[1]Vimal A. Rathod
[2]Dr. C. A. Patel

An Analysis of Location-Based Techniques of Authentication for Internet of Things

Journal of Electrical Systems

Abstract: - Internet of things is the concept which is going to be generalized in our daily-life. As IoT is the moving towards becoming one of the essential requirements for any system, it is required to make device as well as user authentication. As the number of devices increases the problem of authentication Location-based authentication is a technique with can be used for detecting the device location and authenticating them to the network they visit and allowed to do their task. An IoT device can be in static position or in dynamic position. Authenticating device in static position is quite easy task but this easiness is not applied if the device is in moving or dynamic position. The study will discuss about available techniques for authentication of device which is in continuously moving condition. There are many ways to identify location of the device like using Global Positioning System, using location tag, co-location-based identification and many more. The study includes location-based authentication techniques which incorporate the inhouse as well as outdoor location detection and authentication techniques. The intension behind the study is to find out the most prominent and convenient technique for location-based authentication.

Keywords: location-based authentication, Internet of Things, location tag, co-located address, global positioning system

I. INTRODUCTION

The technology of the new era is the internet of things. People always like to be connected with Internet and they want their devices to be connected with internet always. This concept allows people and devices to communicate with each other. It can build a sizable network of smart gadgets, and all of the devices can talk to one another to make life easier for people. Actuators and sensor networks are examples of physical devices in the IoT ecosystem, and other software settings are used in a variety of applications, including medical, industrial, civic, etc. [40]. In order to interact with a wide number of devices and give users trusted gains in the smart environment, embedded devices are integrated with IoT [41]. As per discussion about the interfacing of various devices, there is a need to consider a number of factors, including communication protocols, authentication, authorization, and the security of the devices given that they are all connected to the Internet and each other. But in this case, the study only focuses on authentication.

Authentication plays very important role in making the system secure. There are many ways to do authentication [1]:

- Password-based Authentication
- Biometric Authentication
- Location-based Authentication
- Multi-factor Authentication

The information for each of the aforementioned types of authentications is provided below:

A. Password-based Authentication

In this type of authentication, the user gives the system their username and password. Depending on whether the credentials provided are valid, the system verifies them in its database and either approves or rejects the user's admission [2].

* [1]*Research Scholar, Computer/IT Engineering, Gujarat Technological University, Ahmedabad-382424, Gujarat, India*
Email: vimalrathod1982@gmail.com
[2]*Professor,Information Technology Department, L.E College, Morbi, Gujarat,*
*IndiaEmail:prof.capatel@gmail.com *Corresponding Author*

B. Biometric Authentication

A real person's identification can be verified or recognised automatically using "biometric technologies" based on a physical or behavioural trait [42][43]. It is used to authenticate utilising some physical characteristics; examples include facial recognition, iris scanning, fingerprinting, and retina scanning [3].

C. Location-based Authentication

It is an extremely sophisticated form of authentication used with particular kinds of gadgets. By verifying their location, it is utilised to authenticate IoT devices. One of the first authors to conduct research studies on location-based authentication and to emphasise its significance for enhancing network security was Denning and Macdorman [39]. Location-based authentication can be done using a variety of methods [4]. It is now possible to pinpoint a user's location to within a few metres of where they actually are [38]. Numerous systems already in existence use location data to offer authentication and authorization solutions. These solutions, however, typically call for a specially created infrastructure as well as unique tools that may be used to pinpoint their positions [35] [36] [37].

D. Multi-factor Authentication

Multifactor authentication is a security-related technique that verifies a user's identity using numerous authentication types from multiple independent sources and using various credentials [44,45]. Logins and transactional needs are where the MFA is primarily used [46][47]. The main objective of MFA is to create a multi-layered defence that makes it impossible for an unauthorized person to access the device, location, network, and database [48]. In order to completely compromise the applications and systems through software and hardware, the attacker, hacker, or simply the unauthorized person must get through one or more protection layers if one of the barriers or layers is accessible. The development of multiple authentications was primarily motivated by the need to improve the security and integrity of digital transactions [49,50]. To increase security, this sort of authentication can be used to perform authentication based on numerous factors [5].

II. RESEARCH REVIEW: STATE OF THE ART

Devices that are in a specific area are identified using location-based authentication. When a device enters the range, it is detected, and only devices that have been registered with the trust authority are permitted to pass the barrier. Devices can be any kind of intelligent vehicle, including a smart bicycle, car, or other sort of vehicle. However, the study is not restricted to just vehicles; any device that has accurate location identification can be present. Different kinds of location-based authentication exist. Following are the types of it:

- Location Tag-based authentication
- RSSI-based Authentication
- Hub-based Authentication
- Co-located Device Information based authentication

Details about each authentication technique is given below:

A. Location-Tag based authentication

Location-based information is becoming increasingly necessary for a variety of businesses as wireless communication technologies advance [6]. The user's location can be utilised as an additional factor of identification in situations where physical closeness is necessary, including when engaging in in-person transactions or unlocking a car. To rely only on username and password is not a safe way for authentication, there is a need to add location as an addition factor for the same [7]. Location-based authentication is implemented using geo spatial location tag [20], fuzzy extractor, bloom filter and a unique key-checking function [14].

