Addressing the Concerns around privacy and security in IoT Network

Dr.K VIJAYA BHASKAR[1] B RAJEEV SINGH[2] P.RAMYA LAVANYA[3] DR MAJETI PAVAN KUMAR[4]
[1]ASSOC.PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[2] ASST. PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[3]ASST. PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[4]PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[1,2,3,4] SRI MITTAPALLI COLLEGE OF ENGINEERING

Abstract- Things like vehicles, environmental sensors, and household appliances may all become part of the Internet of Things (IoT) when they are either directly linked to or accessible over the web. Concerns around privacy and security, together with communication and administrative constraints, are inherent in establishing an IoT network. By transferring all complicated operations to the cloud and making them available to users, cloud computing is seen as a viable option for controlling IoT devices. Internet of Things (IoT) systems may be made more reliable and scalable by using cloud computing. The introduction of the cloud paradigm, however, is no easy feat. The idea of edge computing arose from a desire to circumvent the cloud's latency and security issues; nevertheless, this approach is not without its own storage, compute, and mobility limits. In this article, we look at the cloud-edge system's potential for administering an IoT system. In order to overcome the constraints of the Internet of Things, it explains cloud and fog computing. To further evaluate the benefits and drawbacks of these technologies, important measures have been defined. In conclusion, this study presents a methodology that may address the aforementioned constraints, optimise service distribution across cloud and edge servers, and increase overall performance.

Keywords-- IoT, IoE, Cloud Computing, Fog Computing, Edge Computing

I. INTRODUCTION

A relatively new idea, the "Internet of things" (IoT) enables any and all objects with a webcam to exchange data with one another and the outside world. On the other hand, the IT industry has encountered novel and exciting problems as a result of this idea. Issues with information trust and device ownership, together with a lack of worldwide standards for indexing and identifying IoT objects, are among the reasons cited by [1] as preventing the realisation of value from IoT capabilities. To include more than only internet-connected gadgets, the phrase "Internet of everything" (IoE) has been expanded from "Internet of Things" (IoT). People, data, processes, and objects make up the Internet of Everything (IoE), as stated in [2]. By enhancing commercial and manufacturing procedures, IoE also improves people's daily life.When it comes to the Internet of Things (IoT), one possible advantage of cloud computing (CC) technology is that more devices will likely join the network. Accordingly, the cloud will facilitate the efficient expansion of the IoT as it is a great way to increase or decrease the consumption of resources like storage and bandwidth. Data transmission and cloud processing, however, introduce new kinds of difficulties to IoT systems.

Computing power may be relocated to the edge of the network or closer to IoT devices, as shown in [3]. An improvement that addresses the shortcomings of cloud computing might be edge computing (EC). Nevertheless, EC remains in its infancy and encounters certain obstacles depending on the EC devices used. When considering efficiency and cost, this decision is crucial. While some constraints may arise from relying on cloud services, EC is not meant to replace them. To determine which tasks should run on the edge and which in the cloud, a transparent process must be established, bearing in mind that not all tasks can be done in EC.Additionally, it might be difficult to balance loads and distribute duties uniformly across all EC devices when more than one is deployed. In addition, problems with the network, including traffic jams or denial of service, may affect the edge. Therefore, to prevent the aforementioned problems, an effective procedure must be designed. Another important issue is mobility management, as devices' movement might affect their connections to the edge in bad ways in certain situations. Consequently, EC needs a plan B for situations involving considerable mobility. Lastly, and most crucially, EC may encounter privacy and security concerns because to data being sent to the network's periphery, where assaults are very probable. Consequently, top-notch security need a solid structure. The purpose of this article is to examine the potential for implementing an IoT system that integrates cloud and edge computing solutions, as well as to survey the current state of research on IoT systems that have been produced. To have a better grasp of the benefits and drawbacks of these technologies, we provide several motivating situations. Additionally, it compares cloud and fog computing using a number of criteria that reveal their respective strengths and weaknesses. To increase overall performance, it concludes by offering a framework that considers the advantages and limits of each.

