Real-time Advanced Inexpensive Networks (RAIN) of Devices for Reliable M Commerce

K. Rajasekhar
Dy Director General, NIC, MeitY,
Govt of India

Niraj Upadhyay, PhD
Professor, JBIT, RR District

ABSTRACT
The present day solution to any useful, secure, highly scalable system with high concurrency and high availability involve very expensive Data Centre Resources such as application servers, database servers, firewalls, load balancers etc., which involves high CAPEX and OPEX. To reduce the CAPEX and OPEX, a network of devices which can interact reliable to provide secure solution has been presented in this paper. Any Network has to be protected from several attacks such as DDOS to ensure its reliability and high availability. Special Hash tables to create addressable content to increase the reliability, availability and security of the real time advance inexpensive networks. A special category of content addressable network is proposed which can be used reliably for performing e-commerce transactions. The proposed network is robust and can with stand safely the massive DDOS and other attacks practically. No central servers and associated infrastructure is needed to maintain our network. Any node can deterministically search and obtain the target content reliably, cost-effectively and securely in our distributed network.

Keywords
Advanced Networks, Real-time Advanced Inexpensive Networks (RAIN) computing. Real-time Advanced Inexpensive Networks (RAIN) computing. Device Based Computing, Distributed Hash Tables, Content Addressable Networks, DDOS, Security.

1. INTRODUCTION
The m-commerce systems are a type of e-commerce system where most of the transactions happen through the mobile devices. Most of the present computing systems either distributed or centralized, used for e-commerce and m-commerce transactions are very expensive. One more big problem is, even if they are expensive they are not reliable. To enhance the reduce the cost, the distributed devices can be networked and configured to work coherently to achieve the objectives. Bittorrent, Syncplicity,ShareIt etc., are examples of such systems which are used predominantly for sharing the files. The networking of these devices without a central system is possible with an appropriate network coordination system. Network coordinate systems such as vivaldi, which uses a mass-spring-damper system to embed peers into a two-dimensional Euclidean coordinate space with an additional height coordinate. Such distributed algorithms, estimate coordinates of the nodes of distributed D2Ds based on RTTs. In the present most popular decentralized network coordination systems such as Vilvaldi, if the nodes only lookup the adjacent nodes, then the accuracy of coordinates at large scale shall be lesser. So nodes have to contact more nodes at various network distances to get accurate network coordinates. To manage efficiently the search and other operations in the distributed networks with huge number of nodes, distributed hashtables DHTs are used. [1].[2].[3].[4]

The authors surveyed the current research literature related to structured P2P and D2D networks. The reliability which is the ability to prevent and correct the risk due to fradulent transactions is very imortant factor in any m-commerce system. The lack of reliability besides high CAPEX and OPEX is one major problem of the present m-commerce systems.

The RAIN computing which is a device to device (D2D) based low-cost, sustainable, secure computing several years back by the authors.[15],[16],[17],[18]. To address the reliability issue of present e-commerce systems, in this paper we devised a standard comprehensive reliability framework, which we call as '12A framework'. This framework can be imposed on RAIN computing system or even any other present e-commerce and m-commerce systems to ensure the much needed reliability and thus avoid frauds to a large extent in-expensively.

2. SURVEY RELATED RESEARCH WORK
The mobile commerce applications are bound to grow exponentially due to its heavy usage in the day to life by the masses. These mobile commerce applications are changing the personal, professional and social life of masses in the world. The advances in the underlying technologies are heavily contributing to the success of those applications. [6]. However, the underlying technologies are becoming complex and more expensive.

Dynamic fault tolerant content addressible networks (CANs) are being used to tackle addressibility problems, and mitigate DDOS attacks and to search data in reasonable time with heirarchical network architecture. However, such networks have overheads of communication and are not scalable, because as the network size increases, the number of layers have to increase, which increases the load on supernodes at top layer. So restriction of Olog(n) state per node, lookup workload is being imposed [20] where n is the number of nodes in the network. This limits the size of the network.

