SECURE AND PRIVACY-ORIENTED ARCHITECTURE WITH OPEN CLOUD COMPUTING FOR INTERNET OF THINGS DEVICES

Lateef Abd Zaid Qudr, Mohammed Abomaali,Ahmed Mohammed Merza
Department of Computer Technology Engineering, Al-Safwa University College, 56001 Karbala, Iraq
latifkhder@alsafwa.edu.iq; abomaali@alsafwa.edu.iq ;Ahmed.merza@alsafwa.edu.iq

Abstract— Smart devices and sensors are key empowering resources regarding the Internet of Things (IoT) paradigm to gather user's sensed information and facts. However, getting involved in collecting user's sensed data for further processing is definitely not very easy. This is because difficulties associated with application heterogeneity, as well as, the security and privacy that now have eliminated the grow of many sensing networks intended for systematic data gathering. Majority of the current researches state that increasing the superiority of IoT services, can be boost through implementing cloud computing approach. For this reason, it is very vital to be aware of the security and privacy aspects among the setting of cloud computing and as well, recognize the ideal properties and as well, the threats that may help and support design secure IoT based architecture. Therefore, this paper is exploring the concept behind the buildup of cloud computing and as well, examines its significance for gathering up user's sensed data and IoT services. Furthermore, we propose an open architecture for gathering user's sensed data in different IoT services that supported by cloud computing approach, where the security and privacy will be maintained amongst the IoT architecture. The proposed architecture enables the deployment of multiple IoT services in real-time, due to the fact that expected in most IoT applications.

Index Terms— Cloud Computing, IoT, Privacy, Security, Sensors, Smart devices.

1 INTRODUCTION

The embedded devices together with the Internet of Things (IoT) devices are actually turning into all-pervasive computing components in our lifetimes. These types of components are being used by various sectors coming from industrial health and wellness, transport across different scenarios of smart home and smart city [1], [2]. The adoption rate involved with these types of computing components is based on their security measure delivered by way of it's applications. Furthermore, the personal privacy is definitely a critical requirement meant for ordinary users and then the IoT enabled application should always be built by way of an effective security and privacy mechanisms [3]. The smart devices are truly connected devices with the empowering engineering, technological innovation of IoT concept, wherever users generate mass sensed data. However, getting involved in collecting this kind of important information intended for analysis is definitely not straight forward. This is for the reason of various difficulties associated with devices heterogeneity, security measures, and level of privacy which usually would need to be considered [4]. Traditional lightweight security solutions are not enough to support earlier mentioned growing sensed data, where the data volume, velocity, and variety is becoming huge. Therefore, this kind of complications usually requires building an reliable security architecture to get organizing and control of this realization of extensive data [5], [6].

Recently, Cloud Computing was considered to aide in eliminating a good deal of challenges in diverse sector areas. With the use of Cloud Computing, it has become quite a bit less difficult to deal with extensive volume of data with reduced the cost [7]. Cloud Computing processing infrastructure in which some application services can be handled in remote data centers. On the other hand, the data produced by using IoT embedded sensors bring about massive amount of unstructured data in real time that call for the promise of Bigdata analysis and give insights for significantly better decision procedures. For this purpose, we propose an open cloud framework for crowd-sensed IoT services, at which the security measures and user privacy are maintained among the framework stages at the network part. Accordingly, this paper considers a scalable secured architecture for IoT devices to distribute processing and securing real time IoT sensors data by using scalable open cloud computing advances.

2. ARCHITECTURAL OVERVIEW OF IOT AND CLOUD COMPUTING

2.1. INTERNET OF THINGS ARCHITECTURE

The IoT is generally described as interconnection of physical things by way of multi-level networking connectivity which usually employed to collect and exchange critical data. The term 'Thing' is referred to a smart computing device or sensor, which is usually connected to the online world by the internet and exchanges the smart device data to various applications. To be able to realize a reliable communicating between the smart devices and the internet, a layered architecture has been distinguished by having several layers including Embedded Layer, Communication Layer, Hardware Layer,

Application Layer, Security Layer, Integration Layer and DB Layer [8], as shown in figure 1. Numerous technological innovations have been implemented in the IoT applications, which are including for example; Smart sensors, actuators, and Smartphones. These types of devices and objects have the ability to communicate with each other by utilizing a unique addressing schemes pertaining to reach a common target. Various standards have been formulated among all layers to actually empower the functions of smart IoT solutions [9], [10], [11].