A. Delivering healthcare in emergencies

Any anyone, at any time, anywhere, may be the victim of an emergency. In times of medical crisis, getting individuals the treatment they need quickly may lessen danger and perhaps save lives. Having this option in place might be very crucial in times of emergency involving children or elderly individuals living alone. For the second scenario, it's possible to install a network of Internet of Things (IoT) devices in the homes of the elderly in order to monitor their vitals and detect any problems. Having the inferred instances instantly sent to their physicians or sent to the closest medical centre as a warning would be fascinating. A safe location can be found for all health readings. Conversely, physicians may examine patient records remotely, without ever having to set foot in their offices. If a more extensive examination is necessary, they could simply request a visit from the closest medical facility. In order to better understand their patients' health and spot any potential problems, physicians might analyse the gathered data to find out more specific information.

B. Smart Homes

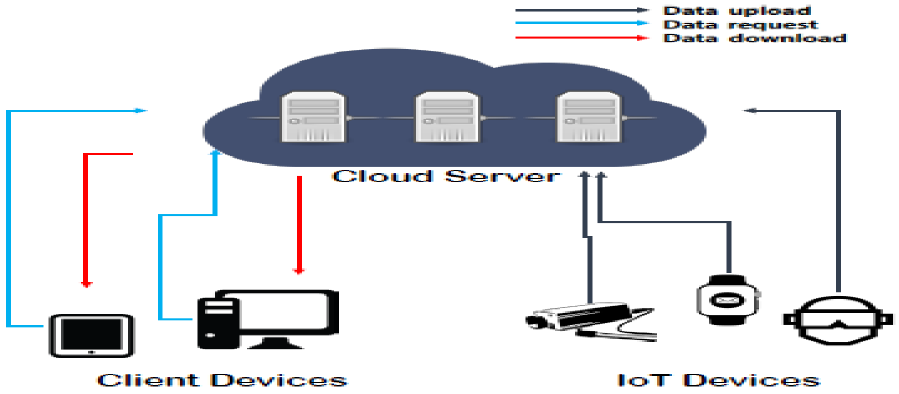
One typical use of Internet of Things applications is making a house smarter by installing gadgets in various rooms (e.g., the kitchen and the living room) and then linking them all together to provide the homeowner with services. As an example, the owner may make afternoon tea or switch on the air conditioner on the way home. Many commonplace items now on the market can be controlled from a distance via a network, allowing for remote management over the internet. From a communication standpoint, however, there are a number of challenges, such as managing smart home components, sending requests to these things, and collecting data from all of the linked objects. Because these items often run on batteries and can't manage too many operations, another obstacle might be connected to their nature; hence, a lightweight protocol has to be established. Developing this protocol should take into account the need to minimise access to these objects and the execution of operations. Lastly, there are ethical and privacy concerns that might arise from accessing smart home IoT items, particularly when doing so via an internet-connected system. In order to prevent assaults that may compromise the system's objects or the data they generate, a robust security mechanism must be in place to guarantee that the acquired data is associated with the homeowner. Home automation presents a number of real-world obstacles, as highlighted in paper [4]. These include, but are not limited to, application and device heterogeneity, service non-interoperability, heavy reliance on the cloud, privacy and security concerns, and the need to fulfil Internet of Things (IoT) standards. The authors devised the idea of edge computing to address these constraints. Application memory and CPU load were both improved by using the suggested prototype, according to the trial findings.

C. Supporting Alhajj event

One of the world's most massive gatherings is the Alhajj. For the able-bodied, the Islamic pilgrimage of Alhajj takes place every year in the Saudi Arabian city of Makkah, and over two million people from all over the globe go there to do it. An intriguing aspect of this event is the constrained location and the large number of participants preparing to execute identical tasks simultaneously. It also entices scholars to propose solutions to problems that may arise during Alhajj or ways to enhance the pilgrim's experience to make it more pleasant and easier for them. Internet of Things (IoT) devices placed strategically throughout the city might provide live coverage of the event. The management centre might use the gadgets to gather data and analyse it for decision-making purposes, which is a potential advantage. Smart tents, modelled after smart houses, are another possibility; with these, pilgrims may use their phones to adjust the temperature, turn on and off lights, and, most crucially, locate their tents in the event that they go misplaced. For instance, the command centre may keep an eye on the smart tents to see any signs of fire before they start or spread. If no one is in the tent, the sensors might automatically turn off the electricity or send a signal to the closest hospital or group of volunteers if they sense an emergency.

