the bat enroll in the social network and after that they can utilize the administrations given by the specialist organization. Essentially each specialist co-op ought to likewise give their accreditations to enlist in a social network. We create security systems for the TSE to manage the assaults that are emerge amid portable social network. The fundamental TSE (bTSE) is empowers clients to appropriate and helpfully ought to present their surveys in a coordinated chain frame by utilizing progressive and total mark procedures. It limits the specialist co-ops to dismiss, change, or erase the surveys. Subsequently, the trustworthiness and genuineness of surveys are moved forward. Further, we extend the bTSE to a Sybil-opposed TSE (SrTSE) to empower the recognition of two sorts of Sybil assaults. In the SrTSE, if a client produces numerous surveys toward a seller in a schedule opening with various pen names, genuine character of the client will be uncovered. Through security investigation and numerical outcomes, we demonstrate that the bTSE and the SrTSE successfully oppose the administration audit assaults and the SrTSE furthermore distinguishes the Sybil assaults in an effective manner.Through execution assessment, we demonstrate that the bTSE accomplishes better execution as far as submissionrate and postponement than an administration survey framework that does not receive client participation. To begin with, clients in a portable social network can't have guide Access to specialist co-ops or any third trusted expert to

get client input that is administration surveys or essentially audits, for example, compliments and protestations about their administrations or items.

V. RESULTS

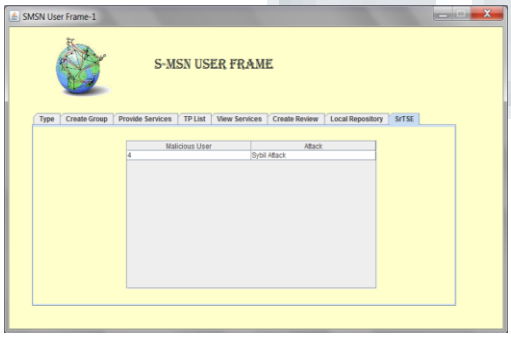
To comprehend finish procedure of this system first we include the client points of interest i.e., ID's and make the gathering which has the both different merchants and the clients. In the perspective of the one merchant other seller who is in his gathering will be as a client the other way around.

Input: - give benefits and send the affirmation token to the gathering individuals.



These can be found in the clients and merchants see administrations page. Before sending the audit to specific seller client need to choose the kind of client he is? The clients can check the audit of different clients survey and his surveys towards the diverse merchants in his nearby vault.

output: - If the client is not pernicious clients the audit will be refreshed in the merchants TPList. In the event that the client is vindictive client the Sybil assault will be enacted and the seller can undoubtedly discover the malevolent clients Id who send the terrible audits in his srTSE page.



1. Under no review rejection attacks: - We first concentrate the framework execution in connection with SR (Submission Review). At the point when SR goes up, the quantity of clients who enter the administration range and in this manner create audits increments. Review that every client has a transmission extend significantly littler than SR. In the non-helpful framework, clients need to move sufficiently close to the merchant to present their audits. Henceforth, the framework demonstrates a diminishing accommodation rate and expanding accommodation delay with SR. We at that point take a gander at how TN (Token Number) impacts the framework execution. Instinctively, when TN goes up, clients have expanded chance to submit surveys, prompting raised framework execution. We watch a doubtful marvel: accommodation rate and postpone both settle after TN is past sure esteem. At the point when there are more tokens circling in the network, at first clients can without much of a stretch get tokens and present their audits. Review that clients never again take an interest in the audit framework once their surveys are submitted to the merchant or sent to others. After some time, the network of taking an interest clients ends up plainly meager and scanty, and these clients have less and less opportunity to get a token because of diminished network thickness.

Under survey dismissal assaults: - The execution examination of Trace based procedure and the non-helpful framework when the merchant dispatches audit dismissal assaults. We watch that the non-helpful framework has a > 25% execution drop in accommodation rate. To be sure, it is not furnished with any security instrument against the assaults and endures execution debasement. Accommodation delay does not demonstrated any detectable change since just direct accommodation is occupied with the non-agreeable framework and just effectively submitted audits are considered amid postpone figuring. Contrasted and the instance of no audit dismissal assaults, follow based method just has marginally decreased (< 10% littler) accommodation rate and almost unaltered accommodation postpone on account of the client collaboration and survey collection components. It is important that follow based strategy accomplishes significantly higher accommodation rate than the non-Cooperative framework, up to 100%. These recreation comes about show that follow based strategy can adequately oppose audit dismissal assaults.