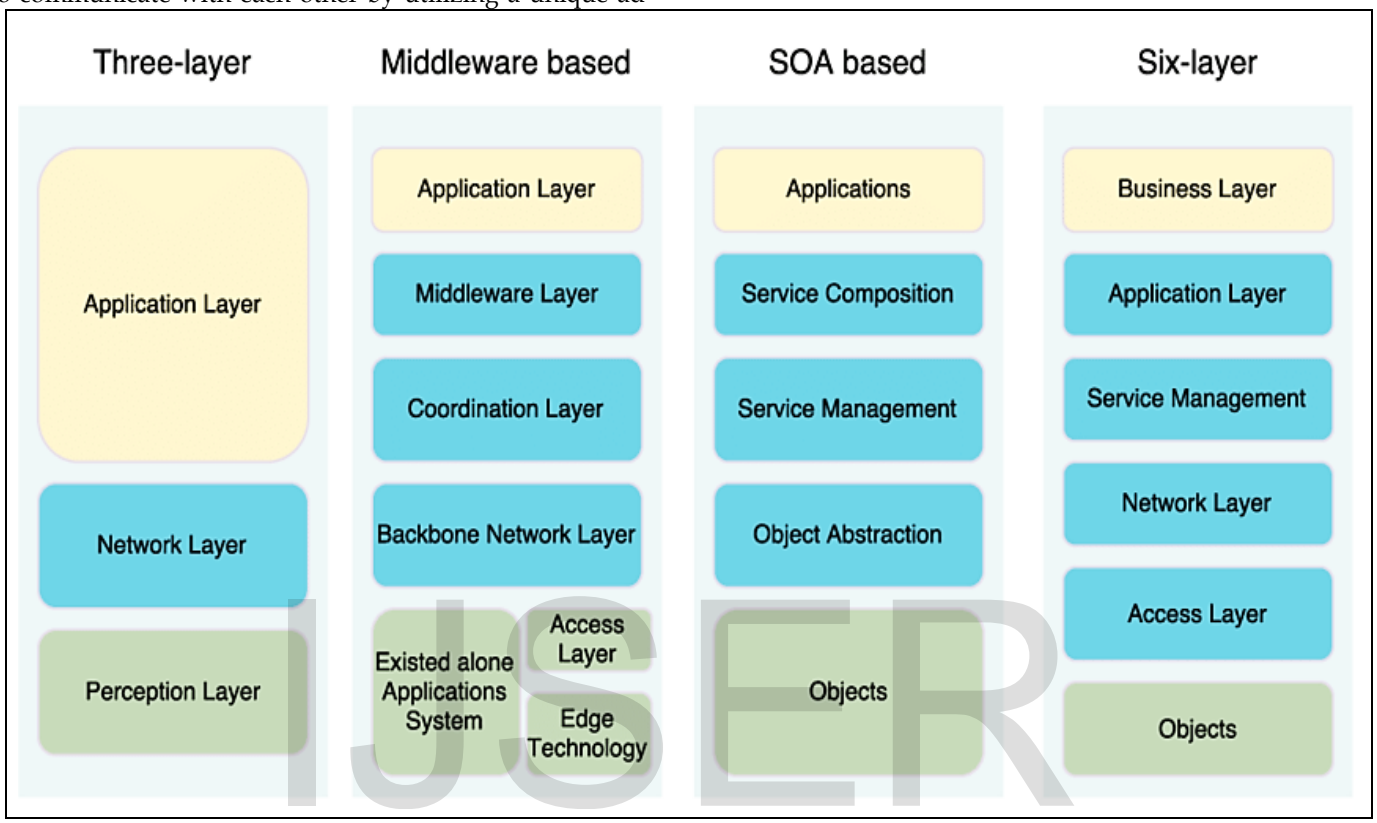

Figure 1: IoT Layered Architecture

1. M2M device domain name: the principal purpose of the domain is usually communicating and getting involved in collecting info all across the physical world. Sensing products designed for brief range interaction are grouped together to attain, accomplish this purpose. The smart products that are involved in this area are likely to be very small, and source restricted. The communication protocols and requirements due to this domain name are built to control communicating through constricted info rates and smaller ranges, with the limited memory capability and low energy usage. As a result of these kind of aspects, M2M device network connections are sometimes introduced because LLN (Low-power and Lossy-Networks).
2. Network domain: the purpose of this domain name is to actually transfer the information obtained within the collection stage to the diverse applications and as a result intended for user rewards. In this domain name, technological innovation h like for example Wi-fi, Ethernet, Digital Subscriber Collection (DSL), and Hybrid Dietary fiber Coaxial (HFC) are actually matched with the TCP/IP protocols to positively interconnect wise objects with all the users using longer ranges. Smart gateways are actually very important to incorporate the LLN protocols associated the collection stage with the ordinary Internet protocols to be utilized in the transmitting stage.
3. Application domain: the application procedure is normally collecting data to acquire useful details about the physical environment. These types of applications might take decisions predicated on these details, maintaining the physical items to respond to the physical environment. This kind of domain also contains a middleware, which is usually accountable for assisting the integration and connection among distinct physical items and multi- system applications. Diverse alliances, regulators, special curiosity organizations, and standard advancement agencies possess proposed a great mind-boggling quantity of conversation solutions intended for IoT, which may create a huge difficult task for end-to-end security in IoT applications [16]. The majority of well-known technological innovation h for IoT consist of Bluetooth Low Energy (BLE), IEEE 802.15.4, Z-Wave, Wireless HART, CoAP, LoRaWAN, RPL, 6LoWPAN, and MQTT.