D. Summary

The scenarios presented above share common characteristics that lead to certain requirements to be considered such as real-time interaction, high performance, vigorous security mechanisms, and efficient energy management, etc. Therefore, the integration of technologies such as the cloud and edge computing can be an effective solution to meet these requirements. However, the integration of these technologies to manage the IoT system can face some issues that need to be tackled. Hence, this research will investigate the ability of integrating the cloud and edge computing to IoT systems for the purpose of meeting aforementioned requirements and dealing with any arisen issues.



II.RELATED WORKS

Kevin Ashton's [5] consideration of radio frequency identification (RFID) tags on commonly used objects originated the idea of the Internet of Things. It wasn't until the late 90s that this particular network topology was identified; subsequent years saw tremendous development and expansion in all directions in terms of IoT ideas. This goes well beyond just tagging items with radio frequency identification; it opens up a vast array of possibilities for human-object interaction in many settings and sectors, including healthcare[6,7], smart homes[8], autonomous cars, and many more. In order to control and personalise the environment in which these devices are installed, end users may take use of the services offered by the Internet of Things (IoT), which is a mix of the Internet as an infrastructure for communication and the IoT itself [9]. Among the most comprehensive and often used definitions of the Internet of Things (IoT) in the literature, the one in [10] is characterised by its ability to communicate over the existing After decomposing the Internet of Things into its three primary components, the author of [10] arrived at this definition. The five-layer structure described in [11] is an advanced design for the Internet of Things. These levels are the following: access gateway, middleware, internet, edge technology, and application.Using the Internet as a foundation for Internet of Things devices is only one of several obstacles to implementing the IoT. An estimated seven billion people will be online by the year 2020, continuing the meteoric rise in internet use that has already begun [12]. Problems will also arise as a result of the interdependencies between devices that are necessary for the execution of Internet of Things (IoT) applications [13]. If many devices or nodes are capable of handling the same set of services or job, then there may be a problem with deciding which one to use to complete the work [14].

A. Merging Cloud Computing with IoT

Cloud computing, sometimes known as the mobile cloud [15], may be a lifesaver when faced with these and other problems since it provides a safe haven to run programs or store and transmit data. Integrating the cloud with the internet of things (IoT) would greatly benefit the internet's future, according to the authors of [16]. Long reaction times and privacy and security concerns are just a few of the obstacles that will make implementing the mobile cloud paradigm into an Internet of Things application a difficult and time-consuming process [17, 18, 19]. To facilitate this connection, cloud and IoT apps should have some distinctive features [20]. In order to demonstrate how new paradigms might manage IoT applications while accounting for their characteristics (such as heterogeneity), the article cites a few case studies. Some examples of these paradigms are SenaaS, DBaaS, EaaS, and VSaaS, which stands for sensing, database, and video surveillance, respectively. Based on its application needs, the authors advised choosing the most appropriate cloud provider. The challenge comes from the fact that these needs are likely to vary often and are not easy to collect. This might lead to problems like relocation and the possibility of moving to a different service provider. The three primary building blocks of an Internet of Things (IoT) system are end-users, middleware, and hardware, according to [21]. The sensors allow the cloud to function as middleware, providing computing and storage functions, rather than just being a physical component. The third part is the end-user or users, who are the ones who will be interested in the data that the middleware processes once it is acquired from the hardware.

