Management Of Privacy And Security Challenges In Iot To Restrict Unauthorized Access In To Cloud Storage

Bukkacharla Kishore Kumar[1] , Idamakanti Akhila[2]

[1] Asst. Professor, Department of Computer Science and engineering , QIS College of Engineering & Technology

[2] M.Tech,Scholar, Department of Computer Science and engineering , QIS College of Engineering & Technology

Abstract:

To summarise: the Internet of Things (IoT) refers to the network of interconnected devices, sensors, and appliances that can all be accessed through the Internet (IoT). The implementation of an Internet of Things (IoT) network poses security and privacy issues, as well as communication and management constraints. All complicated operations are moved to the cloud and made available to users through cloud technology, which is regarded to be an efficient option for administering IoT devices. IoT systems' dependability and scalability may be improved by using cloud technologies. Introduction of the cloud paradigm, on the other hand, is a difficult job. In order to avoid some of the drawbacks of the cloud, such as latency and security issues, edge computing was suggested, although it has its own storage, processing, and mobility restrictions. This article explores the idea of using a cloud-edge system to manage an IoT system. In order to overcome the constraints of the Internet of Things, it adds cloud and fog computing. Critical metrics are also established in order to evaluate the benefits and drawbacks of these new technology. A framework to deal with these issues, balance services across cloud and edge servers, and improve overall performance is proposed in this article.

I. INTRODUCTION

A contemporary idea known as the Internet of things (IoT) enables anything that communicates to send and receive data via the Internet. This idea, on the other hand, has created new and distinct problems in the area of information technology. IoT features can't be used to their full potential because of several issues, such as the absence of worldwide standards for indexing and assigning IDs to IoT objects, as well as a vague approach to information trust and ownership. As a result, the Internet of Things (IoT) has been renamed to the Internet of Everything (IoE). IoE is made up of people, data, processes, and objects, much as in [2]. The Internet of Everything also improves the quality of people's lives by expanding the reach of commercial and industrial operations. Using cloud computing (CC) technology may provide the added advantage of allowing additional IoT devices to join the network. Due to its ability to increase or decrease resource consumption, such as bandwidth and storage, the cloud will help the Internet of

Things (IoT) develop more quickly and effectively. Sending and processing IoT device data via the cloud, on the other hand, presents new difficulties for IoT systems.

As demonstrated in [3], one option is to bring processing power closer to IoT devices or to the network's edge. When it comes to dealing with cloud computing's constraints, edge computing (EC) may be an improvement. However, EC is still in its infancy and faces a number of obstacles depending on the EC devices used. This decision affects both the cost and the efficiency of the project. While restrictions may need to be dealt with as a consequence of using the cloud solution, EC is not intended to replace it. Because not all tasks can be completed in EC, a method must be developed to determine which tasks should be completed in the cloud and which should be completed on the edge. It may also be difficult to balance and distribute work equally among many EC devices while using multiple EC devices. Denial of service or traffic congestion at the edge are other possible problems. The above-mentioned scenarios may be avoided by creating an effective procedure. An important issue to consider is how to control device mobility, since this may have a detrimental effect on connections between devices and the edge when mobility is significant. As a result, EC requires a method for dealing with situations with high mobility. Last but not least, EC may run into security and privacy problems because to data being pushed to the network's edge, where there is a significant probability of attack. In order to maintain high levels of security, a solid foundation is needed. For the purposes of this article, current IoT system research will be reviewed, and the feasibility of implementing an IoT system that integrates cloud and edge computing technologies will be examined. A few motivational examples are presented to help explain the benefits and drawbacks of these new technology. Fog computing is also compared to the cloud, with different metrics used to determine the advantages and disadvantages of both. In the conclusion, a framework is proposed that takes into account the advantages and limits of each to enhance overall performance.

A. Providing emergency medical services

It's possible for an emergency to happen to anybody, anywhere, at any time. Providing emergency healthcare services may help reduce hazards and perhaps save lives in certain cases. Emergency situations involving a youngster or an older person who is living alone may necessitate the use of this safety net. Multiple IoT devices may be installed in places where old people reside to monitor their health and attempt to infer any abnormalities in their health, if the latter is applicable. Having the determined instances sent to their physicians or perhaps triggering an alert at the closest medical facility would be fascinating. It is possible to gather and preserve all health data in a safe location. Doctors, on the other hand, may access patient data without ever having to set foot in the patient's house, and if a particular exam is necessary, a request could be sent to the closest medical facility to have a doctor come to the patient's home and do the evaluation that is required. To assist physicians better understand their patients' health and spot any problems, the gathered data may be examined.