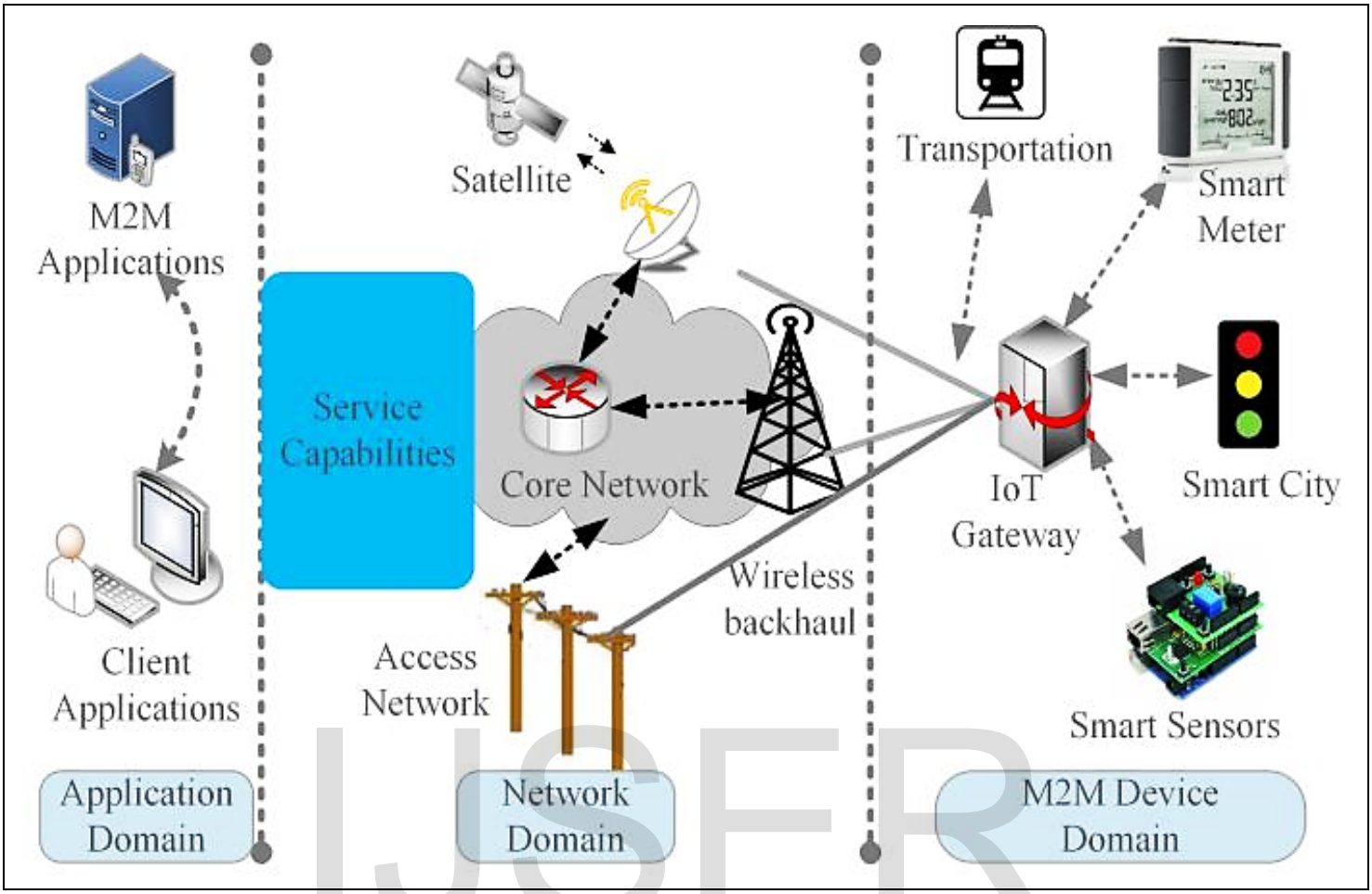

Figure 2: High-level IoT architecture [15]

2.2. CLOUD COMPUTING ARCHITECTURE

The cloud processing architecture is usually a kind of processing model utilized for the delivery of managed support via the internet to deal with real time applications [17]. Furthermore, the cloud computer procedures offer on require access to a pool of configurable resources to share and promote critical information. It has the positive aspects in cellular communications, which usually can be executed towards the transmission devices sector [18]. Furthermore, cloud support services incorporate numerous application models like a private, general public and a hybrid atmosphere intended for being able to access resources kept in the impair. Cloud providers are categorized into 3 