B. Fog Computing

Just as in [22], it's obvious that placing servers near these IoT items and in front of the cloud would be far more efficient than transferring every single piece of data acquired from them to the cloud. Fog computing, cloudlets, and mobile edge computing are all variations on this architecture. The answer is not to do tasks on IoT items themselves but rather to offload them to another location, like the cloud. In actuality, the edge layer may be implemented in one of three ways: cloudlets, mobile edge computing, or fog computing. Based on their respective methods of implementation, the authors of [23] contrasted these three words. When servers are placed on cellular network base stations, it is called mobile edge computing. On the other hand, cloudlets refer to servers that are closer to users and operate as a smaller-scale cloud capability. Moving equipment like wireless routers and machine-to-machine (M2M) gateways to the edge layer enables fog computing, where fog nodes store and process data before sending it to the cloud. Fog computing allows a wide variety of access methods, including mobile networks, Wi-Fi, and Bluetooth, in contrast to cloudlets and mobile edges, which only accept Wi-Fi and mobile networks, respectively. Cloudlets and mobile edges can only support a single hop in proximity, whereas fog computing can support several hops.When it came to assisting Internet of Everything (IoE) applications, the writers of [24] contrasted cloud and fog computing. The formal cloud has its limits, but fog computing offers a solution by addressing these issues with characteristics like heterogeneity and interoperability, which allow it to manage a diverse range of devices. By placing fog nodes close to requesters, latency may be reduced and location awareness improved. Wireless connections are also essential to fog computing, which uses them to improve mobility and decrease traffic at the network's core. Furthermore, fog computing may provide a different, less expensive location to handle the acquired data. The ability to handle requests locally rather than sending them all to the cloud or even just filtering them is another key aspect of fog computing. This leads to better network utilisation and less bandwidth wasted.The speed with which the system reacts to requests or events is an important consideration when operating IoT applications. Problems with task execution or communication might cause delays. To prevent running activities on objects with restricted resources, tasks may be relocated outside of IoT devices to address the first kind of delay. Delaying computation on central servers and improving real-time interaction are both possible outcomes of moving computation to edge servers [25]. Instead than relying only on edge computing to handle delays and real-time interactions, cloud and edge computing might work together. Potentially faster reaction times and less latency relative to cloud computing may be brought about via edge or fog computing. If your service or activity requires real-time interactions, fog computing is the way to go since the distance is shorter. The steps of task submission, deployment, execution, and result return time may be used to estimate the reaction time of any Internet of Things (IoT) job or event [26].Cloud computing, which provides computing power and storage on demand, was suggested as the ideal option for processing in IoT networks. Nevertheless, many application needs aren't satisfied by the cloud's rising reliability as a centralised solution or by its considerable distance from the user's location [27]. Applications' functionality and performance might also be impacted by an unforeseen surge in traffic. As a result, fog computing might be a way to fix these problems. If situated correctly, being close to users may improve performance and provide other benefits like increased network resilience. Since less data is sent from local devices to the cloud via edge computing, traffic bottlenecks are less likely to develop, which in turn reduces network strain [25].Multiple factors, including the amount of concurrent sessions, connections, and users, must be taken into account in order to get improved network resilience and reduced traffic in the IoT. A measure of both the number of requests made and the average time it takes to handle each request. To effectively handle the traffic load, it is necessary to establish a predefined threshold and scale the resources accordingly [23]. Overall, by limiting data interchange with the cloud, fog computing situated on the network's periphery and close to IoT devices may significantly improve network resiliency and decrease traffic. Shorter connections allow Internet of Things devices to interact with fog nodes, also known as edge servers. Internet of Things (IoT) devices may take use of the vast amounts of storage space offered by the cloud data centre, which is a major advantage of using cloud computing as a solution. But, delays are inevitable with such a framework, therefore it cannot satisfy the needs of real-time applications. Therefore, edge computing may gather data close to its origins, resulting in reduced latency and enhanced performance. But as the number of gadgets connected to the internet is growing, this brings up yet another problem. Edge servers will either need to upgrade their storage capacity or transfer data to a cloud service in order to handle this surge. In general, IoT systems might benefit from implementing an edge computing solution; nevertheless, it is important to take into account the edge's restricted storage capabilities. Furthermore, a plethora of functional requirements are established for the management of storage space in IoT systems.When working with unstructured files, a file processor is useful for storing and managing them in a file repository. When dealing with structured data, the database module is useful for merging and unifying various databases. Improved and streamlined data access necessitates a mapping from objects and entities to mapping. In order to establish automated services, a service module must first generate configurable data, which must then be mapped to the database and file repository appropriately. Lastly, considering needs and preferences during setup, the resource configuration module is used for both static and dynamic data management [19]. The security of data and resources is of the utmost importance in cloud computing. Data security, privacy, and authentication would all take a hit if we connected to the cloud. The ability to easily authenticate and authorise any device connected to the network is made possible by fog nodes, which are location aware devices. Fog nodes may do intrusion detection locally instead of in the cloud. This aids in the detection of localised, harmful assaults before they impact the whole cloud [23]. There are primarily three levels of fog computing. The physical and datalink layers make up the sensing layer, the topmost layer. Attacks such as denial of service, device tampering, and spoofing are among the many security concerns that this layer faces. Data encryption/decryption methods, hash verification, and generational safeguards are all part of the authorisation and cryptography processes put in place to deal with these kinds of risks. Managing the channel of transmission is the responsibility of the middleware layer, the second level. Here you may find the transport and network layers together. Eavesdropping, acknowledge flooding, and selective forwarding—in which a rogue node drops or blocks packets—are common attacks that may happen at this layer. Transport layer security and Internet Protocol security protocols are among the tools at one's disposal to counteract such dangers. Firewalls and private keys might also be very useful in this regard. The needs of individual applications determine the specifics of the fog server, the third layer of fog computing. This makes it very difficult to control the risks to its security. Common security vulnerabilities at this layer include node identification and phishing attempts.In a centralised design, Internet of Things (IoT) devices communicate with a server in the cloud, which processes and stores data. Cloud computing uses a lot of power when transmitting massive volumes of data. Contrarily, fog nodes reduce network overhead, latency, and complexity by acting as an intermediary layer between linked devices and the cloud. A distributed architecture's goal is to drastically cut power consumption, which means processing data near to the network's edge [15]. With features like location awareness, low latency, and mobility support, fog computing is superior than cloud computing. Communications, data storage, and control will all take place close to the user. As a whole, this will help reduce power use in the cloud compared to a centralised model [16].