The EpiChord which is a type of circular address space with a unique addressible identity to each node. The unique address of each node is given by computing hashvalue of the key to which the node is responsible. The DHTs based structured D2D networks normally separate the lookup process and routing state maintenance process by pro-acatively probing all the routing entries periodically to determine their current status. However, EpiChord employs a reactive routing state maintenance strategies by issuing multiple queries asynchronously in parallel as a result, EpiChord reported to have achieved - O(1)-hop lookup performance under lookup intensive workloads, and at least O(log n)-hop lookup performance under churn-intensive workloads even in the worst case. [11]. As the network size grows, the network maintenance services shall also grow enormously, and thus causes performance issues. Moreover, reliability factor

desired for m-commerce transactoins, is not adequately addressed in EpiChord.

Tambour is another DHT protocol which uses parallel lookup to reduce retrive latency and limits the communication overhead by estimating the probabilities of routing entries-liveness, taking into consideration the node lifetime history and evicts dead entries in case of lookup failures. If the network nodes are unstable, their corresponding routing entries are removed, thus reducing the size of the routing tables, which results in minimizing the number of timeouts for later lookup requests. Based on lab experiments, it was claimed that, Tambour protocol is relatively more efficient in using bandwidth and reducing lookup latencies. [21].

Due to mismatch between the physical topology of the network and the network topology created by DHT, the network performance decreases by around 18% due to high latencies and the communication overheads. To overcome this problem, the physical network architecture aware, global network positioning system (GNP) based distibuted D2Ds are preferable.[5]

Distributed Hashtables Based Peer to Peer networks determine the relation between nodes based on entries in the DHTs. However, as the topology determined by DHTs differ from that of physical network topology, additional network latencies usually takes place in the DHT based networks. To overcome this problem, physical location based overlay construction, where locations are determined using the global network positioning (GNP) system was advocated by [13],[14].

However, in the communication networks TraingularIneqailityVoilations shall be prevelent, due to various network characteristics, unlike in physical world. So geographic distance is an imperfect proxy for RTTs in the communication networks. So longer circuits may not allways result in higher latencies and infact longer circuits can reduce latencies, if chosen in a way that favors TIVs. [23][24].

However, all the existing distributed network systems are vulnerable to Byzantine failures. There exists potential risk of routing attacks. There are several counter measures proposed in the literature, however, all such counter measures are in-effective, as attackers can still easily exploit triangle inequality violations. [8].

To overcome such problmes and ensure security, edge-centric Computing which is the natural confluence of peer-to-peer and cloud computing to create hybrid architectures that combine stable resources with mobile terminals are being advocated by some researchers.[7]. However, they are relatively more expensive as central cloud resources are required.

One more important factor is, the ownership rights of the transacting parties should be protected and verified in the e-commerce transactions. Special Virtual Distribution Environments (VDEs) were proposed to ensure the integrity, availability, and/or confidentiality of the information and to control the transactions. The VDEs can also meter or otherwise monitor use of electronically stored or disseminated information. [9]. However, such VDEs are CAPEX and OPEX intensive, so there is need for devicing low-cost alternatives.

3. PROBLEMS OF DISTRIBUTED DEVICE BASED NETWORKS

The D2D networks suffer from following type of attacks predominantly.

Sybil attack - A illegal node, tries to project it-self as genuine node by stealing the identity details of other nodes.

This attack takes place by credential counterfeiting. As shown in figure 1 the actual membership number of a node may be 978, but it may falsly produce a counterfiet identity 325, which may some previleges.

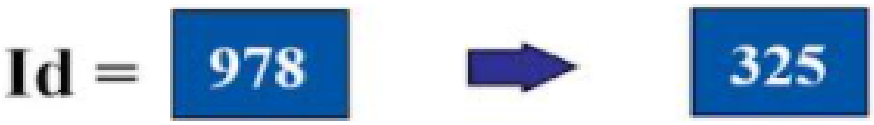

Figure 1. Credential Counterfeiting

Eves dropping: Un-authorised node can get connected to the network and evesdrop the communication between any two nodes, thus effecting communication integrity. In the fugure 2. communication is taking place between node A and B, the node C is silently intercepting and copying the content of communication between A and B.