classes, which are Infrastructure like a Service (IaaS), Software being a Service (SaaS) and System as a Support (PaaS). Personal clouds are actually utilized for the purpose of storing and posting the information for a great enterprise without sharing the physical assets for others. The sources of the private impair is usually supplied outside the body or perhaps internally. In contrast, Public atmosphere are provided by third-party suppliers and mostly intended for hosting and handling the physical assets and backups. Because public impair services preserve a number of clients, the digesting system is certainly even more international and a lot more than the personal cloud [9]. Figure 3 shows the cloud computing architecture.

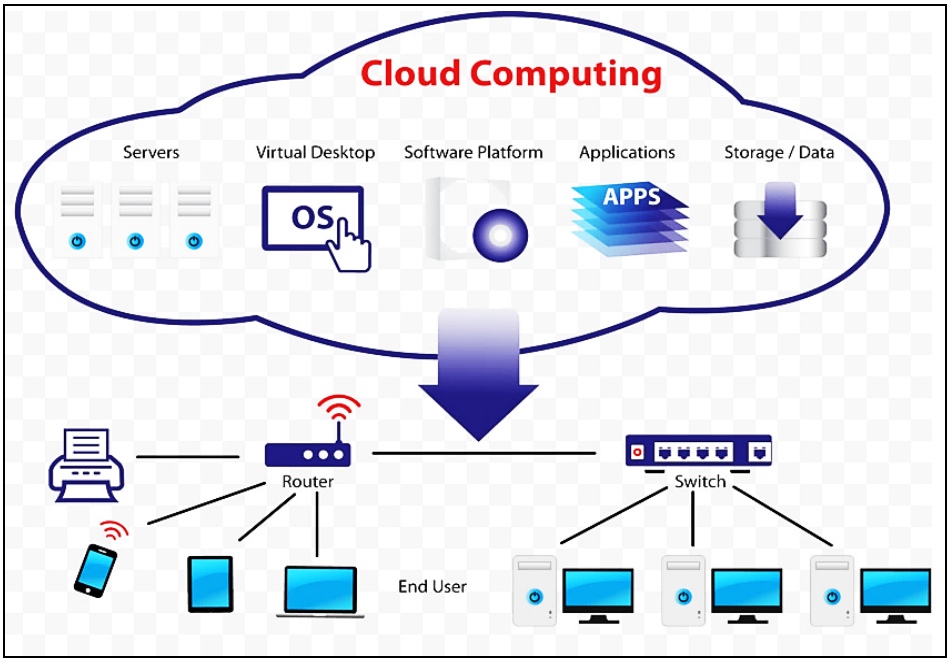

Figure 3: Cloud computing architecture.