Location tags are nothing but a special kind of location representation. They can be produced by gathering wireless and cellular signals from the environment. Location tags are seen as evidence that a point is related to another in terms of space and time. They can be used to provide location privacy. For regular users, location privacy is a major

concern. The main reason is that the location servers are frequently run by outside service providers, including cloud platforms, who customers don't always entirely trust [21].

During location authentication, the requester and IoT devices automatically exchange secret keys using the lightweight cryptographic primitive fuzzy extractor [8].

The location tags are laconically expressed using Bloom Filters. It is a space-efficient probabilistic data structure that enables membership queries with a low false positive rate [9]. It has been used to facilitate forwarding and routing [22] [23] [24]. Web caching [25] [26] [27] [28], distributing content [34], network monitoring [35], security enhancement [36] [37], etc.

A novel key checking function is used to estimate if the secret key got from the candidate is the same as the secret key from the requester. It is a discrete logarithmic problem which is used to verify the keys.

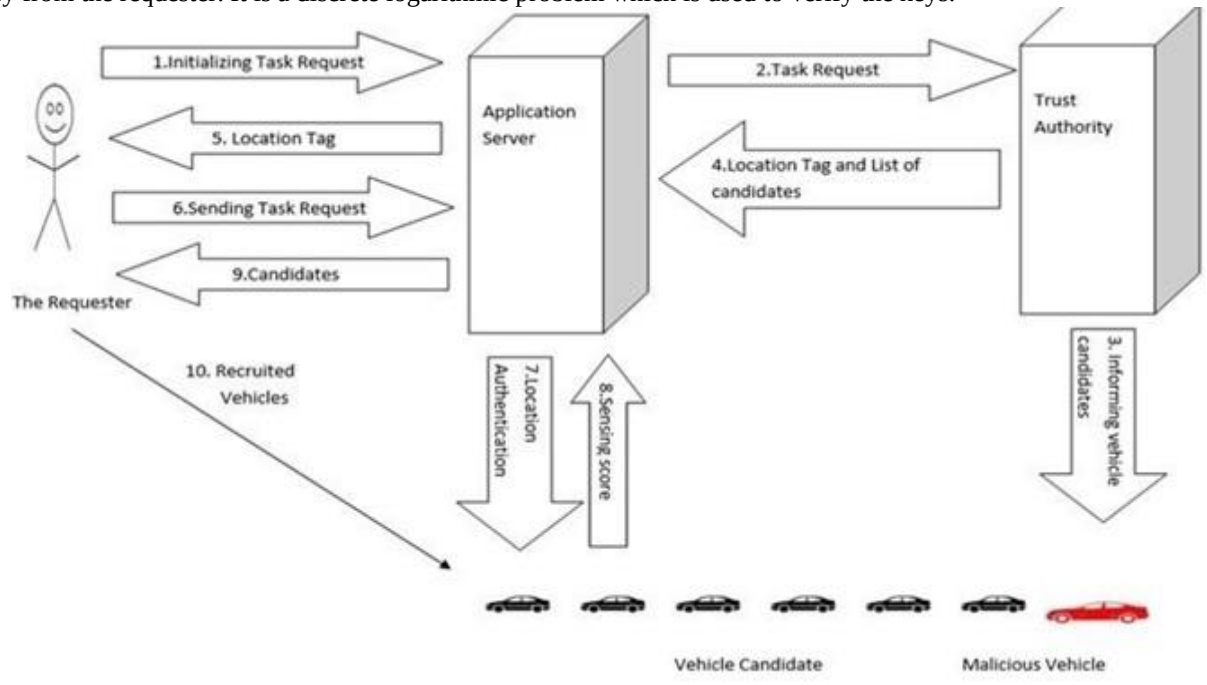

Fig.1 Vehicular Crowdsensing System Model[14]

Vehicular Crowdsensing System

To achieve secure tasking or privacy-reserving navigation, numerous academics have worked to propose security and privacy protection techniques for vehicular crowdsensing. The secrecy of both crowdsensing tasks and reports must be guaranteed. Studies like [19], [18], and [17] only focused on the privacy of user-collected sensing data. The vehicular crowdsensing system is depicted in Figure 1. The four major participants in the system are the requester, application server, trust authority, and vehicle candidates.

The application server that is registered with the trust authority receives the request from the requestor, who is carrying out a sensing task S. The trust authority will choose a few vehicles that are actively taking part in the crowdsensing, with V= "V1,..., Vn," and will then return the set to the application server. During the process of participant recruitment, the requestor develops Evaluation Criteria and sends it to all candidates by server.

All the concerned members(candidates) calculate their own sensing score and encrypt using extracted key for the recruiter to make recruited decision.

During the process of location-based authentication, the requestor sends a set of all required security parameters and the task's location tag with embedded encoded secret key to the application server. Then the Application server broadcasts the message to vehicle candidates. The candidates generate their own location tags and try to extract the secret key for completing location-based authentication.