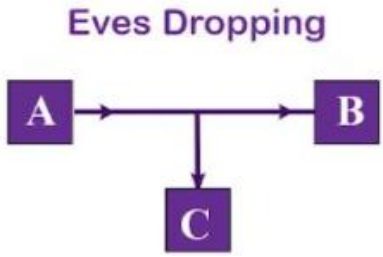

Figure 2 Eves dropping.

Fabrication - Creating illegitimate information, process, and communication as shown in the figure 3. The content

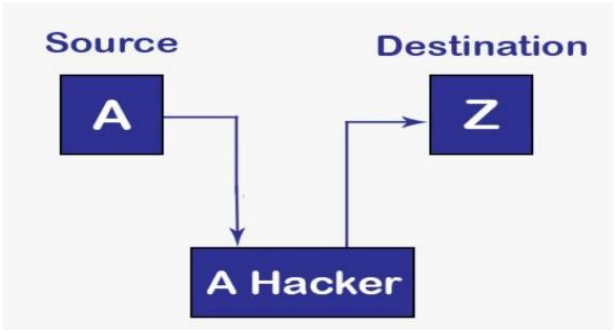

Figure 3. Content fabrication or modification attack.

Route Injection Attack: The attack takes place by diverting the content from actual destination node to another illegal node. As shown in figure 4. the content from node A has to reach node B actually, but due to route injection attack the content gets diverted to node Y.

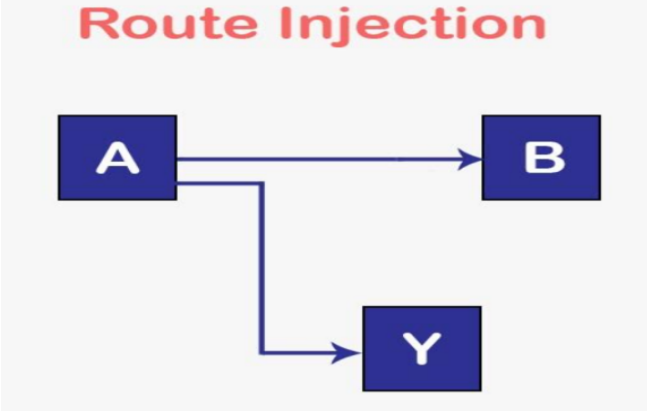

Figure 4. Route Injection Attack

DDOS Attack: The service seeking requests shall be generated from several nodes to consume and exhaust the resources of the target node. As shown in the figure 4, thr node x is under attack from several nodes, as a result node x shall not be able to render any services to the genuine customer nodes.

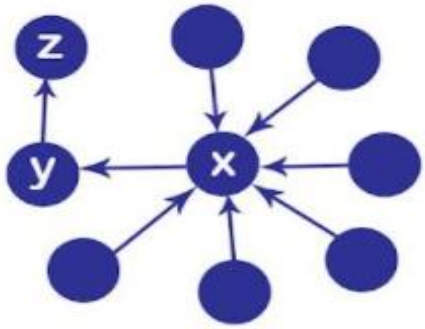

Figure 5. DDOS attack

The trustworthyness of producer or consumer is very important for performing m-commerce transactions, the reviews related to the properties of the product or services and the characteristics, behaviour and attitude are very important in building trust in the m-commerce systems.[21]

The existence of good mobile commerce applications contribute to improved and efficient supply chain management in the industry clusters. [13]

4. RELIABILITY FRAMEWORK OF RAIN

To overcome the problems described, we have introduced innovative distributed device to device network. The distributed network of devices may be structured or un-structured. The un-structure network of distributed devices are not suitable for e-commerce transactions.The structured distributed networks are also not suitable for e-commerce transactions unless they are reliable. The reliability is a vital and essential characteristic of any e-commerce infrastructure.

The RAIN as the title indicates is very in-expensive network of devices. We have deviced and introduced a reliability framework to ensure the desired reliability of any network. This framework can be used to introduce the much needed reliability of the RAIN.