3. SECURITY AND PRIVACY ISSUES IN IOT AND CLOUD COMPUTING INTEGRATION

There exists a fast and independent advancement taking into consideration the two domains from the IoT and Cloud Processing. To start with, the practically unrestricted capacities and sources of Impair Computing to be able to compensate the technical constrains, such as for example storage space, processing, and communication, is actually an advantage intended for the IoT technologies [19]. Additionally, the IoT concept expands its settings in order to really handle the real life tasks in a far more allocated and powerful style simply by providing innovative solutions in a big quantity of real world situations, might end up being effective to get the usage of Impair Computing engineering, technological innovation. Oftentimes, Impair can offer the intermediate level between the objects and the applications, trying to hide all of the complexity and functionalities essential to apply the recent [20]. Improving security is usually a substantial element of IoT approaches, because of the complicated process of securing the very sensitive data which is transmitted and analyzed in hostile settings all across IoT domain [14]. The IoT protection may be the region of effort worried about preserving linked products and networking models inside the IoT. The IoT entails the raising prevalence of things regarded, in this situation as items granted with completely unique verifications and the capability to immediately transmit information and facts across the network. A lot of the upsurge in IoT communications derives from smart processing and realizing products utilized in commercial machine-to-machine (M2M) marketing communications [20].

On the other hand, impair security can be an innovating subdomain of information secureness. It identifies a broad group of regulations, technological innovations, and settings deployed to guard data and applications. Impair processing and storage alternatives can offer individuals and businesses with numerous features to procedure and shop their info in third-party data centers [19]. Businesses utilize the Cloud in a number of distinctive support versions because (SaaS, PaaS, and IaaS) and application models (Private, Public, and Hybrid options) [21]–[24]. There are many security considerations affiliated with the cloud computer [24], [25]. These concerns can be falled in line with two wide groups: security problems faced by simply cloud suppliers and reliability problems experienced by their clients who sponsor services or perhaps keep their particular data inside the cloud) [26], however the responsibilities can be shared one of them. The service provider must make sure that their facilities is definitely protected and also their very own potential clients ' data and applications will be secured as the customer need to consider actions to secure their program and make use of solid security passwords and authentication procedures [20], [27].

Even so, the execution of protection and personal privacy features and benefits accelerates an operation concern, since an IoT resolution consists of multiple essentials: embedded gadgets, program interface remote control data digesting and many more. The IoT answer includes each of those open-source and proprietary components, but some of these may not be managed by an individual [3]. Even though the safety and the level of privacy are actually together vital investigate difficulties that have received a lot of interest, they will remain open up problems that need even more efforts. Certainly, creating varied threats coming from hackers continues to be a concern

[28], [29]. Furthermore, another issue provides the suitable authorization protocols and procedures while making sure only certified users get access to private info; this is essential for protecting users' personal privacy, particularly once data honesty should be assured [30].

4. PROPOSED ARCHITECTURE

In this section, we propose an open cloud architecture for gathering user's sensed data for IoT services, where security and privacy are managed within the architecture. This paper discusses a scalable secured architecture for IoT devices to distribute processing and protecting real time sensor data using scalable open cloud computing technologies. The various Things in the IoT context have to be secure, remotely manageable asset and connected to the cloud. Therefore, the typical IoT architecture has key features such as; sensors and actuators, processing and storage, run analytics, and the wireless communications to stream data and receive commands, as shown in figure 4.