B.RSSI-based Authentication

Location-based authentication is done with the help of signal characteristics like RSSI (Received Signal Strength Indicator). Let's see how the RSSI-based authentication plays roles in detection of the Bluetooth and Wi-Fi devices in the trusted zones. It has been applied to the LocAuth (Location Authentication) system for detection of devices in the trusted zones made in the same building [6]. Let's discuss the LocAuth system to understand the significance of the RSSI.

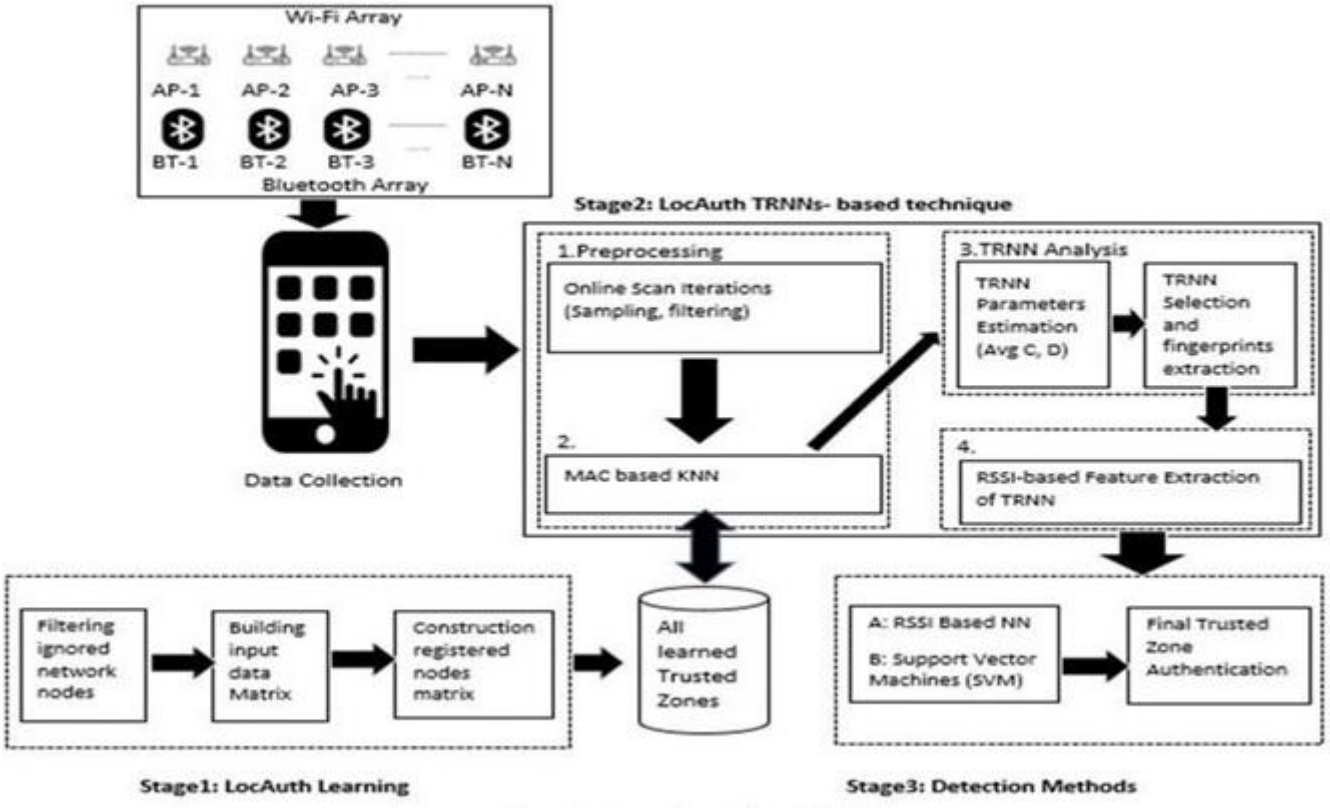

Fig.2 Overview of LocAuth [6]

LocAuth System: Figure 2 depicts a general view of the LocAuth system, which divides the entire procedure into three primary phases that are carried out sequentially as follows:

- LocAuth Learning: Stage one is in charge of collecting fingerprints at each trusted zone for protracted intervals of time. The researchers perform three steps in succession during the stage, which include (1) creating the input data matrix from all network nodes observed at each trusted zone, (2) determining the sampling period and removing any unnecessary network nodes, and (3) creating the wireless characteristic

data of only the registered network nodes[6]. Finally, the database contains the fingerprints of each learnt trustworthy zone in the space.

- LocAuth TRNNs-based technique: consists of the following steps: (1) online scan processing; (2) K-nearest neighbors (KNN) trusted zone selection from all learned trusted zones stored in the database based on MAC addresses; (3) inferring the Top Ranked Network Nodes (TRNNs) fingerprints of the selected KNN trusted zones; and (4) extracting RSSI-based features from the inferred TRNNs[6].
- Detection methods: It is in charge of identifying the last trusted zone that verifies the user's identity. RSSI-based Nearest Neighbors (NN) shown in Figure 3 and Support vector machines (SVMs) are two alternative detection techniques that will be used to accomplish this. By measuring the distances between online fingerprints and those of learnt trusted zones recorded in the database, the researchers deploy RSSI-based NN as a detection tool [6].