1. Addressability, 2. Availability, 3. Accessibility, 4. Acceptability, 5. Authenticity, 6. Accuracy, 7.Affordability, 8. Alertness, 9. Anonymity-Avoidance, 10. Alignment 11. Advertisement, 12. Assured-Security are the desirable metrics of the device to device D2D network for use for secure reliable e-commerce applications.

Addressibility: Addressability is the ability of a digital device to individually respond to a message sent to many similar devices. CAN - Distributed Hashtable used to ensure the addressibility of each node. Mobile number is the single unique addressability character used in the network.

Availability: It is the ability to provide the requested services to the requested nodes in a reasonable time. The node should be alive and respond quickly to become available. The round trip time (RTT) between the two transacting nodes is the measure of availability of the node. When same service is available from several nodes, the nodes with smaller RTT is preferable to ensure better availability and completion of transaction in time. The RTT is the single character used to indicate the availability.

The figure 6 below shows the framework of reliability.

Figure 6 the reliability framework of Reliable Advanced Inexpensive Network

Accessibility: The transaction services of a given node 'A' are accessible to only to the nodes permitted by node 'A'. When a node offering a new product or service is added to the network, such addition takes place as per the pre-determined membership criteria. At least three existing nodes have to permit the addition of any new node. These three nodes act as scrutinizer, verifier and approver.

Similarly, deletion of any member has to take place based on the recommendation of any three different nodes. The date of deletion also to be mentioned. The member's addition and deletion information to be shared instantly through broadcast mode in real-time. Priority is given to deletion informaiton to avoid frauds or transaction failures. Before performing any transaction, the deletion data and addition data is synchronized with nearby nodes by each node to ensure the trustworthiness of the network and its members.

The mobiles permitted to access the content is also recorded to ensure secure accessibility.

Accessibility Score is Hashvalue of the permitted node numbers.

Acceptability: The acceptability of the transactions to both parties is ensured by avoiding double spending besides the accuracy of the product.

The affordability score gets updated at the end of each transaction for the participating nodes. This information gets propagated to all other nodes in broadcast mode.

The acceptability of the products and goods to end customer is ensured by exchanging product information besides Accuracy information of other member nodes. The double spending is avoided with authenticity information.

Affordability score and Accuracy Score of the participating nodes indicate the Acceptability Score.

Authenticity: Unique mobile number, IMEI numbers of permitted members are recorded.

The total number of members. The number of latest added and deleted member data is exchanged between the nodes. If the data matches, these nodes are ready for transactions. If the data do not match, the data gets exchanged over a period of time. In between transactions takes place among the available authenticated members only.

If a request comes from a un-recorded member in a node to perform the transaction, then request to be sent to the new member about its scrutinizer, verifier approver and any other fourth member. Subsequently, request for 8A criteria related to new member to be sought before performing any transactions from its scrutinizer, verifier, approver and any other fourth member nodes. Transactions to be performed with nodes which have relatively better 8A reliability score. In the absence of information from atleast three member nodes, the request for performing transactions to be denaid.

So unknown nodes, cannot become members, Even if they become due to Benzantine attacks, such members shall not be able to do any transactions. DDOS attacks also can be avoided, as the communication among the nodes is encrypted with special encryption alogorithm as described by the authors in their earlier paper. So new members cannot create and send the specially encrypted content. Even if tried, such messages, get ignored at the outset, so scope for DDOS attacks gets reduced drastically.

