International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Demystifying User Data Privacy in the World of IOT

Shruti Patil, Shashank Joshi

Abstract: ***Internet of Things (IoT) would touch upon almost all aspects of everyday life, as a consequence of which, everything (i.e. living and non-living things) will have a counterpart virtual identities on the internet which would be readable, addressable and locatable. Although it would empower its users with 24×7 connectivity around the global world, unknowingly they would also provide it permission to peep into user's personal world, which can generate a huge risk on the usability of IoT by users. Thus analyzing the framework of IOT from the perspective of user data protection is a very crucial self-test which is required for IoT implementation. Often the term security and privacy are used interchangeably, but in the IoT environment, both these concept would play a crucial but differentiating role. In this paper, we have scanned the IoT environment with the perspective of privacy requirements, possible threats and the mitigating solutions which are currently in use.***

Keywords: Data Privacy, Anonymization, Differential Privacy, Security, Access Control.

I. INTRODUCTION

Internet of Things (IoT) is the vision of future internet for creating an omnipresent computing world. It would evolve existing internet and provide an intelligent connectivity between huge amount of smart devices and living beings. It could be called as a dynamic global infrastructure with self-configuring capabilities with respect to standards and communication protocols where physical as well as virtual things with identities, different kinds of attributes, personalities, interfaces etc. are integrated into informative form of network [24]. One of the key challenges for practical realization of IoT is the security and privacy of "Things" involved in IoT and also of the data generated and consumed by those "Things". Key stakeholders of this future internet would be the service providers and consumers, and gaining usability trust of these stakeholders would be the major first hand task. Already multinational tech giants such as Google, Intel, Cisco, Microsoft, IBM has started launching their beta version products of various segments into the market, but are falling short in providing 100% security assurance to the users. IoT consists of multi sensor data that might be collected in fragments. The data collected, in combination with data from other sources, may reveal information on individual's habits, locations, interests and other personal information and preferences, resulting in increased user traceability and profiling. This may lead to an elevated risk of authentication issues, Identity spoofing, or modification of data in flow or at storage. Thus there is a need of more robust, adaptive and cognitive framework for IoT user data privacy and security.

Internet of Things can be realized in three paradigms—internet-oriented (middleware), things oriented (sensors) and semantic-oriented (knowledge) [Atzo,2010]. Although the usefulness of IoT can be unleashed only in an application domain where the three paradigms intersect. The RFID group defines the Internet of Things as –The worldwide network of interconnected objects uniquely addressable based on standard communication protocols.

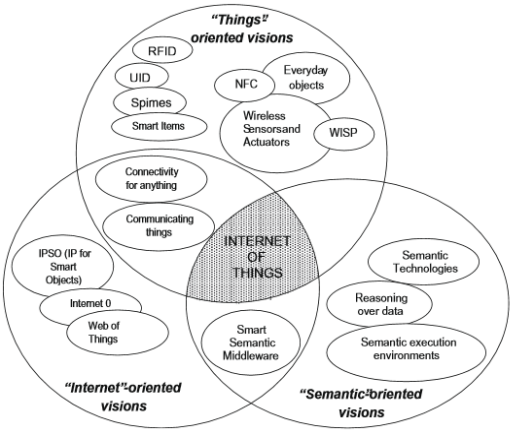

Figure 1: Internet of Things paradigms [Atzo,2010]

1.1 Internet Oriented:

IoT requires interactions with miscellaneous raw sensors, aggregators, actuators and diverse domain of context aware applications, preserving the security and privacy[2][3]. It consists of two definite components Internet and Things. Internet is a universal network environment comprising scalable, self –configuring expansion competence with the help of communication protocols whereas "Things" are physical/virtual entities/devices / information having identities, physical and virtual characteristics that use intelligent interfaces. For this purpose, IoT will require middleware. The middleware is a software platform or a pack of sub-layers intervened between the technological and the application levels. Role based information hiding is the main advantage of using middleware oriented IoT architecture.