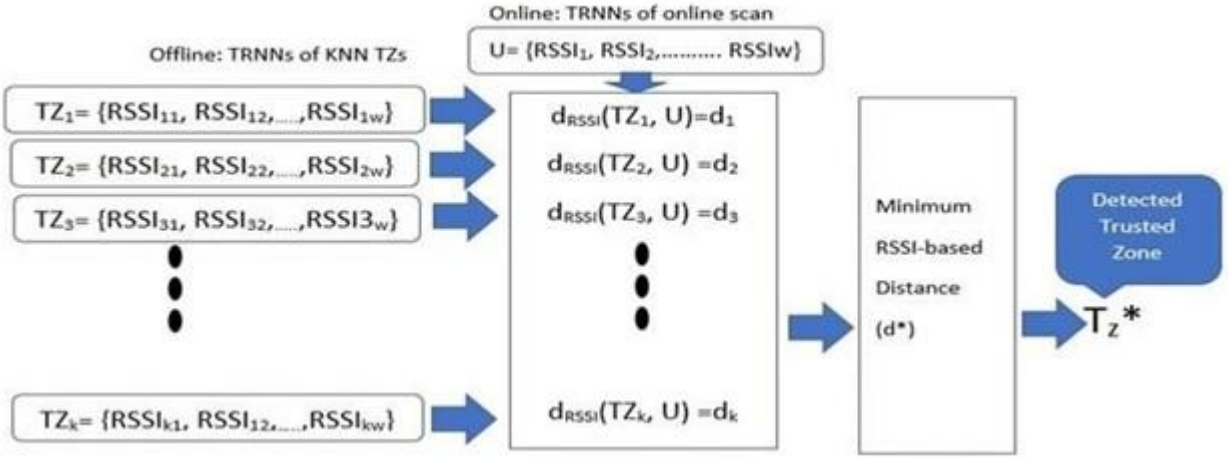

Fig.3 Illustration of RSSI-based nearest neighbor detection method [6]

C.Hub-based Authentication

This approach is focusing on retrieving user location and authentication based on their actual location. One system called Icelus is created to authenticate user by his/her location. Icelus arranges all the IoT devices in to a hierarchy, where powerful IoT devices collects data from small devices. In turn those devices send data to the hub where the Icelus service is running. Figure.4 describes the architecture.

The Icelus Hub

It serves as the Icelus system's brain. It has been assumed that the user has control over it, making the information acquired inaccessible to outside parties. It is assumed that it is either a smart home hub [11] or located on the cloud [10]. Cloud hosting is available to us with all of its advantages and disadvantages. The cloud provider may be curious or compromised, but the researchers assume that it is not harmful.

The User Owned Devices

All the devices are classified according to their characteristics for the Icelus system as below:

- Trinkets can connect directly or indirectly with the Internet. Smart phones, smart watches and even internet connected cars can be included in the list of trinkets [12]. To connect to the system, Trinkets must first register with the Hub; during this process, the parties exchange public keys. Then, the Hub uses its public key to encrypt data being transmitted, and the Trinket digitally signs all of the data it reports using its private key.
- While fragments resemble trinkets, they cannot be directly connected to the Internet. However, they can directly connect to a Trinket (for instance, using Bluetooth). These gadgets could be in-body devices or smart wearables for the wrist like Fitbits or other smart footwear. The IoT contains a wide variety of Fragments. They are more similar to Trinkets in that they can register with the Hub and sign their data,

even if they still depend on a Trinket to communicate their data to the Hub, depending on whether it is possible to install additional client software on them. A shared secret key can be established with the Hub to use more straightforward data signing algorithms if public-key cryptography is not practical. The majority of the functions of other Fragments devices, however, depend on Trinkets. A Trinket might only be able to notify the presence of a Fragment in the most limited scenario (such as using BLE tags [13]).

- A token is a physical item that is unable to actively connect to any device, including smartcards, magnetic identification cards (sometimes called swipe cards), RFID tags, etc. The only way to view passive tokens, which are typically something other than a reader, is through another device.

Beacons

A person or one of his devices can report information about their whereabouts using beacons, which are external devices or even complete systems. Reports may be produced after a user engages a beacon or while a user's device is being observed. For instance, while credit card usage at POS or putting in valid authentication information at a terminal, the user engages with a beacon. When a user's smart phone authenticates with a Wi-Fi hotspot, a beacon observes the device. Both times, Beacons' precise location is known. To push observation data to the Hub, services connected to beacons must first register with it. It is feasible to extract data that is already present in other channels, though. Many banks transmit credit card usage statistics through SMS or email to locate Tokens like credit cards, for example [7].

Avatars

An avatar serves as a digital representation of a user's perceived position in the real world. Even Trinkets that are not with the user will construct their own Avatars since every Trinket that sends geospatial data tries to produce an Avatar there, which it then joins with all of its slave Fragments. All nearby technology will be unified by a single avatar. The current commercial GPS technology's worst-case [15] accuracy can be used to represent the same region as a circle with an 8-meter radius and a centre situated at the last Avatar location coordinates. A token is connected to the Avatar present at the site of the report when it manifests as a result of a beacon or another device's observation. When utilised, tokens only momentarily appear; as a result, they stay tied to the associated Avatar until a new report on them is obtained. Wherever tokens are observed, a new avatar is formed when they appear far from existing avatars. Our system's assessment of how well an avatar represents a user is reflected in its confidence score [7].