Alignment: Alignment is the ability of the large number of network nodes located at various geo-graphical locations to function as nodes of a single network without adverse effects of network size such as transactions latency and integrity. If the network size increases, the directory size in the hashtables also increases proportionately. That will lead to lot of overheads as the network maintenance services shall consume most of the available resources of memory, computation power and bandwidth. This becomes maitain referential integrity of the network directory information. The directory of members and their products are maintained in each node. . So the network directory is maintained geographical region wise. The geographical code, preferably PIN code or ZIP code wise. So the size of directory on each node shall be small, the hashtable sizes shall be small. The Network maintenance overheads shall be small. To small geographical location wise RAIN nodes gets aligned with the geo-graphical codes. The new membership information, and deletion of in-eligible members information gets exchanged among the nodes proactively and periodically among the nodes of particular geo-graphical zone only. So nodes even with smaller directory size, can get aligned with nodes located anywhere in the world. Addition of geographical code in the directory is inderectly is a measure of the alignment index. Because, it facilitates drastic reduction of the directory sizes and thus facilitates sustainability and maintenance of the network. As shown in figure 7, the huge D2D network spread over wide geo-graphical area is constructed with set of internconnected small networks pertaining to smaller geographical areas.

Figure 7 Alignment of smaller networks to compose a bigger wide network.

Accuracy: The Accuracy endorsement information is captured at the end of each transaction from participating nodes. Before each transaction the Accuracy score is checked and transactions are encouraged with nodes with high-endorsement points. The accuracy parameters are related to the characteristics announced by the vending node of the product and the actual characteristics found.The quality of the product, the physical dimensions and other usability characters announced and actual to be verified and Accuracy score to be provided by purchasing node at the end of each commerce transaction.

Affordability: The net-credit worthyness of each node also recorded at the end of each transaction. The amount exchanged to be between the transacting nodes gets converted to the net-credit worthyness of the participating nodes. This information gets broadcasted to all other nodes. Option also facilitated to update this information through any secure API advocated by the central bank such as Bhim API in India, so that the affordability index, in terms of local currency gets updated in real-time.

Earlier the authors have devised a method for supply chain and value chain management, those techniques can be adopted easily for updating the affordability information related to the commodities or products in case of bartering system, as central banks may not deal with the bartering system of trade mostly.

So facility is available for paying money or other equivalent agreed products or commodities to perform the e-commerce transactions reliable through the proposed decentralized network through the RAIN computing.

Alertness: It is the ability to be watchful to promptly prevent, avoid illegal transactions. This is an important criteria, by broadcasting the membership information, each node is alerted about the in-eligible members. As alerts are sent about the creditworthiness score of each member, fraudulent transactions gets prevented. Even if any nodes, do not receive the broadcasted messages about additions and deletions of new members, it can seek proactively, the information abouts its scrutinizers, verifiers and approvers etc., and decide. So there is a double check incorporated in the network. Deletion of member's information should be updated to the nodes, which approved it and which got approved by it. It is a built in characteristic of the RAIN. To avoid communication overheads, no seperate metric is used to measure and store value of this characteristic mandatorily. However, if required,

and affordable resources and time are available, then special score can be also given to alertness index.

Anonymity Avoidance: Anonimity is avoided and prevented by ensuring authentic members are permitted into the network especially for e-commerce transactions. A directory of authentic admitted members and deleted members is maintained and exchanged, as and when new members are added or any existing nodes are deleted. In case of enrolling a member node, which is a producing node or trading node, then, its physical coordinates are also mandatorily obtained and recorded in the respective nodes. This information is cross checked with the GPS coordinates of the device, if there is match then only member gets admitted. Geo-fencing or coordinates are index of Anonymity Avoidance. However, by encrypting the content as advocated by authors earlier, privacy of the identiy information shall be gets ensured.

Advertisement: The products or services being offered are to be advertised to the member nodes by the producer nodes. The consumer nodes which are potential customers or consumers to the advertised service can approach the producer node directly. Along with the membership information, the product codes are also recorded. Producer if producing a product, trading is a type of service / product, if a node is involved simply in trading, then, product code given is related to the trading code. Though it is preferable to procure products from the producers directly to get better price, but to ensure delivery of product with high accuracy, a trader near to the end consumer is preferable.