Manuscript published on 30 August 2019.
*Correspondence Author(s)
Shruti Patil, Ph.D. research scholar, Bharati Vidyapeeth Deemed University, College of Engineering, (Assistant Professor, Symbiosis Institute of Technology, Symbiosis International (Deemed University)), Pune, India.
Dr.Shashank Joshi, Professor, Bharati Vidyapeeth Deemed University College of Engineering,Pune India

1.2 Things Oriented:

The idea of IOT can be realized into real world by placing devices in a spatially distributed manner with embedded intelligence via sensing capabilities, ability to communicate with each other by exchanging data, autonomous reactions to physical/virtual world events and taking appropriate actions by running processes without human interventions. The term "Things" encapsulates various objects that senses and provides information. They form the base of IoT framework, through which information is passed on to the middleware software. Generally these objects are designed to perform single task at a time.

1.3 Semantic Oriented:

Number of items involved in IoT is destined to be very high. So, the issues of how to represent, store, interconnect, search and organize the information generated by the IOT will become very challenging. This means that having interoperable things in IOT is a basic requirement to support attribute tracking, object identification and discovery, information storage, exchange and analysis. Semantic interoperability means, that different stakeholders can access and interpret the data unambiguously. IOT "things" will keep on sending and receiving data from other things connected to IOT network. Providing unambiguous data descriptions in a way that can be processed and interpreted by machines and software agents is a key enabler of automated information communications and interactions in IoT.

1.4 Key Elements and Challenges of IoT:

IOT is a combination of sensing tags, connectivity, people and process. It has a circular workflow where hardware senses and provides data about users and environment to the middleware which navigates the same for processing and from that knowledge is inferred which is provided to the users again. As data keeps flowing from one domain to another, it is very crucial to ensure legal data accessibility and usage. Vital user information is at high risk which would lead to unlawful profiling and harmful consequences.

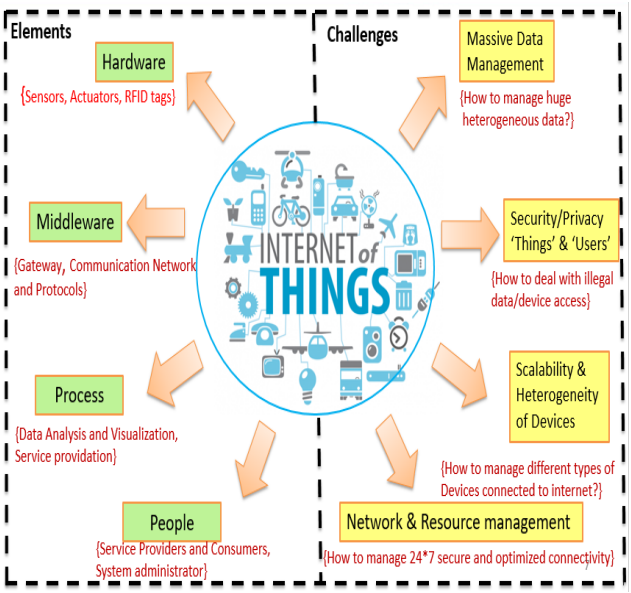

Figure 2: Key elements and challenges of IoT

On field implementation and success of IoT environment, products is still hindered by various challenges such as managing huge amount of dissimilar format data which is coming from heterogeneous devices. Also maintaining the right balance between service performance, network connectivity and scalability of the environment needs a special attention. Sicari et al. has mentioned security and privacy as one of the most crucial challenge of IoT, as till the time consumer would not feel 100% confident about personal data safety, IoT products would not be used on daily basis.[4][5]

II. DATA SECURITY VS DATA PRIVACY

Often the concept of security and privacy are used interchangeably or their functions are misunderstood. The same confusion is reiterated when it comes to security or privacy of data also. Basically privacy and security of data goes hand in hand with different but parallel functions with a single aim of protecting the data against illegal access. Data security encompasses physical and technical techniques that prevent an unauthorized access to the system where the data is stored and helps to achieve and maintain data integrity. Whereas data privacy is about achieving and maintaining the confidentiality of the personally identifiable data related to various organizations or individuals. This is done by exercising control over the purpose of data usage by whom, from where and for how much period of time. Privacy techniques mainly focuses on the sensitive data whereas security is about securing all types of information and data irrespective of their location, and sensitivity quotient. Under the privacy policy framework, it enables the data owners to establish a protocol which decides who can legitimately have access to the data for viewing or medication purpose. And security techniques helps to enforce these protocols. For example, online shopping portals, once you add items to the cart, the next step is of online payment. This step requires information mostly about your most sensitive data i.e. address, credit card number, username and password, contact number for online transaction. Protection to this data would be provided by combination of the implemented security mechanisms i.e. use of strong encryption algorithms for the network data travel as well as a very good fine grained access control which would be defined by the privacy preserving algorithms. So a strong data protection framework for any application would need presence of both security mechanisms, privacy preserving policies and techniques. [25][12] Depending upon the domain and requirement of the system, some applications might have only security mechanisms in place. Existence of security doesn't necessarily requires presence of privacy schemes. Sometimes security schemes alone are also enough to provide data protection. But vice a versa is not true [10][15]. To implement privacy, apt security schemes needs to be implemented first, because strength of security schemes defines which privacy techniques are required and should be implemented in combination.