B. Houses with Smart Technologies

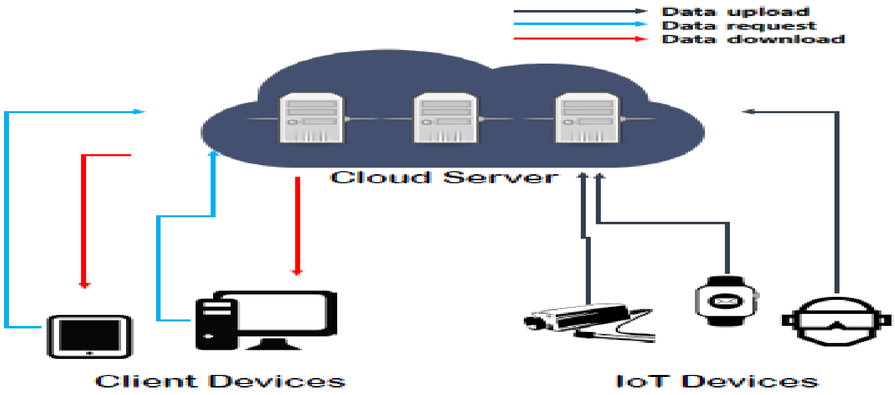
IoT applications are often used to turn a house into a smart one by placing devices around the house, such as in the kitchen and living room, and then connecting these devices or appliances to fulfil the needs of the owner... Think of it this way: when the owner is driving home, prepare an afternoon tea or switch on the AC. There are many instances of home appliances available on the market that can function in a networked environment and be controlled from a distance (i.e., over the internet). Some communication issues, such as how to manage smart home devices, make requests to these things, and gather data from each of the linked objects, remain, even with the latest technology. Another issue is that these devices are often battery-powered and thus cannot perform a large number of operations; as a result, a lightweight protocol is required. When designing this protocol, keep in mind that accessing these objects and performing activities should be kept to a minimum. There are additional ethical and privacy concerns when using smart home IoT devices, particularly if they're connected to the internet. Since the gathered data must be connected to the owner, a robust security mechanism must be implemented so that unauthorised access to the system objects or data they generate cannot be achieved. IoT security and privacy concerns were also addressed in Paper [4], including the heterogeneity of apps and devices, the lack of interoperability of service offerings, as well as fulfilling IoT standards. Edge computing was proposed by the authors as a solution to these issues. The results of the experiments indicated that the suggested prototype may improve the memory and CPU burden of the programme.

c. Supporting the Alhajj Event

The Alhajj is a massive religious gathering. Alhajj, a religious obligation for Muslims who can afford it, draws more than 2 million pilgrims from across the globe to the Saudi Arabian city of Makkah. This event is fascinating because of the restricted area and large number of participants who are all presenting themselves to do the same thing at the same time. In addition, it draws researchers who may give suggestions on how to lessen the difficulties pilgrims may face during Alhajj, or how to enhance the pilgrims' overall experience so they have a pleasant one. One option is to use Internet of Things (IoT) devices placed around the city to keep tabs on the whole event. One advantage is that the management centre will have access to the devices, which will allow them to gather and analyse data to assist in decision-making. Pilgrims may use mobile devices to control the temperature, lighting, and other aspects of their tents, similar to how smart houses work. They could also use these same mobile devices to track down their lost tents if they become separated from them. If a fire starts or spreads quickly, the control centre can keep an eye on the smart tents and alert the proper authorities. If no one is in the tent, the sensors may reduce power usage and send an alarm to volunteers or the closest medical facility, alerting them to an emergency.

D. Summary

Efficient energy management, real-time engagement, and excellent performance are just a few of the criteria that must be taken into account while evaluating the various situations described above. It may be possible to fulfil these needs via the combination of cloud and edge computing technologies. To administer an IoT system, it may be necessary to integrate various technologies, but there are certain challenges that must be overcome. As a result, this study will look at whether or not IoT systems can be integrated with cloud and edge computing in order to fulfil specific needs.