5. THE EXPERIMENTATION DETAILS

The RAIN sytem was implemented using 100 devices in Telangana State in India for over a year. The savings in terms of CAPEX is very very huge. The reliability framework was imposed as a result, we could overcome the Benzatine problem, as only accurate authentic information was permitted. The content was verified and approved by the nodes apriori. Nodes with verified reliable content only were considered for inclusion in the network. To update the content related to products or customers, the encrypted messages were exchanged between appropriate nodes. Both the nodes exchange tokens for doubly confirming the of exchange of the content. The results of the experiment related to one of the fairprice shop having number 1674498 were tabulated. The experimentation data of the real m-commerce transaction times were recorded. Due to space constraints only few sample records of the experiments were shown in the tables. The table1 shows data related to January 2020, the table 2 shows the data related to December 2019 and the table 3 shows the data related to November 2019.

The m-commerce transaction times obtained from the locations where the RAIN computing based devices were introduced, were compared with the m-commerce transactions times of the legacy systems by preparing the charts.

The average transaction time of the legacy system is 293 milliseconds. The average transaction time of new innovative low cost device based computing solution is around 155 milliseconds during January, 2020, December 2019, and also November 2019.

The average transaction time of the legacy system is a bit higher due to one additional process. So on the average, the new innovative solution is as effective as the established, data centre infrastructure intensive, CAPEX and OPEX intensive, legacy solution.

Similar results were obtained when the data was compared with the transactions data pertaing to any other randomly selected shop, among the 100 shops where the experiment was carried out.Table 1. below shows the transactions times of a few transactions recorded at Shop 167449 during January 2020.

The figure 8 shows the comparision of the average transaction times of legacy system and the new experimental system as a bar diagram.

Table 1. The transactions times of each transaction recorded at Shop 167449 during January 2020.

Transactions using Dealer's Mobile(ShopNo 1674498) from 11th Jan,2020 to 15th Jan, 2020							
Trans_id	**RC_No**	**Shop_no**	**Month**	**Year**	**Trans_Start_time**	**Trans_end_time**	**Trans_time_in_seconds**
20011109135533235	365360399716	1674498	1	2020	2020-01-11 09:12:45.07	2020-01-11 09:13:55.187424	70.11742
20011109452835128	365360410113	1674498	1	2020	2020-01-11 09:45:14.31	2020-01-11 09:45:28.166368	13.85637
20011109481435294	365360410047	1674498	1	2020	2020-01-11 09:47:51.907	2020-01-11 09:48:14.953457	23.04646
20011109534835628	365360410344	1674498	1	2020	2020-01-11 09:51:58.724	2020-01-11 09:53:48.533975	109.80998
20011109573135851	365360410122	1674498	1	2020	2020-01-11 09:57:12.386	2020-01-11 09:57:31.570389	19.18439