PROPOSED METHOD

While much of the data generated by IoT devices may be saved and processed locally, allowing for faster response times and less latency, a portion of this data, especially that which is particularly important for certain applications, can be stored and processed in the cloud [20]. The overarching idea is to store and handle data locally wherever feasible. In contrast to the proactive nature of fog servers, cloud servers are better suited to analysing data, choices, and log files over the long term. Load balancing of processing for IoT systems is an advantage of the proposed fog-cloud architecture. Some services would operate in the fog, while others would be in the cloud.

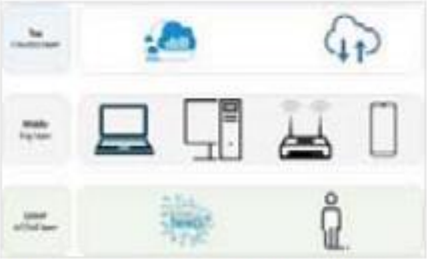


Fig. 1. Proposed framework.

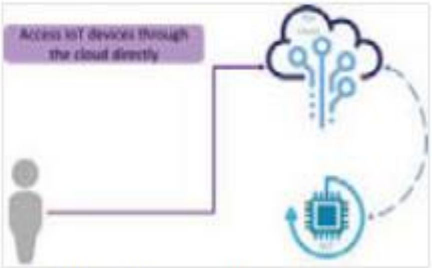
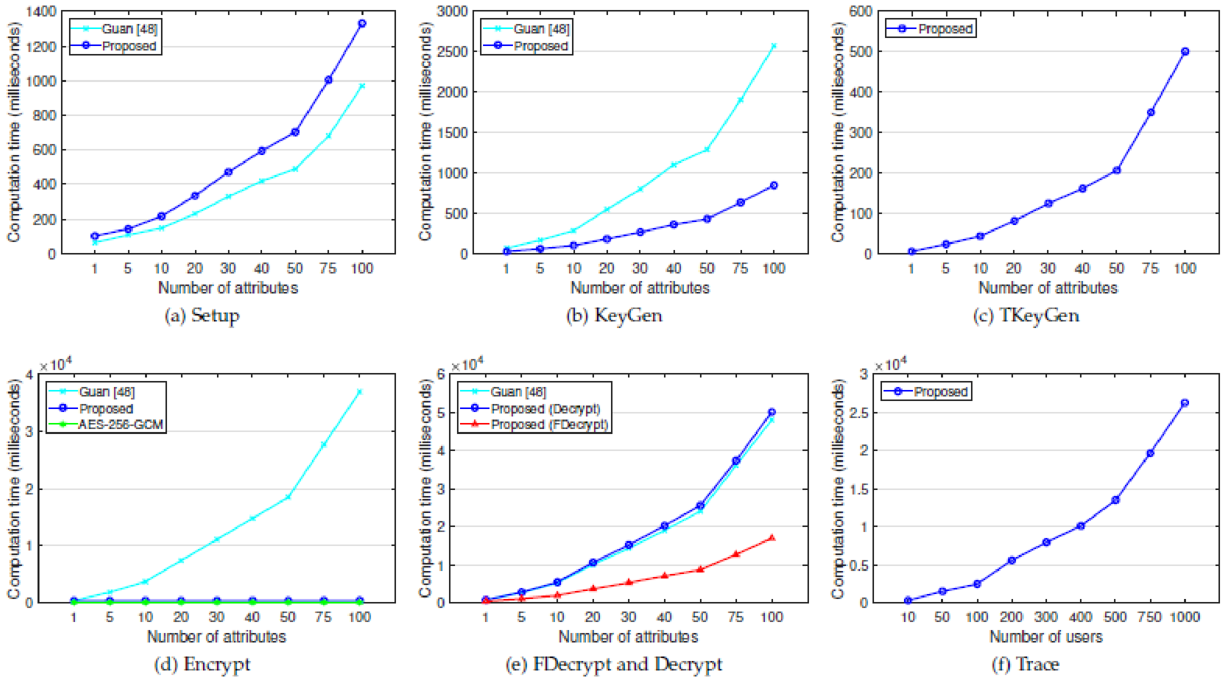