Retrieval Number: J98350881019/19©BEIESP
DOI: 10.35940/ijitee.J9835.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

2.1 Security in IoT

Figure 3 represents an overview of data security and privacy issues, technological solutions and currently used techniques and algorithms which are available to implement those technology solutions. The area of security is mainly facing issues of various kinds of attacks that happens at various stages of data flow. The environment of IoT has added number of objects such as sensors /actuators who sense the information and forward it to the cloud storage via gateways. The processing capacity of these devices possesses a major hindrance in implementation of various security algorithms at the device end. Due to which providing strong security measures at all data point in IoT is not getting possible.

Sr.No	Security Objectives	Security threats and attacks
1	Integrity	Data tampering/modification, forging attack, false-message attacks, user manipulation attack,
2	Confidentiality	Unlawful information disclosure ,Man-in-middle attack, Eavesdropping attack, movement tracking attack
3	Availability	DOS/DDOS attacks
4	Authentication	Identity/device spoofing, Identity theft attack, stolen verifier attack, impersonation attack
5	Authorization	Privilege upgradations

Table 1: Mapping from various security attributes to possible threats

Another issue is the computation power and time required by normal encryption algorithms like RSA or AES is considerably more for an IoT environment and it will grow proportionally to the number of devices increasing in IoT and generating more data day by day. In that case, a lighter version of these algorithms would be needed which will consume less computation power and less time for encryption. Similar would be true for other security mechanisms also such as authentication authorization and key exchange protocols. One of the major goal of data security is to maintain balance between availability of data and the required confidentiality. IoT data security measures have to take care of passive as well as active threats. Passive threats are those where an attacker will only eavesdrop on the communication channel or on any available network. By eaves dropping he can collect valuable sensitive information from the sensing devices which can be further misused. Whereas under active threats, an attacker can not only eavesdrop and capture the data but can also tamper the sensitive data as well as can also change the configuration of the IoT system itself. Impersonation, Sybil attacks, spoofing, man-in –the –middle attacks are some of the well-known active threats.

2.2 Privacy in IOT

"Change is the new trend in the technology enabled 21st century". This change is taking us towards a complete new digitally led daily lifestyle which would have smart vehicles, smart hospitals, smart agriculture, smart retail, and smart education….and the list goes on. But when we are allowing technology into our day to day life, we are exposing our self also to the threats that would come along with it. Internet of Things is about having an intelligent conversation among the human beings and devices which are connected to each other 24*7 via a communication network. This conversation would be completely based on the information which the devices would capture and the decisions that humans would take based on this data. So successful smart IoT world would basically depend upon accurate data capturing, secure data flow and protected data analysis. All these three phases has to be encapsulated under the blanket of strong privacy arrangement, because till the time users of IoT will not feel safe, they would not like to be a part of this new smart connected world. Currently the privacy techniques are plagued with following threats:

Individual Identification, linking and profiling: One of the biggest privacy threat is identification of an individual from the attributes which are part of the data that is either shared publically or is accessed illegally. This is done basically for the purpose of preparing a profile of an individual. This profile then forms a base for various activities such as targeted advertising, improving the accuracy of recommendation systems etc. In most of the cases, consequences of unlawful profiling is always very harmful.