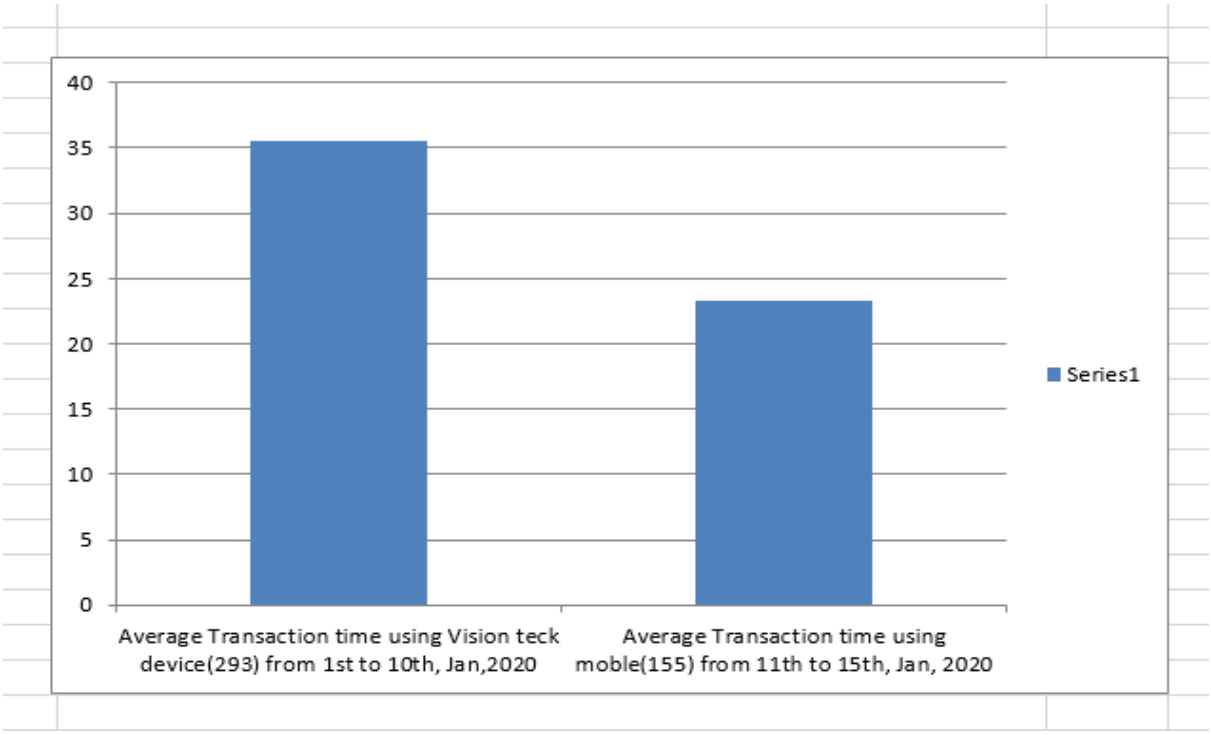

Figure 8. The Comparision of Transaction Times of Legacy system and New System

6. CONCLUSION

Each node of RAIN, provides defined m-commerce services named by keys like a bucket in classic hash tables, and it employs the proposed innovative reliability framework to search and collaborate with other nodes to ensure deliverables reliably. This simple and elegant mechanism makes RAIN a potential universal building block for many distributed system applications such as m-commerce.

Acknowledgments: The authors thank the owners of the 100 shops who have taken part successfully in the pilot research project besides other team members.

7. REFERENCES

[1] Attacks - Types of Attacks [WWW Document], 2021. . Engineering LibreTexts. URL https://eng.libretexts.org/Courses/Delta_College/Information_Security/01%3A_Information_Security_Defined/1.4_Attacks_-_Types_of_Attacks (accessed 5.20.22).

[2] Chowdhury, F., Furness, J., Kolberg, M., 2017. Performance analysis of structured peer-to-peer overlays for mobile networks. Int. J. Parallel Emerg. Distrib. Syst. 32, 522–548. https://doi.org/10.1080/17445760.2016.1203917

[3] Dabek, F., Cox, R., Kaashoek, F., Morris, R., n.d. Vivaldi: A Decentralized Network Coordinate System 12.

[4] Dhamodharan, U.S.R.K., Vayanaperumal, R., 2015. Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method. The Scientific World Journal 2015, e841267. https://doi.org/10.1155/2015/841267

[5] Fantar, S.G., Youssef, H., 2009. Locality-aware Chord over Mobile Ad Hoc Networks, in: 2009 Global Information Infrastructure Symposium. Presented at the 2009 Global Information Infrastructure Symposium, pp. 1–6. https://doi.org/10.1109/GIIS.2009.5307057

[6] Feldman, S., 2000. Mobile Commerce for the Masses. IEEE Internet Computing 4, 74–75.

[7] Garcia Lopez, P., Montresor, A., Epema, D., Datta, A., Higashino, T., Iamnitchi, A., Barcellos, M., Felber, P., Riviere, E., 2015. Edge-centric Computing: Vision and Challenges. SIGCOMM Comput. Commun. Rev. 45, 37–42. https://doi.org/10.1145/2831347.2831354

[8] Ginter, K.L., Shear, V.H., Sibert, W.O., Spahn, F.J., Wie, D.M.V., 2011. Systems and methods for secure transaction management and electronic rights protection. US8055913B2.