VI.CONCLUSION

In this paper, we proposed a TSE framework for S-MSNs. The framework utilizes various leveled signature and total mark methods to change autonomous audits into organized survey chains. This change incorporates disseminated client collaboration, which enhances audit uprightness and altogether decreases merchants' adjustment ability. We have presentedthree audit assaults which demonstrates that the bTSE can viably oppose survey assaults without depending on a third confided in specialist. Development of pen names the mystery enters in the bTSE, and acquired a SrTSE framework.

REFERENCES

[1] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure Friend Discovery in Mobile Social Networks," Proc. IEEE INFOCOM, pp. 1647-1655, 2011.

[2] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "Diviner: A Secure and Efficient Service Review System for Service-Oriented Mobile Social Networks," Proc. IEEE 32nd Int'l Conf. Circulated Computing Systems (ICDCS), pp. 647-656, 2012.

[3] X. Liang, X. Li, T. Luan, R. Lu, X. Lin, and X. Shen, "Profound quality Driven Data Forwarding with Privacy Preservation in Mobile Social Networks," IEEE Trans. Vehicular Technology, vol. 61, no. 7, pp. 3209-3222, Sept. 2012.

[4] T.H. Luan, L.X. Cai, J. Chen, X. Shen, and F. Bai, "VTube: Towards the Media Rich City Life with Autonomous Vehicular Content Distribution," Proc. IEEE CS Eighth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. Networks (SECON), pp. 359-367, 2011.

[5] J.R. Douceur, "The Sybil Attack," Proc. Overhauled Papers First Int'l Workshop Peer-to-Peer Systems (IPTPS), pp. 251-260, 2002.

[6] Newsome, E. Shi, D.X. Tune, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses," Proc. Third Int'l Symp. Data Processing in Sensor Networks (IPSN), pp. 259-268, 2004.

[7] Quercia and S. Hailes, "Sybil Attacks Against Mobile Users: Friends and Foes to the Rescue," Proc. IEEE INFOCOM, pp. 336-340, 2010.

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs," IEEE Trans. Clever Transportation Systems, vol. 13, no. 1, pp. 127-139, Mar. 2012.

[9] R. Lu, X. Lin, T. Luan, X. Liang, and X. Shen, "Pen name at Social Spots: An Effective Strategy for Location Privacy in VANETs," IEEE Trans. Vehicular Technology, vol. 61, no. 1, pp. 86-96, Jan. 2012.

[10] X. Boyen and B. Waters, "Full-Domain Subgroup Hiding and Constant-Size Group Signatures," Proc. tenth Int'l Conf. Practice and Theory Public Key Cryptography, pp. 1-15, 2007.

[11] X. Liang, Z. Cao, J. Shao, and H. Lin, "Short Group Signature without Random Oracles," Proc. Ninth Int'l Conf. Data and Comm. Security (ICICS), pp. 69-82, 2007.

[12] C. Upper class and Z. Ramzan, "Personality Based Aggregate Signatures," Proc. Int'l Conf. Open Key Cryptography, pp. 257-273, 2006.

[13] Y. Zhang, Z. Wu, and W. Trappe, "Versatile Location-Oriented Content Delivery in Delay-Sensitive Pervasive Applications," IEEE Trans. Versatile Computing, vol. 10, no. 3, pp. 362-376, Mar. 2011.

[14] H. Tsai, T. Chen, and C. Chu, "Benefit Discovery in Mobile Ad Hoc Networks Based on Grid," IEEE Trans. Vehicular Technology, vol. 58, no. 3, pp. 1528-1545, Mar. 2009.

[15] Z. Zhu and G. Cao, "Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System," IEEE Trans. Versatile Computing, vol. 12, no. 1, pp. 51-64, Jan. 2013.