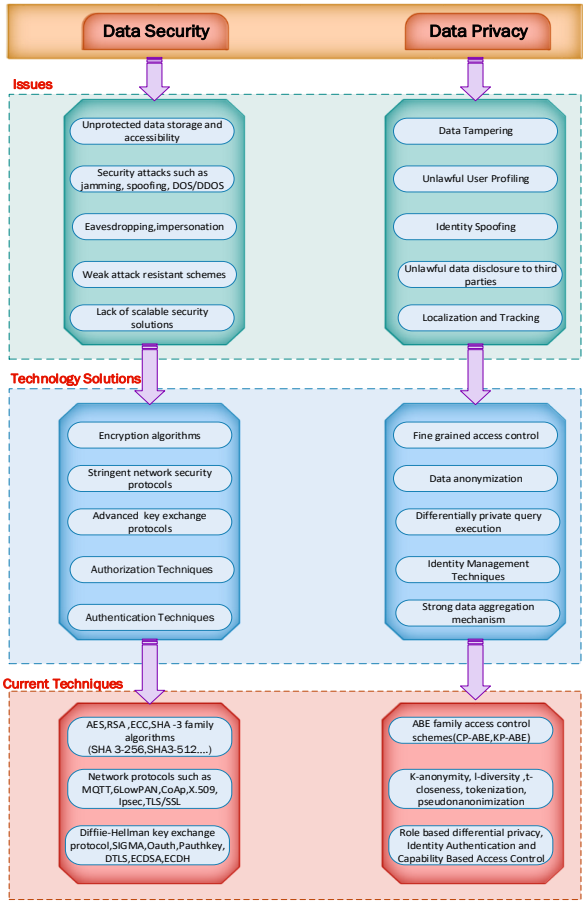

Figure 3: Overview of data security and privacy issues and solutions

Location Tracking: Location tracking is about tracking the whereabouts of an individual via various ways such as GPS location, mobile location, internet IP, Facebook check-ins etc. Again sometimes this activity can be very helpful and sometimes it can be done with a harmful intent also.

Identity Spoofing: Identity management is one of the core responsibility that comes under the umbrella of privacy management. Some years back identity was related to only physical characteristics of an individual but now along with that everyone has single or multiple virtual identities in the digital world. Physical identities are not cloaneable but virtual identities are very easily cloneable and it is known as identity spoofing. Identity spoofing is considered as a major privacy offence.

Data Tampering: Data tampering is basically a type of active privacy threat where an attacker will not only have access to the data but can also modify the data that flows in the network. All the further knowledge extraction and actions would then be based on this intentionally modified wrong data.Table 2 represents a mapping of privacy goals to the possible privacy threats if proper preventive steps are not taken at appropriate time. Privacy is about the appropriate use of data. That data can be of an individual person or of an organization and it can be in various formats such as text, video data, audio data, images, numerical content etc. So confidentiality of the data is the main goal of privacy. This confidentiality needs to be maintained at following levels:

Sr.No	Privacy objectives	Privacy threats and attacks
Sr.No	Privacy objectives	Privacy threats and attacks
1	Anonymity	Unlawful profiling /identifiability/linkability attack
2	Unlinkability	Unlawful profiling /identifiability, linkability attack
3	Confidentiality	Unlawful information disclosure, packet tracing attacks
4	Deniability	Non-repudiation, DOS/DDOS attacks
5	Accessibility	Data Tampering, Substitution attack, message modification attack,

Table 2: Mapping from various privacy attributes to possible threats

1) Privacy-preserving data publishing

Raw data captured by the devices is of no use until some kind of processing is not done on them and information is not extracted. Based on this information, knowledge is inferred which forms the base of any strategic decision. So for this purpose, publishing the data is important on which various data mining and analytics techniques are implied to gain knowledge. If the datasets consists of sensitive information, then sanitizing these datasets is very important orelse these sensitive information can reveal identity of individual. So data publishing happens in three stages; data collection, data sanitization and then publishing by the data holder.

In data sanitization step, data holder sanitizes the data to preserve data confidentiality. In data publication phase, data holder publishes data for data mining or another purpose to public or third party service providers. The improved technique proposed by Yang et al. [3], makes use of statistical analysis and encryption for privacy preserved medical data which is stored on the cloud environment.

Numerous data sanitization techniques have been proposed in the literature. It includes generalization techniques [4], [5], [6]. The suppression techniques by [6], [7]. Swapping techniques by [8] [9].

2) Privacy preserving database outsourcing

With the advent of efficient cloud computing technologies, many applications now prefer to outsource there databases on the cloud platforms. So a very strong data security and privacy arrangements needs to be done to ensure the confidentially at this level. So a combination of encryption algorithms, privacy policies, fine grained access control and stringent authentication schemes are used to ensure data confidentiality. During the data outsourcing stage, a very good balance needs to be maintained between data availability and data confidentiality as we want access to cloud data to be there 24*7 and it should not reveal any unlawful details about the individual [18].