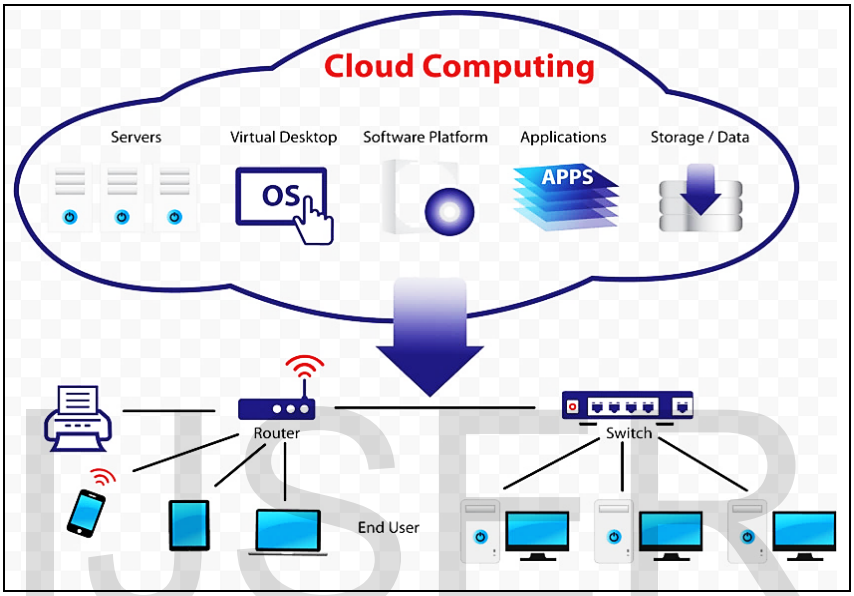

Figure 4: key features of the typical IoT architecture

In general, the proposed architecture consists of three levels of data transformation, beginning by data collection from IoT sensors and client work stations which are connected a cloud by data transfer level for transfer and storage into the database and finally, storage of user's sensed data in the cloud.

The architecture represented in Determine 5 explains one feasible and advantageous application situation of the suggested architecture which includes its subsystems. It displays the haze computing getting controlled in the centre located in the IoT entrance network. All of the collaborating bodies are required to actually ask for individual authentication and special certificates concerning the PKI. The main thought behind working the haze computing is the fact it handles gain access to qualifications, such as protection tokens or perhaps CDS ask for signature personal keys. For that reason, admission to this fabric should be effectively guaranteed through a managed environment. Subsequently, if the IoT gateway is utilized by a limited group of individuals, procedure located in a demilitarized zone (DMZ) by using double-staged firewall will protect users by managed isolation coming from malicious Web-based attacks.

The fog processing presents a support control panel to approved and verified users. In the present execution, that is recognized like a REST internet services guaranteed across a SSL interconnection. The user software program is usually delivered like a stand-alone practical application which includes a Java API to ensure that this can be utilized upon multiple systems and, even more notably, that could be incorporated into client- part products. The fog processing is certainly implemented on well-resourced nodes mainly because it requires digesting intense methods for key sharing. Like a measure intended for reducing possibility of data remanence, the haze computing executes all magic formula sharing calculations in- memory space with no localized caching, which usually on the 1 side plays a part in shorter procedure events, yet however needs larger quantities of RAM. Nevertheless, this kind of a deployment allows thin-clients or perhaps low-resourced cellular clients to obtain secret posting delegated on to powerful products so that these kinds of nodes can easily take part in the secure backup platform also.

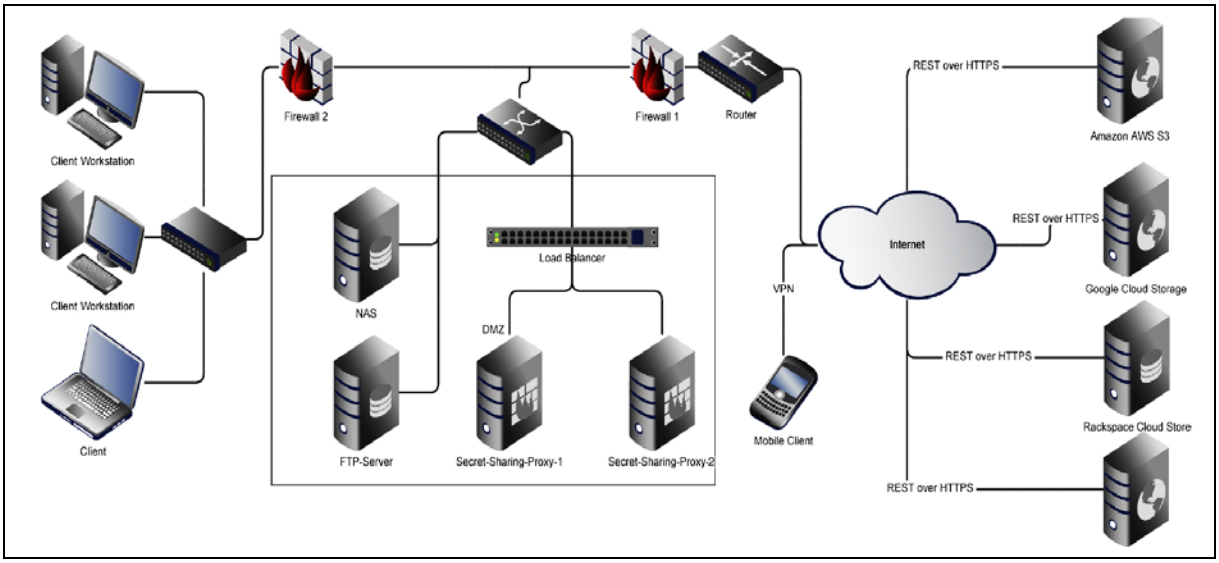

Figure 5: proposed architecture for gathering user's sensed data for IoT services

Operating the IoT gateway upon a central server likewise permits single administration of cloud gain access to credentials and takes its solitary point intended for program repair, security correcting, and observance of user access control. Specifically the configuration guidelines of the key sharing plan should be established globally and, for that reason, will be advisable to end up being designed in one example. Furthermore, features, such as for example ask for queuing, could possibly be added in future in this environment. Likewise, convenient logging and auditing could be accomplished.