II. RELATED WORKS

When Kevin Ashton [5] pondered the application of radio frequency identification (RFID) tags on everyday goods, he proposed the idea of the Internet of Things. IoT ideas developed significantly and expanded in all directions after a few years in the late 1990s when this kind of network was initially recognised. An huge number of gadgets and items can interact with people and be introduced to many environments/domains, such as healthcare [6, 7], smart homes [8,] and autonomous cars, and so on. This is not only about attaching RFID tags to goods and products. With IoT, you may offer services to end users and manage/customize the environment in which these gadgets are deployed by using the Internet as the infrastructure [9]. One of the most comprehensive and frequently used definitions of the Internet of Things (IoT) is provided in [10]. In [10], the author created this concept by breaking the Internet of Things (IoT) into three distinct levels. While a basic architecture for the Internet of Things (IoT) is described in [11], a more sophisticated one includes five layers: an access gateway layer, middleware, internet, edge technology, and an application layer. In addition to utilising the Internet as an infrastructure for IoT devices, there are many difficulties associated with the IoT. The number of people using the internet has exploded in recent years, with estimates putting the number at over 7 billion by 2020 [12]. Other difficulties to be faced include the interactions needed between devices for IoT-based applications, which will necessitate new technologies. If more than one device/node may offer the same set of services or deal with the same job, another problem might be how tasks are carried out and in which node they are performed [14].

Combining Cloud with Internet of Things (IoT)

When it comes to dealing with some of the issues listed above, cloud computing (or the mobile cloud [15]) may play a significant role by offering a trustworthy location to carry out activities or transmit and store produced data. Using the cloud in conjunction with IoT, according to the writers in [16], will be very useful in the future of the internet. Mobile cloud paradigm introduction to IoT applications is not an easy job because of the system's inherent constraints, such as slow reaction times and concerns about security and privacy [17, 18, 19].. To cope with this connection, cloud and IoT apps need have certain special features [20]. Some examples of new paradigms that may handle IoT applications are given in the article, which considers the nature of these applications (like heterogeneity). Sensing as a Service, Data Base as a Service, Ethernet as a Service, and Video Surveillance as a Service are some examples of these concepts (VSaaS). Researchers proposed that depending on the application needs, the best cloud provider might be selected. What's hard about gathering all of these criteria is how often they'll change. If this is the case, you may need to change service providers and run into problems with migration. End users, middleware, and hardware make up the three major components of an IoT system, according to [21]. It is possible for the cloud to serve as a middleman by using sensors as hardware components to provide computing and storage services. Data acquired from the Hardware component and processed by the middleware are of relevance to end users.

The Fog Computing Company, Inc.