[9] Girlich, F., Rossberg, M., Schaefer, G., Boehme, T., Schreyer, J., 2013. Bounds for the Security of the Vivaldi Network Coordinate System. Presented at the Proceedings - International Conference on Networked Systems, NetSys 2013, pp. 66–75. https://doi.org/10.1109/NetSys.2013.21

[10] Jo, M., Maksymyuk, T., Strykhalyuk, B., Cho, C.-H., 2015. Device-to-device-based heterogeneous radio access network architecture for mobile cloud computing. Wireless Communications, IEEE 22, 50–58. https://doi.org/10.1109/MWC.2015.7143326

[11] Leong, B., Liskov, B., Demaine, E.D., 2004. EpiChord: Parallelizing the Chord Lookup Algorithm with Reactive Routing State Management, in: In Proceedings of the 12th International Conference on Networks. pp. 1243–1259.

[12] Liu, J., Pan, B., Zhang, X., Li, D., 2021. Mobile E-Commerce Information System Based on Industry Cluster under Edge Computing. Mobile Information Systems 2021, e7930799. https://doi.org/10.1155/2021/7930799

[13] Manian, Z.N., n.d. (71) Applicant: SkuChain, Inc., Mountain View , CA (US) 27.

[14] Ng, T.S.E., Zhang, H.,n.d. A Network Positioning System for the Internet 15.

[15] Rajasekhar, K., Upadhyaya, N. (2014). Modified Real-Time Advanced Inexpensive Networks for Critical Infrastructure Security and Resilience. In: Satapathy, S., Avadhani, P., Udgata, S., Lakshminarayana, S. (eds) ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol II. Advances in Intelligent Systems and Computing, vol 249. Springer, Cham. https://doi.org/10.1007/978-3-319-03095-1_84

[16] K. Rajasekhar and N. Upadhyaya, "Communication Security in Real-Time Advanced Inexpensive Networks," *2014 International Conference on Devices, Circuits and Communications (ICDCCom)*, 2014, pp. 1-6, doi: 10.1109/ICDCCom.2014.7024704.

[17] Rajasekhar, K., Upadhyaya, N. (2016). Low-Cost Supply Chain Management and Value Chain Management with Real-Time Advance Inexpensive Network Computing. In: Satapathy, S., Raju, K., Mandal, J., Bhateja, V. (eds) Proceedings of the Second International Conference on Computer and Communication Technologies. Advances in Intelligent Systems and Computing, vol 380. Springer, New Delhi. https://doi.org/10.1007/978-81-322-2523-2_68

[18] K. Rajasekhar and N. Upadhayaya, "Data driven mobile commerce intelligence: With real-time advanced inexpensive network computing," *2014 International Conference on Data Science & Engineering (ICDSE)*, 2014, pp. 6-11, doi: 10.1109/ICDSE.2014.6974603.

[19] Saia, J., Fiat, A., Gribble, S., Karlin, A.R., Saroiu, S., 2002. Dynamically Fault-Tolerant Content Addressable Networks, in: Druschel, P., Kaashoek, F., Rowstron, A. (Eds.), Peer-to-Peer Systems, Lecture Notes in Computer Science. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 270–279. https://doi.org/10.1007/3-540-45748-8_26

[20] Sarkar, S., Chauhan, S., Khare, A., 2020. A meta-analysis of antecedents and consequences of trust in mobile commerce. International Journal of Information Management 50, 286–301. https://doi.org/10.1016/j.ijinfomgt.2019.08.008

[21] Shu, X., Li, X., 2012. A Scalable and Robust DHT Protocol for Structured P2P Network. IJCNS 05, 802–809. https://doi.org/10.4236/ijcns.2012.512084

[22] The IBM Cyclops-64 Architecture [WWW Document], 2013. URL https://web.archive.org/web/20130606000628/http://www.capsl.udel.edu/~venetis/Cyclops-64.html (accessed 4.20.22).

[23] Wararkar, P., Kapil, N., Rehani, V., Mehra, Y., Bhatnagar, Y., 2016. Resolving Problems Based on Peer to Peer Network Security Issue's. Procedia Computer Science, 1st International Conference on Information Security & Privacy 2015 78, 652–659. https://doi.org/10.1016/j.procs.2016.02.113