Fig. 2. Access IoT devices through the cloud directly

Although it is possible to store and process most of the data produced by IoT devices locally, which results in lower latency and quicker reaction times, some of this data, especially that which is crucial for certain applications, may be stored and processed in the cloud [20]. Data should be stored and processed locally wherever possible; this is the main concept. Cloud servers are more suited to long-term analysis of data, decisions, and log files, in contrast to fog servers' proactive nature. One benefit of the proposed fog-cloud architecture is that it can balance processing loads for IoT devices. There would be services that run in the cloud and others that run in the fog.

III. RESULTS AND DISCUSSION

The suggested method was put into action by use of jPBC [15]. Desktop computers with Intel Core i5-3570 CPUs running at 3.40 GHz and 4GB of RAM were used to execute the key authority algorithms, KeyGen and Setup. The following cloud algorithms were executed on Amazon EC2 virtual machines: TKeyGen, PDecrypt, and Trace. The hardware configuration included a 2.50 GHz Intel Zeon platinum 8175 processor, 24 cores, two virtual CPUs, and 8GB of RAM. The algorithm for Internet of Things devices (Encrypt) was executed on a Raspberry Pi 3 Model B+ equipped with 1 GB of LPDDR2 SDRAM and a 1.4 GHz Broadcom BCM2837B0. Finally, a SAMSUNG laptop with four gigabytes of RAM and an Intel Core i7-3517U processor running at 1.90 GHz was used to execute the mobile device algorithm (FDecrypt). In addition, we made use of jRAPL [16], which is a collection of low-level APIs for power-and energy-usage profiling in Java applications. In order to record the charging state of an Internet of Things device running the Encrypt algorithm, we used a power meter tester [7]. Furthermore, we evaluate the suggested method in comparison to [18], which offers the fundamental capabilities of CP-ABE in IoT networks. Each algorithm's computing cost under different situations is shown in Fig. 3. Systemwide setup time is proportional to the amount of characteristics, as shown in Fig. 3(a). There are three kinds of keys that are associated with each characteristic in the proposed scheme: positive, negative, and wild-card. This process takes more time than [18]. Since the Setup method is executed only once during startup, it is considered a one-time cost. The correlation between the total time required to generate keys and the quantity of characteristics is seen in Figures 3(b) and 3(c).



(a) Setup (b) KeyGen (c) TKeyGen

(d) Encrypt (e) FDecrypt and Decrypt (f) Trace

Fig. 3: Computation cost of each algorithm

Figure 4 shows that when the number of characteristics and users rises, the time it takes for outsourced cloud decryption also increases. From what we can see in our scenario, the cloud handles around 66% of the total decryptions, with 66% of those computations being acquired computationally. When it comes to supporting access control over numerous users, symmetric encryption could be a better option than ABE method. In symmetric encryption, this is accomplished by assigning a unique secret key to each user and then using those keys to create separate ciphertexts. As can be seen in Figure 5(b), this method will not be able to handle a growth in the number of users. Figure 1 depicts the computational load on the IoT device for varying user access densities. Assuming KEM makes use of 50 characteristics, we encrypted 128-byte worth of IoT data using AES256-GCM in the experiment.