Querying Locations for Servicing - Sites

The ability to run a system query to determine if it is practical to be present for a user at a particular area belongs to sites. The user is the owner of any Site, any Party (including the user's bank or organization), Icelus itself, or any Third Party (including the Trinkets connected to the user's home or vehicle). Sites must register with the Hub and receive user authorization by listing the areas they wish to publish questions for before they are allowed to receive inquiries.

The Hub keeps track of site requests using the semantic structure "Could the user be at place L??" Trinkets is asked to report any new information in response to a query. The system can then wait for a finite period of time while receiving additional information and updating its model of potential user locations. It should be emphasized that the model is updated frequently regardless of Having devices report on a regular or ad-hoc basis will allow you to determine if there have been any requests. The only variable is the age of the decision-making model, which could be a few minutes or a few milliseconds old, hence Icelus can always reply in a finite length of time.

After then, the Hub looks to see whether there is an Avatar in a location other than L with a confidence score greater than the Site's defined rejection threshold. The threshold can also be set globally. The idea is flexible; other rules can be implemented and further information can be added when responding to requests. If a consumer's device has such a feature, for instance, Icelus can alert them and encourage them to log in rather than immediately taking action against them[7].

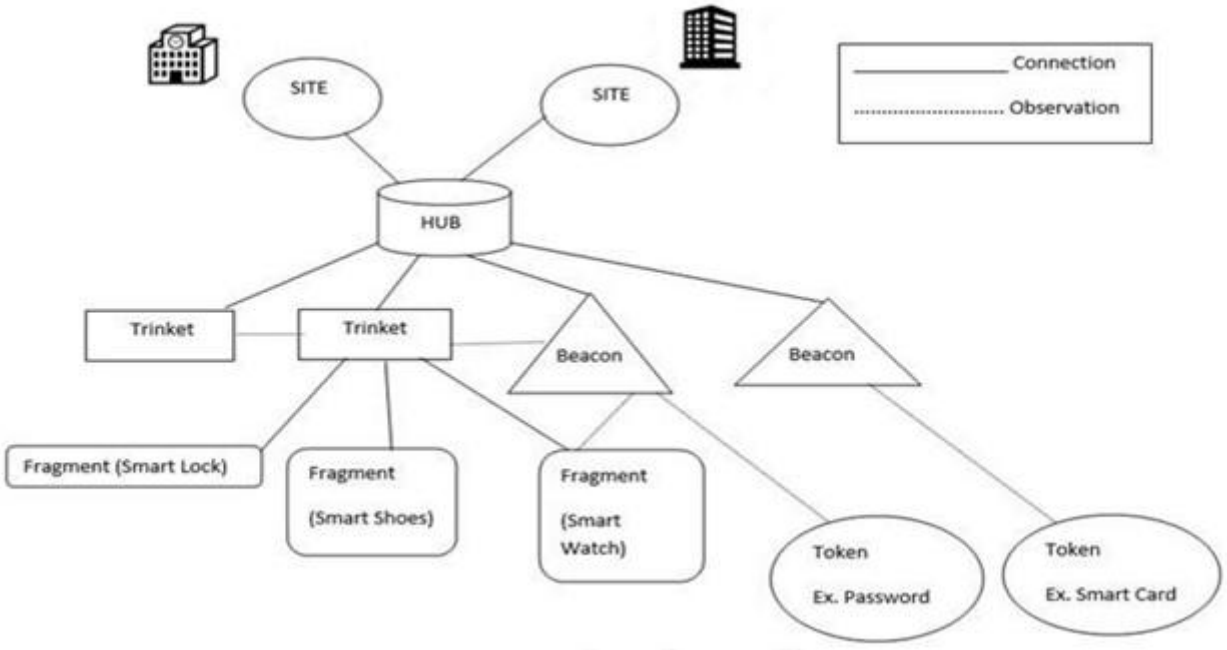

Fig.4 Icelus Architecture [7]

D. Co-located Device Information based authentication

The machine-learning technique employed in this study for authentication is shown in detail in Figure 5. The general procedure depicted in the diagram is typical of machine learning; nevertheless this study's method for collecting characteristics from sensed-context bags is distinctive to it [16].