Implementing the haze computing prior to the IoT entrance is quite recommended. Benefits have in it the computational extreme processing within the secret posting and restoration, that bigger assets happen to be recommendable. An additional advantage may be the uniform and secure administration of impair credentials and secret writing parameters, and also destruction of central signing and auditing features. The IoT entrance, furthermore, provides a two-staged tampering recognition mechanism to get generated stocks that require fog magic formula key where the share-creating proxy may recognize acting up CDSs. In the event that shares, nevertheless , result from multiple gateway installation using diverse key materials, the system is decreased to an one-staged tampering diagnosis since instance- particular confirmation keys vary as multiple fog nodes are participating. Likewise, if sent and kept in the impair, a trusted consent and authentication schema can be hardly realizable.

5. CONCLUSION

The IoT is now an extremely all-pervasive computing system which in turn necessitates large amounts of data storage space as well as , digesting capabilities. The IoT provides limited features with regards to the processor and storage space, while there likewise can be found resulting issues such as for example security, personal privacy, overall performance, and reliability; Because this kind of incorporation of the Impair in to the IoT is quite helpful with regards to conquering these issues. In this newspaper, we offered the necessity intended for the creation of the open up cloud-based IoT architecture. Conversation also centered on the Cloud-based IoT structures and the diverse challenges facing the effective integration.

REFERENCES

[1] W. D. Fang, W. He, W. Chen, L. H. Shan, and F. Y. Ma, "Research on the application-driven architecture in internet of things," *in Frontiers in Artificial Intelligence and Applications*,vol.293, pp. 458 - 465, 2016.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutorials*, vol. 17, Issue: 4, pp. 2347–2376,2015.

[3] B. C. Chifor, I. Bica, V. V. Patriciu, and F. Pop, "A security authorization scheme for smart home Internet of Things devices," *Futur. Gener. Comput. Syst.*, vol. 86, pp. 740–749, 2018.

[4] L. Luceri et al., "VIVO: A secure, privacy-preserving, and real-time crowd-sensing framework for the Internet of Things," *Pervasive Mob. Comput.*, 2018.

[5] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wirel. Networks,* vol. 20,Issue 8, pp. 2481–2501, 2014.

[6] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," *in Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud,* I-SMAC 2017, Palladam, India,pp. 492-496, February 10-11.

[7] A. M. Helmi, M. S. Farhan, and M. M. Nasr, "A framework for integrating geospatial information systems and hybrid cloud computing," *Comput. Electr. Eng.*, vol. 67, no. March, pp. 145–158, 2018.

[8] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, and W. Liu, "Study and applica-

tion on the architecture and key technologies for IOT," *in 2011 International Conference on Multimedia Technology,* ICMT 2011, Hangzhou, China, July 26-28, 2011,pp. 747 - 751 .

[9] G. Manogaran, R. Varatharajan, D. Lopez, P. M. Kumar, R. Sundarasekar, and C. Thota, "A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system," *Futur. Gener. Comput. Syst.,* vol. 82, pp. 375–387, 2018.

[10] A. A. H. Hassan, W. M. Shah, M. F. Iskandar, M. S. Talib, and A. Abdul-Jabbar Mohammed, "K nearest neighbor joins and mapreduce process enforcement for the cluster of data sets in bigdata," *Journal of Advanced Research in Dynamical and Control Systems,* vol. 10, no. 4 Special Issue. pp. 690-696, 2018.

[11] M. S. Talib, A. Hassan, B. Hussin, Z. S. Talib, Z. S. Rasoul, and M. Sammour, "Data dissemination based clustering techniques for VANETs: A review," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 10, no. 4 Special Issue. pp. 596–604, 2018.