IoT items don't have to send all of their gathered data directly to the cloud, as described in [22], since it's obvious that putting servers near the devices and in front of the cloud would be much more efficient. Fog computing, cloudlets, and mobile edge computing are all variations on this concept. Instead of performing tasks on IoT devices, the answer is to offload them to someplace else (such as the cloud). Fog computing, mobile edge computing, and cloudlets are all viable edge layer implementations in reality. [23] compared the implementation techniques of these three keywords. Mobile edge computing occurs when servers are placed on cellular network base stations, while cloudlets occur when the servers function as a cloud capability near to users, albeit on a smaller scale. But if equipment like M2M gateways and wireless routers are relocated to the edge layer, fog computing is used, and the devices, known as fog nodes, have the function of storing and processing support before sending data to the cloud. Cloudlets accept Wi-Fi, while mobile edges accept mobile networks, and fog computing accepts many more, including mobile networks, Wi-Fi, and Bluetooth. Cloudlets and mobile edges accept mobile networks, while fog computing accepts many more. Cloudlets and mobile edges can only communicate with each other over a single hop, while fog computing allows many hops. When it comes to enabling Internet of Everything (IoE) applications, researchers at [24] made a comparison between cloud and fog computing. With important characteristics like heterogeneity and interoperability, fog computing promises to cope with the formal cloud's constraints by handling a broad range of devices. Reduced latency and enhanced location awareness are two additional benefits of fog computing. Placed in close proximity to the people making the requests. Fog computing makes use of wireless connections to cut down on traffic in the network's core while simultaneously improving mobility across the network. Fog computing, on the other hand, may provide a lower-cost option for handling gathered data. Fog computing also has the advantage of handling requests locally rather than submitting them entirely to the cloud, or at least filtering them. Increased usage of networks and reduced bandwidth consumption are the results. Managing IoT applications requires that the system react quickly to requests and events. Delays may arise as a result of problems with the execution of duties or a breakdown in communication. To prevent running activities on objects with restricted resources, jobs may be relocated away from IoT devices for the first kind of delay. By moving processing to edge servers, latency will be reduced, allowing for improved real-time interaction [25]. When dealing with delays and real-time interaction situations, cloud and edge computing may work together instead of replacing each other. To increase the speed of reaction and reduce latency, edge or fog computing may be preferable to cloud computing. Since real-time interactions need a shorter distance, fog computing is the way to go. Task submission, deployment, execution, and ultimately result return time may all be used to estimate IoT task or event reaction times according to [26]. On-demand computation and storage for IoT networks have been made possible with cloud computing. Some application requirements cannot be met by growing reliance on the cloud as a centralised solution and the distance from the cloud [27]. Furthermore, a sudden increase in traffic may degrade an application's responsiveness and usefulness. Fog computing, therefore, may be seen as a possible answer to these problems. In addition to improved performance, closeness to users may also lead to other benefits, such as increased network resilience provided the server is situated correctly. By transmitting less data to the cloud from local devices, edge computing may assist alleviate traffic bottlenecks and therefore lower network strain [25]. Multiple factors such as the number of concurrent sessions, connections and users must be taken into account if improved network resilience and reduced traffic are to be achieved in the IoT. How many requests are made, and how long does it take to process them? (a.k.a. Average response time). To effectively handle the traffic load, a defined threshold and scalability of resources should be established. The bottom line is that by placing fog computing at the network's edge, close to IoT devices, it may improve the network's resilience while also decreasing traffic on the network. Shorter connections allow IoT devices to interact with fog nodes (or edge servers). The enormous storage capacity offered by the cloud data centre is one of the most significant aspects of presenting cloud computing as a solution for IoT devices. Real-time applications can't be built on top of such a framework since delays would arise. As a result, edge computing collects data closer to its sources, resulting in reduced latency and improved performance. However, as the number of IoT devices grows, this creates a new problem. Larger storage capacity on the edge servers is required, or data must be moved to the cloud. IoT systems may benefit from adding an edge computing solution, however the restricted storage capacity of the edge must be taken into account. The management of storage capacity in IoT systems also comes with many functional needs. Unstructured files are stored and managed in a file repository using a file processor. Multiple databases for structured data may be merged and unified with the help of a database module. To make data access faster and easier, you'll need a mapping between objects and entities. An automated service module is created by producing specified data and then mapping it to the database and file repository as needed.

III. PROPOSED METHOD

Data generated by IoT devices may be saved and processed locally for faster response and decreased latency, while part of them can be stored and processed on the cloud [20]. Keeping and processing local data close at hand is essential. Cloud servers, on the other hand, may be utilised for long-term data processing and decision-making, as well as logging. By using a fog-cloud architecture, IoT processing load may be balanced between services that operate in the fog and those that run in the cloud.

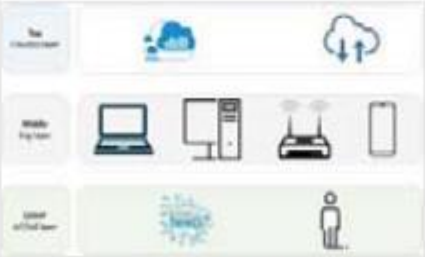


Fig. 1. Proposed framework.