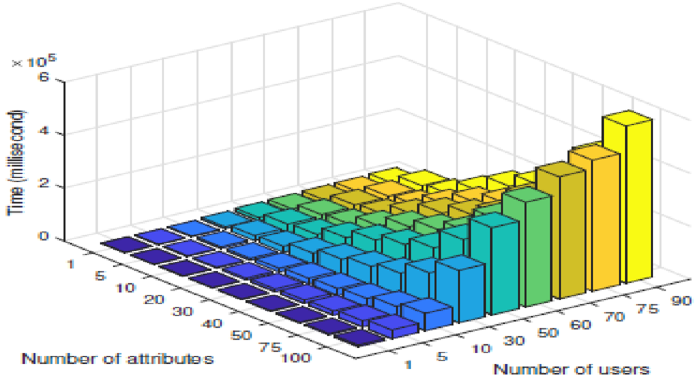
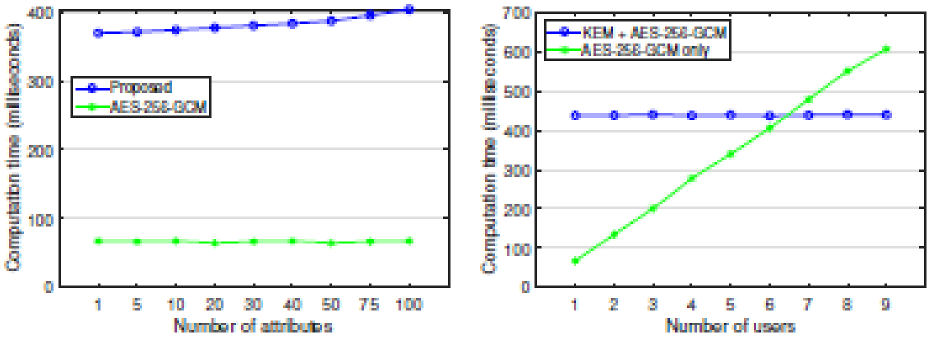


Fig. 4: Computation cost of PDecrypt on cloud server



(a) (b)

Fig. 5: Computation cost of symmetric encryption and proposed KEM

VI. FUTURE SCOPE AND CONCLUSION

The Internet of Things (IoT) has recently become popular as a result of its useful applications in many domains, particularly those related to daily living. The Internet of Things (IoT) has a lot of problems and limits, but cloud computing's wonderful advantages, such its massive storage capacity and processing capabilities, make it a good match for IoT systems, according to several academics. Cloud computing, on the other hand, introduces additional difficulties such security risks and significant latency.

.

REFERENCES

[1] M. R. Belgaum, S. Soomro, Z. Alansari, S. Musa, M. Alam and M. M. Su'ud, "Challenges: Bridge between cloud and IoT," 2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS), Salmabad, 2017, pp. 1-5.

[2] M. H. Miraz, M. Ali, P. S. Excell and R. Picking, "A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," 2015 Internet Technologies and Applications (ITA), Wrexham, 2015, pp. 219-224.

[3] H. El-Sayed et al., "Edge of Things: The Big Picture on the Integration of Edge, IoT and the Cloud in a Distributed Computing Environment," in IEEE Access, vol. 6, pp. 1706-1717, 2018.

[4] T. Chakraborty and S. K. Datta, "Home automation using edge computing and Internet of Things," 2017 IEEE International Symposium on Consumer Electronics (ISCE), Kuala Lumpur, 2017, pp. 47-49.

[5] T. Teixeira, S. Hachem, V. Issarny and N. Georgantas, "Serviceoriented middleware for the Internet of Things: a perspective," in Proceedings of the 4th European Conference on Towards a Service- Based Internet, Poznan, Poland, Springer-Verlag, 2011, pp. 220- 229.