[12] A. Abdul-Jabbar Mohammed, M. A. Burhanuddin, and H. Basiron, "Key enablers of IoT strategies in the context of smart city innovation," *Journal of Advanced Research in Dynamical and Control Systems,* vol. 10, no. 4 Special Issue, pp. 582-589, 2018.

[13] M. S. Talib, A. Hassan, B. Hussin, Z. A. Abas, Z. Saad, and Z. Sabah, "A Novel Stable Clustering Approach based on Gaussian Distribution and Relative Velocity in VANETs," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 4, pp. 216–220, 2018.

[14] M. A. Burhanuddin, A. Abdul-Jabbar Mohammed, R. Ismail, and H. Basiron, "Internet of things architecture: Current challenges and future direction of research," *Int. J. Appl. Eng. Res.,* vol. 12, no. 21, pp 11055-11061, 2017.

[15] A. Hakiri, P. Berthou, A. Gokhale, and S. Abdellatif, "Publish/subscribe-enabled software defined networking for efficient and scalable IoT communications," IEEE Commun. Mag.,vol. 53,issue 9,pp 48-54, 2015.

[16] A. Meddeb, "Internet of Things Standards□: Who Stands Out from the Crowd□?," *IEEE Commun. Mag. – Commun. Stand. Suppl.*, no. July, pp. 40–47, 2016.

[17] A. Souri, N. J. Navimipour, and A. M. Rahmani, "Formal verification approaches and standards in the cloud computing: A comprehensive and systematic review," *Comput. Stand. Interfaces,* vol. 58, no. December 2017, pp. 1–22, 2018.

[18] M. S. Talib, B. Hussin, and A. Hassan, "Converging VANET with vehicular cloud networks to reduce the traffic congestions: A review," *International Journal of Applied Engineering Research*, vol. 12, no. 21. pp. 10646–10654, 2017.

[19] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing - The business perspective," *in 44th Hawaii International Conference on Systems Science* (HICSS-44 2011), Proceedings, Koloa, Kauai, HI, USA, January 4-7, 2011, ,pp. 1-11.

[20] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, "Secure integration of IoT and Cloud Computing," *Futur. Gener. Comput. Syst.*, vol. 78, no. December 2017, pp. 964–975, 2018.

[21] S. Goyal, "Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review," *Int. J. Comput. Netw. Inf. Secur.*,vol. 6, no. 3, pp. 20-29, 2014.

[22] F. Mohammed and O. Ibrahim, "Models of adopting cloud computing in the E-Government context: A review," *J. Teknol.*,vol.73, no. 2, 2015.

[23] P. F. Hsu, S. Ray, and Y. Y. Li-Hsieh, "Examining cloud computing adoption intention, pricing mechanism, and deployment model," *Int. J. Inf. Manage.,* vol. 34, Issue 4, pp. 474-488, 2014.

[24] A. Lin and N. C. Chen, "Cloud computing as an innovation: Percepetion, attitude, and adoption," *Int. J. Inf. Manage.*, vol. 32, Issue 6, pp. 533-540, 2012.

[25] A. Tsohou, H. Lee, and Z. Irani, "Innovative public governance through cloud computing: Information privacy, business models and performance measurement challenges," *Transform. Gov. People, Process Policy*, vol. 8, Issue 2, pp. 251-282, 2014.

[26] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," *Nist Special Publication,* PP 800-145, 2012.

[27] A. A.-H. Hassan, W. M. Shah, M. F. Iskandar, and A. Abdul-Jabbar Mohammed, "Clustering methods for cluster-based routing protocols in wireless sensor networks: Comparative study," *Int. J. Appl. Eng. Res.,* vol. 12, no. 21, pp. 11350-11360, 2017.

[28] M. A. Burhanuddin, A. Abdul-Jabbar Mohammed, R. Ismail, M. E. Hameed, A. N. Kareem, and H. Basiron, "A review on security challenges and features in wireless sensor networks: IoT perspective," *J. Telecommun. Electron. Comput. Eng.*, vol. 10, no. 1–7, 2018.

[29] M. Sammour et al., "DNS Tunneling: a Review on Features," *International Journal of Engineering & Technology,* vol. 7, no. 3.20 , Special Issue 20, pp. 1-5,2018.

.

[30] H. F. Atlam, A. Alenezi, A. Alharthi, R. J. Walters, and G. B. Wills, "Integration of Cloud Computing with Internet of Things: Challenges and Open Issues," 2017 *IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data*, pp. 670–675, 2017.