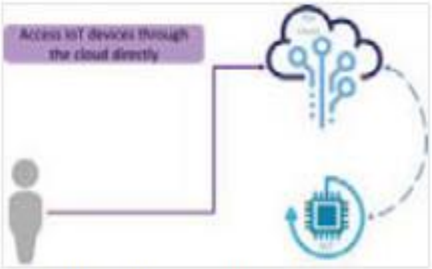


Fig. 2. Access IoT devices through the cloud directly

Fog-cloud framework for the Internet of Things

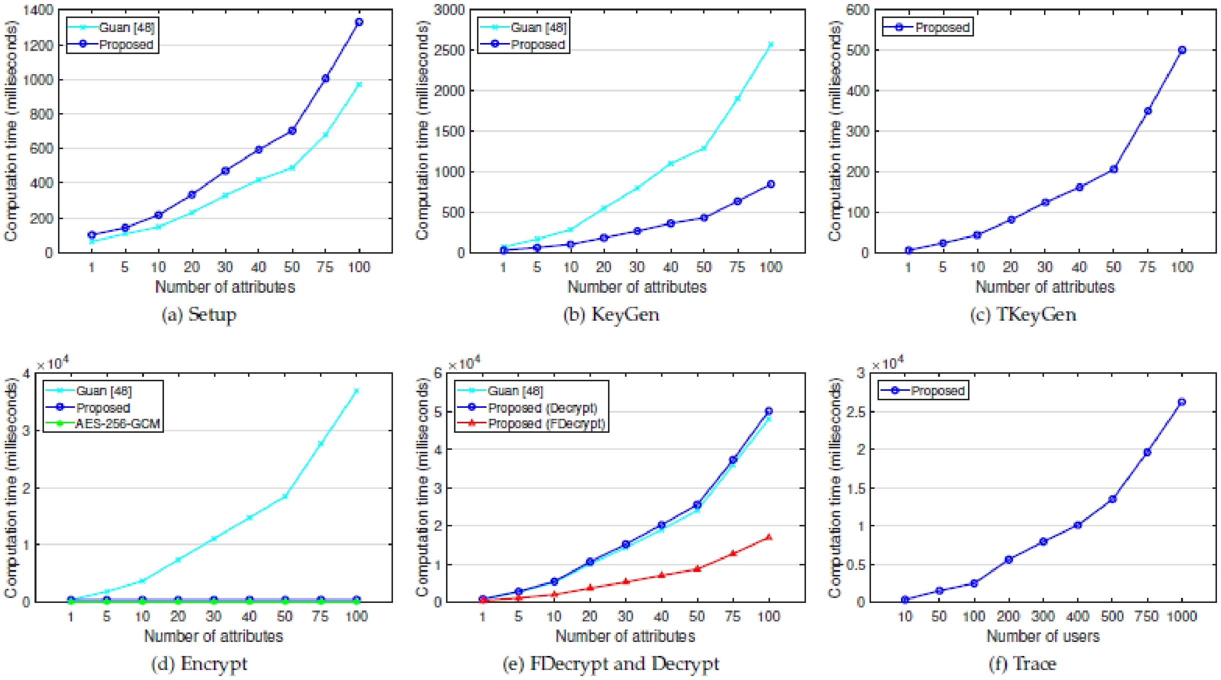
Figure 1 depicts the proposed framework's three major levels, each of which will be discussed in detail in the following paragraphs.

the cloud computing platform that primarily provides storage, processing, and connection to the whole system; this is known as the top layer. Registering all IoT devices is part of the cloud function. This means that IoT devices may directly feed the cloud as necessary. To receive real-time data, the cloud may have a direct connection to these IoT devices. The cloud also keeps track of the middle-layer fog nodes that are actively communicating with IoT devices as intermediary nodes. If a direct connection to the cloud is not available, IoT devices may contact the cloud through fog nodes. Every contact with users is also reported/stored in the cloud for smart actions or suggestions to be carried out.

It's at this layer where all the fog nodes are placed that can enable IoT devices and cloud connection. Instead of sending the same request straight from the device to the cloud, they may get better performance, such reduced latency. Fog nodes have the added benefit of reducing cloud load while also improving performance because of their cooperative nature. For example, routing requests to the cloud by utilising nearby nodes or fulfilling users' requests locally without using the cloud are both examples of cooperating. Each and every fog node must be registered in the cloud for the sake of security.

IV. RESULTS AND DISCUSSION

We used a PC with two 3.40 GHz Intel Core i5-3570 CPUs and four gigabytes of RAM to execute our authority algorithms (Setup and KeyGen). Amazon EC2 VM instances with 2.50 GHz Intel Zeon platinum 8175 microprocessors and two virtual CPUs and 8GB RAM were used to execute cloud algorithms (TKeyGen, PDecrypt, and Trace). Using the Raspberry Pi 3 Model B+ with Broadcom BCM2837B0 at 1.4 GHz and 1GB of LPDDR2 SDRAM, we ran the IoT device algorithm (Encrypt). This method was tested on a Samsung laptop with an Intel Core i7-3517U CPU clocked at 1GHz and 4GB memory. The jRAPL low-level interfaces we developed to profile Java applications were utilised as well [16]. When an IoT device uses the Encrypt technique, we utilised a power metre tester to record the current charging state [7]. As an added bonus, we evaluate the proposed method against [18], which implements the core functionality of CP-ABE for Internet of Things systems. As can be seen in Fig. 3, the computing costs of each method are shown in different scenarios. Figure 3(a) shows how the number of characteristics affects the system wide setup time. Because it computes positive, negative, and wild-card keys for each characteristic, the suggested method takes longer than [18]. Because it happens just once in the beginning, running the Setup algorithm costs nothing. There is a direct correlation between the total key generation time and the number of characteristics, as seen in Figs 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 as the number of characteristics and users grows, so does the time required for cloud-based outsourced decryption. Decryptions computed by the cloud for the user account for around 66% of all computations, with computing providing access to the remaining 36%. Symmetric encryption, rather than the ABE method, may be more effective in controlling access for numerous users. Each user should be provided with their own (symmetric) secret key, and an encryptor utilises the keys to create unique cipher texts for each person. This is how symmetric encryption works. Because of this, as the number of users grows (see Fig. 5(b)), this method becomes more unworkable. The graph illustrates the IoT device's computational load as a function of the number of users accessing the IoT data. We utilised