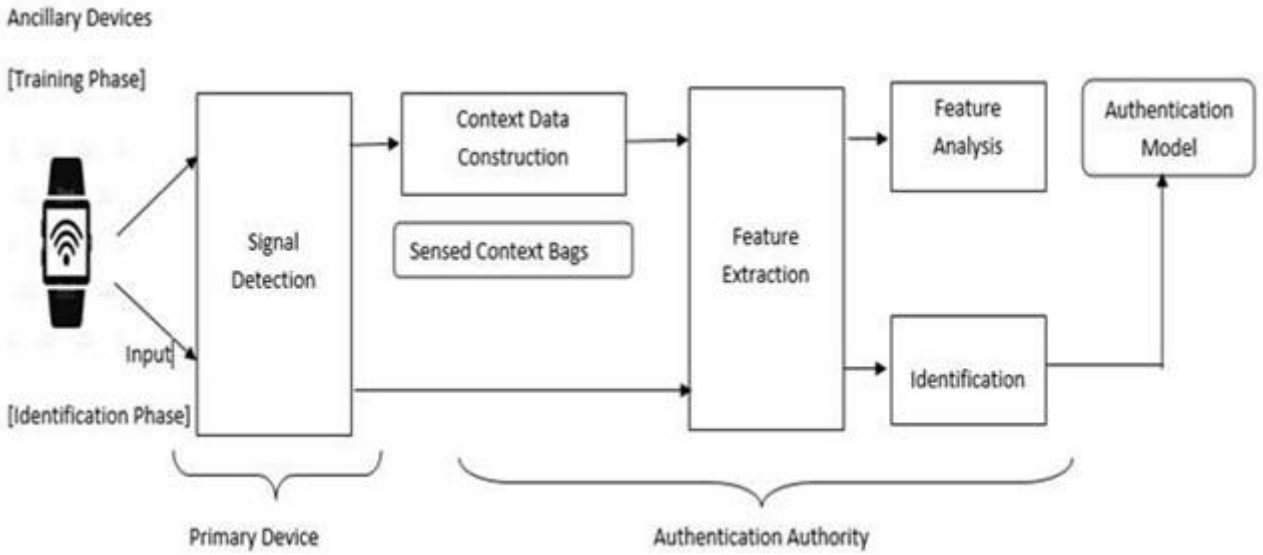

Fig.5 Authentication technique using Machine Learning [16]

The development of a sensed-context bag is triggered by a user's primary device during the training phase, and if the user has already authenticated with the system, the sensed-context bag is linked to the user's identification. When the primary device detects the radios of ancillary devices in the user's device context when the user is online or in the office on the primary device, the system generates bags storing the sensed-context records of genuine, authenticated users. The system keeps track of the various users' perceived context packs. The authentication authority uses the data set of a sensed-context bag and a user identification related to one another to extract the features, creating a model for each bag to identify the person. The authentication models can then be used to determine if an action taken by a user in a certain device environment without authentication corresponds to an action taken by an authorised user who is subject to control by the authentication authority [16].

Using the authentication model developed during the training phase, the proposed system attempts to identify a specific user during the identification phase. When a user does an action on their primary device, such as browsing a webpage in a particular device context, the authentication authority extracts the user's features from sensed context data that was acquired concurrently with the access. The authority determines whether the extracted features are compatible with the authentication model and determines the degree to which the model accurately predicts the user's behaviour. It then uses a threshold for the estimated confidence to decide whether the user is legitimate [16].

The bag technique employed in this study is novel since it allows continuous, implicit authentication from a practical standpoint, despite the fact that the aforementioned procedure follows a general machine-learning process.

III.COMPARISON

After discussing various location-based authentication strategies in the study, let's compare them to see how they differ and how they might be used in authentication. Table 1 displays the comparison.

Table 1: Comparison of Available Approaches for Location-based Authentication

Sr. No	1	2	3	4
Authentication Technique	Location Tag-based authentication	RSSI-based Authentication	Hub-based Authentication	Co-located Device Information based authentication
Techniques used for Location Detection	spacial-temporal location tags andfuzzy extractor	GPS, WIFI Capability, Bluetooth	Mobile phone location	identifies user based on co-location information
Authentication Mechanism	spatial-temporal location tag, fuzzyextractor, key transmission	RSSI-based nearest neighbors, supervised machine learning algorithm.	A movement model	Context Aware Authentication
Where the location data will be stored	Server	Data is stored in text files labeled with trusted time zone and date/time.	cloud/ Icelus hub	sensed context bags
Provides protection against which attacks	Location Cheating	attacks in sensitive locations	security tokens,biometrics and compromising passwords	Stalking/Tailgating, Stealing, Fake device provisioning, Context GuessingAttack
Benefits	provides time efficiency and privacy guarantee	highly accurate and effective approach	the device user's location can be detected even if it is unreachable.	Perform with accuracy in in-house environment
Challenges	Minimize crowd sensing data storage and	Very small area is covered	compromising passwords, security tokens or biometrics	Provide protection against context replay attack

	cryptographic overhead			
Future Work	privacy protection of data collected	exploit lights and soundsof the surrounding environment	Learn habits of user forfuture to identify probability of a location of a person	Mechanism to incorporate physical context

III.CONCLUSION

The study has discussed various techniques of location-based authentication. In the study, there is a comparison of all of them according to various criteria. All of them are working with the location-based authentication. In the first method it has been observed that the authentication was based on location tags which a special kind of geo-spatial representation of location and by the use of them different vehicles were being identified and authenticated. In the second approach devices were being identified based on the received signal strength characteristics and also the use of machine learning technique to authenticate the device. For the third technique, all the devices are authenticated by a special kind of hub called Icelus. In the last approach devices are authenticated by the use of sensed context bags. All the approaches were working on location-based authentication. According the need and the situation we can prefer one of them. The challenges and future work also discussed. This survey will be benefited to the scholars who wants to explore in the field of authentication in IoT.