[6] S. M. Shyam and G. V. Prasad, "Framework for IoT applications in the cloud, is it needed? A study," 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, 2017, pp. 1046-1048.

[7] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, _Internet of Things (IoT): a vision, architectural elements, and future directions,_ Elsevier: Future Generation Computer Systems 29, 2013, pp. 1645- 1660.

[8] M. Gusev and S. Dustdar, "Going Back to the Roots.The Evolution of Edge Computing, An IoT Perspective," in IEEE Internet Computing, vol. 22, no. 2, pp. 5-15, Mar./Apr. 2018.

[9] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing," 2017 Global Internet of Things Summit (GIoTS), Geneva, 2017, pp. 1-6.

[10] K. Velasquez, D. Abreu, M. Assis, C. Senna, D. Aranha, L. Bittencourt, and E. Madeira, _ Fog orchestration for the Internet of Everything: state-of-the-art and research challenges!_ Journal of Internet Services and Applications, vol. 9, no. 1, pp. 14, 2018.

[11] S. Singh, "Optimize cloud computations using edge computing," 2017 International Conference on Big Data, IoT and Data Science (BID), Pune, 2017, pp. 49-53.

[12] A. Modarresi and J. P. G. Sterbenz, "Toward resilient networks with fog computing," 2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM), Alghero, 2017, pp. 1-7.

[13] F. Metzger, T. Hoßfeld, A. Bauer, S. Kounev and P. E. Heegaard, "Modeling of Aggregated IoT Traffic and Its Application to an IoT Cloud," in Proceedings of the IEEE, vol. 107, no. 4, pp. 679-694, April 2019.

[14] L. Jiang, L. D. Xu, H. Cai, Z. Jiang, F. Bu and B. Xu, "An IoTOriented Data Storage Framework in Cloud Computing Platform," in IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 1443-1451, May 2014.

[15] D. Zhe, W. Qinghong, S. Naizheng and Z. Yuhan, "Study on Data Security Policy Based on Cloud Storage," 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), Beijing, 2017, pp. 145-149.

[16] S. H. L. Kanickam, L. Jayasimman and A. N. Jebaseeli, "A Survey on Layer Wise Issues and Challenges in Cloud Security," 2017 World Congress on Computing and Communication Technologies (WCCCT), Tiruchirappalli, 2017, pp. 168-171.

[17] C. Esposito, A. Castiglione, F. Pop and K. R. Choo, "Challenges of Connecting Edge and Cloud Computing: A Security and Forensic Perspective," in IEEE Cloud Computing, vol. 4, no. 2, pp. 13-17, March-April 2017.

[18] B. Z. Abbasi and M. A. Shah, "Fog computing: Security issues, solutions and robust practices," 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, 2017, pp. 1- 6.

[19] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan and R. Ranjan, "Fog Computing Security Challenges and Future Directions [Energy and Security]," in IEEE Consumer Electronics Magazine, vol. 8, no. 3, pp. 92-96, May 2019.

[20] R. Oma, S. Nakamura, T. Enokido and M. Takizawa, "An Energy- Efficient Model of Fog and Device Nodes in IoT," 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), Krakow, 2018, pp. 301-306.

[21] K. Shahryari and A. Anvari-Moghaddam, "Demand Side Management Using the Internet of Energy Based on Fog and Cloud Computing," 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom)

and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, 2017, pp. 931-936.

[22] J. Xu, K. Ota, and M. Dong, "Saving Energy on the Edge: In- Memory Caching for Multi-Tier Heterogeneous Networks," in IEEE Communications Magazine, vol. 56, no. 5, pp. 102-107, May 2018.

[23] C. Tseng and F. J. Lin, "Extending scalability of IoT/M2M platforms with Fog computing," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 825-830.

[24] A. El-Mougy, I. Al-Shiab and M. Ibnkahla, "Scalable Personalized IoT Networks," in Proceedings of the IEEE, vol. 107, no. 4, pp. 695- 710, April 2019.

[25]Muppavarapu, Rajasekhar, and Mastan Rao Kale. "An Effective Live Video Streaming System."

[26]LAKSHMI, MANNAM SWARNA, and KALE MASTHAN RAO. "Dynamic Audit Services for Cloud Outsourced Storages with Key Updates." (2017).