AES256-GCM to encrypt 128-byte IoT data and assumed KEM had 50 characteristics in the experiment.

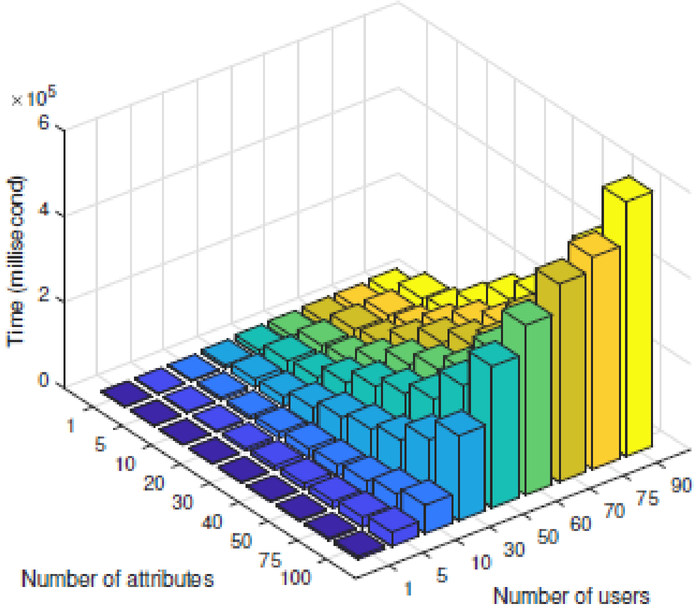
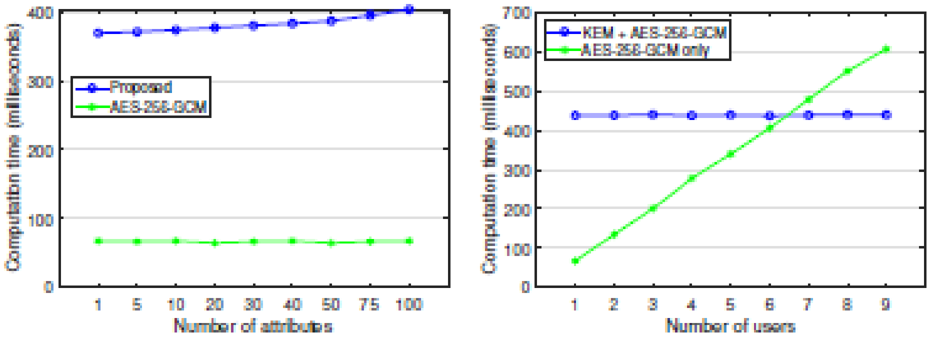


Fig. 4: Computation cost of PDecrypt on cloud server



(a) (b)

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

VI. FUTURE SCOPE AND CONCLUSION

As a result of its effective application in different situations, such as real life, IoT has recently become more popular. It has been suggested by many academics that cloud computing technology may help IoT systems cope with their problems and limits by taking use of excellent characteristics offered by this technology, such as huge storage capacity and processing power. Cloud computing, on the other hand, brings additional difficulties including latency and security.

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 (bigdata security), 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 (I Things) and IEEE Green Computing and Communications (Green Com) and IEEE Cyber, Physical and Social Computing (CPS Com) and IEEE Smart Data (Smar tData), 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] D. Grigoras and P. Gepner, "The Distributed Mobile Cloud Supporting the Internet of Things," 2015 14th International Symposium on Parallel and Distributed Computing, Limassol, 2015, pp. 9-16.

[26] H. N. Alshareef and D. Grigoras, "Mobile Ad-hoc Network Management in the Cloud," 2014 IEEE 13th International Symposium on Parallel and Distributed Computing, Marseilles, 2014, pp. 140-147.