IV.REFERENCES

[1] Sreenivasa Rao Basavala, Narendra Kumar, Alok Agarrwal, "Authentication: An Overview, its types and Integration with Web and Mobile Applications", 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.

[2] Aybek Imamaliyev, Zarif Khudoykulov ,"Analysis Password-based Authentication Systems with Password Policy",2021 International Conference on Information Science and Communications Technologies (ICISCT).

[3] Asadullah Laghari, Waheed-ur-Rehman, Dr. Zulfiqar Ali Memon ,"Biometric Authentication Technique Using Smartphone Sensor", 2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST).

[4] Feng Zhang, Aron Kondoro, Sead Muftic ,"Location-based Authentication and Authorization Using Smart Phones",2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[5] Yue Guo, Yuan Liang, Yan Zhuang, Rongtao Liao, Liang Dong, Fen Liu, Jie Xu, Xian Luo, Xiang Li, Wangsong Ke, Guoru Deng ,"A security protection technology Based on Multi-factor authentication", 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC).

[6] Mohsen A. Alawami, , Hyoungshick Kim, "LocAuth:A Fine-grained Indoor Location-based Authentication System using Wireless Networks Characteristics", Computers and SecurityVolume 89,Issue C,01 February 2020.

[7] Ioannis Agadakos,Per Hallgren,Dimitrios Damopoulos,Andrei Sabelfeld,Georgios Portokalidis, "Location-enhanced Authentication using the IoT", ACSAC '16: Proceedings of the 32nd Annual Conference on Computer Security Applications, December 2016,Pages 251–264.

[8] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data Advances in Cryptology" - EUROCRYPT 2004 Conference paper.

[9] L. Luo, D. Guo, R. T. B. Ma, O. Rottenstreich, X. Luo,"Optimizing Bloom Filter: Challenges, Solutions, and comparisons", IEEE Communications Surveys & Tutorials, Volume 21, Issue 2,23 December 2018, Pages 1912-1942.

[10] Microsoft. Event hubs. Microsoft Azure. http://azure.microsoft.com/en-us/services/event-hubs/.

[11] Insteon. Insteon hub. http://www.insteon.com/insteon-hub/.

[12] B. Cooley. Cadillac rolls out in-car Internet access. c|net,2009. http://www.cnet.com/news/cadillac-rolls-out-in-carinternet-access/.

[13] Find your phone, keys, anything. Tile, September 30 2016.https://www.thetileapp.com.

[14] Danxin Wang, Chuanhe Huang, Xieyang Shen, Naixue Xiong ,"A General Location-Authentication Based Secure Participant Recruitment Scheme for Vehicular Crowdsensing Computer Networks",Volume 171, 22 April 2020, 107152,

[15] US AirForce. GPS Accuracy.http://www.gps.gov/systems/gps/performance/accuracy/.
[16] Hidehito Gomi, Shuji Yamaguchi, Wataru Ogami, Teruhiko Teraoka and Tatsuru Higurashi ,"Context-Aware Authentication Using Co-Located Devices",Yahoo Japan Corporation, 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)
[17] G. Zhuo, Q. Jia, L. Guo, M. Li, P. Li, "Privacy-preserving verifiable data aggregation and analysis for cloud-assisted mobile crowdsourcing", in: IEEE INFOCOM, 2016, pp. 1-9.
[18] Q. Wang, Y. Zhang, X. Lu, Z. Wang, Z. Qin, K. Ren, "RescueDP: Real-time spatio-temporal crowd-sourced data publishing with differential privacy", in: IEEE INFOCOM, 2016, pp. 1-9.
[19] X. Jin, Y. Zhang, "Privacy-preserving crowdsourced spectrum sensing",IEEE/ACM Trans. Netw. 26 (3) (2018) 1236-1249.
[20] Y. Zheng, M. Li, W. Lou, Y. T. Hou, "Location Based Handshake and Private Proximity Test with Location Tags", IEEE Trans. Dependable Sec. Comput. 14 (4) (2017) 406-419.
[21] X. Liang, R. Lu, L. Chen, X. Lin, and X. Shen, Pec: "A privacy preserving emergency call scheme for mobile healthcare social networks", Journal of Communications and Networks, vol. 13, no. 2, 2011.
[22] F. Angius, M. Gerla, G. Pau, "Bloogo: Bloom filter based gossip algorithm for wireless NDN", in Proc. ACM workshop on Emerging Name-Oriented Mobile Networking Design-Architecture, Algorithms, and Applications, Hilton Head, SC, USA, 2012
[23] A. Marandi, M.F. Imani, K. Salamatian, "Practical Bloom filter based epidemic forwarding and congestion control inDTNs: A comparative analysis", Computer Communications, vol. 48, pp. 98-110, 2014.
[24] D. Li, H. Cui, Y. Hu, Y. Xia, X. Wang, "Scalable data center multicast using multi-class Bloom filter", in Proc. IEEEICNP, Vancouver, BC Canada, 2011.
[25] X. Tian, Y. Cheng, "Loop mitigation in Bloom filter based multicast: A destination-oriented approach", in Proc. IEEEINFOCOM, Orlando, FL, USA, 2012
[26] I. Nikolaevskiy, A. Lukyanenko, T. Polishchuk, V. Polishchukc, A. Gurtov, isBF: "Scalable in-packet Bloom filterbased multicast, Computer Communications", vol. 70, pp. 79-85, 2015
[27] D. Guo, Y. He, Y. Liu, "On the feasibility of gradient-based datacentric routing using Bloom filters", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 180-190, 2014.
[28] H. Chen, H. Jin, L. Chen, Y. Liu, L.M. Ni, "Optimizing Bloom filter settings in peer-to-peer multi-keyword searching",IEEE Transactions on Knowledge and Data Engineering, vol. 24, no. 4, pp. 692-706, 2012.
[29] O. Rottenstreich, I. Keslassy, "The Bloom paradox: When not to use a Bloom filter?" ,in Proc. IEEE INFOCOM, Orlando, Florida, USA, 2012
[30] H. Alexander, I. Khalil, C. Cameron, Z. Tari, A. Zomaya, "Cooperative web caching using dynamic interest-taggedfiltered Bloom filters",IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 11, pp. 2956-2969, 2015.
[31] Y. Li, R. Miao, C. Kim, M. Yu, FlowRadar: A better NetFlow for data centers, in Proc. USENIX NSDI, Santa Clara, CA, USA, 2016.
[32] E.A .Durham, M. Kantarcioglu, Y. Xue, C. Toth, M. Kuzu, B. Malin, "Composite Bloom filters for secure record linkage", IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 12, pp. 2956-2968, 2014
[33] M. Moreira, R. Laufer, P. Velloso, and O. Duarte, "Capacity and robustness tradeoffs in Bloom filters for distributed applications", IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 12, pp. 2219-2230, 2012.
[34] B.M. Maggs, R.K. Sitaraman, "Algorithmic nuggets in content delivery", in Proc. ACM SIGCOMM, London, United Kingdom, 2015.
[35] YounSun Gho, L. Bao, M.T. Goodrich, "LAAC: A Location-Aware Access Control Protocol", Mobiquitous, Third Annual International Conference on Mobile and Ubiquitous Systems, Networking, and Services, pp.1-7, 2006
[36] Denning, D. and Macdoran, P., "Location-based Authentication: Grounding Cyberspace for better Security, Computer Fraud & Security", 1996(2), pp.12-16.
[37] Jansen, W. & Korolev, V., "A Location-Based Mechanism for Mobile Device Security, in WRI World Congress on Computer Science and Information Engineering", Los Angeles, California USA, pp. 99-104, 2009
[38] S. von Watzdorf and F. Michahelles, "Accuracy of positioning data on smartphones", International Workshop on Location and the Web,2010, pp. 1–4.

[39] Denning, D. and Macdoran, P., "Location-based Authentication: Grounding Cyberspace for better Security", Computer Fraud & Security, 1996(2), pp.12-16.
[40] Tweneboah-Koduah, S., Skouby, K. E., & Tadayoni, R. (2017). "Cyber security threats to IoT applications and servicedomains". Wireless Personal Communications, 95(1), 169–185. https://doi. org/10.1007/s11277-017-4434-6
[41] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural lements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010
[42] B. Miller, Everything you need to know about biometric identification. Personal Identification News 1988 Biometric Industry Directory, Warfel & Miller, Inc., Washington DC, January 1988
[43] J. Wayman, A definition of biometrics National Biometric Test Center Collected Works 1997–2000, San Jose State University, 2000.
[44] Sahan, S.; Ekici, A.F.; Bahtiyar, ¸S. "A Multi-Factor Authentication Framework for Secure Access to Blockchain". In Proceedings of the 2019 5th International Conference on Computer and Technology Applications, Istanbul, Turkey, 16–17 April 2019.
[45] Dasgupta, D.; Roy, A.; Nag, A. Multi-Factor Authentication. Adv. User Authentication 2017, 185–233.
[46] Dostalek, L. Multi-Factor Authentication Modeling. In Proceedings of the 2019 9th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 5–7 June 2019; pp. 443–446.
[47] Shah, Y.; Choyi, V.; Subramanian, L. Multi-factor Authentication as a Service. In Proceedings of the 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2015, San Francisco, CA, USA, 30 March–3 April 2015; pp. 144–150
[48] Cardoso, J.A.A.; Ishizu, F.T.; De Lima, J.T.; Pinto, J.D.S. Blockchain Based MFA Solution: The use of hydro raindrop MFA for information security on WordPress websites. Braz. J. Oper. Prod. Manag. 2019, 16, 281–293.
[49] Gupta, R.; Kumari, A.; Tanwar, S. A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles. Trans. Emerg. Telecommun. Technol. 2021, 32, e4009.
[50] Yue, K.; Zhang, Y.; Chen, Y.; Li, Y.; Zhao, L.; Rong, C.; Chen, L. A Survey of Decentralizing Applications via Blockchain: The 5G and Beyond Perspective. IEEE Commun. Surv. Tutor. 2021, 23, 2191–2217.