3) Privacy preserving query processing

One more approach for data privacy is to store the data sensed by sensors into the cloud with minimal data anonymity because sometimes anonymizing the data can also lead to losing the essence of the information which inturn hampers the knowledge extraction and decision making activity. So many times such crucial data is kept in the cloud storage with minimal anonymization and information is extracted by firing the queries on the database. In such scenarios, the privacy is taken care of by differentially private query processing techniques which restricts the outcome of queries to make sure they would not reveal any sensitive information about the user. Along with this homomorphic encryption is also a suitable cryptographic algorithm in providing privacy-preserving query processing. [26]

Table 3 represents the mapping of which privacy objectives can be achieved via which specific privacy techniques and various types of algorithms that come under them.

To provide an enhanced privacy preservation, fine grained access control is one of the preferred methods in cloud based systems. These access control schemes basically provides access based on the attributes of the individual users which is known as Attribute based encryption scheme (ABE). In this scheme, the attribute set forms a key for granting the access to the data. The data owner can decide and set a data access policy which can be enforced on the data. This access policy is also known as access tree or access structure. Each ciphertext contains the set of policies. ABE scheme is further classified as Key-Policy Attribute Based Encryption (KP-ABE) and Ciphertext-Policy Attribute Based Encryption (CP-ABE).

Retrieval Number: J98350881019/19©BEIESP
DOI: 10.35940/ijitee.J9835.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Privacy Objectives / Privacy Techniques	Algorithms	Confidentiality	Unlinkability,	Anonymity	Undetectability
Data anonymization	K-anonymity model, l-Diversity, t-closeness, pseudoanonimity		√	√	√
Encryption techniques	Homomorphic encryptions, ECC , AES, SHA3,RSA	√			√
Access control techniques	CP-ABE,KP-ABE,DCAPBE	√			
Information hiding	Covert channels, Steganography techniques, Obfuscation		√	√	√
Authentication	Mutual authentication, NDLW authentication, ECC based authentication, decentralized authentication.		√	√	

Table 3: Mapping of privacy technique to algorithms which implement them to privacy objective which they fulfill.

KP-ABE is a scheme in which the set of attributes are used to describe the ciphertext and access structure is defined on user private key. The user access structure associated with private key matches with access structure implanted with ciphertext. If the match is found then only the encrypted message is allowed to be decrypted. Whereas in CP-ABE the access structure is embedded with ciphertext and attribute set are embedded with private key of user. The decryption of message is possible only if the attribute of user's private key is matched with access structure which is embedded with ciphertext. Figure 4 shows the conceptual difference between both the schemes.

KP-ABE	CP-ABE
Ciphertext + Attribute Sets	Ciphertext + Access Structure
&	&
User's Secret Key + Access policy	User's Secret Key + Attribute Sets

Figure 4: KP-ABE vs CP-ABE key combinations

There are many version available of both the above mentioned scheme, but still they suffer from the problem of attacks on the third party locations who manage the secret keys of the user. Existing CP-ABE scheme works by tagging along the data owner decided access structure along with the cipher text. But many times these access structure also reveals sensitive information about the individuals. So hidden CP-ABE came into existence which coined the idea of encrypting the access structure also along with cihertext, so that even if attack happens, the original text as well as the access structure, both would be safeguarded. This scheme also suffered from the data leakage attack if someone gets hold of the secret key then they can easily decrypt the access structure as well as the encrypted text. Also the complexity and the computational overhead of these schemes is a concern. So we propose predicate based CP-ABE scheme which without adding much complex logic and computational overhead will help to provide double security to the key storage locations, avoid attacks and data leakage.

2.3 PROPOSED PREDICATE BASED HIDDEN CP-ABE SCHEME

We propose a predicate based hidden CP-ABE scheme in which, the data owner can decide the access structure, and then the attribute values of this access structure would be replaced by random predicate based tokens. Then, along with the original text, this dummy access structure would also be encrypted and stored at the cloud storage. The mapping of the original attribute values to the token values would also be stored at the cloud storage. On the decryption side, the data users would have their individual secrets keys. Using these secret keys, the access structure would be decrypted and then the dummy values would be replaced with the original values if the data user is a valid user.

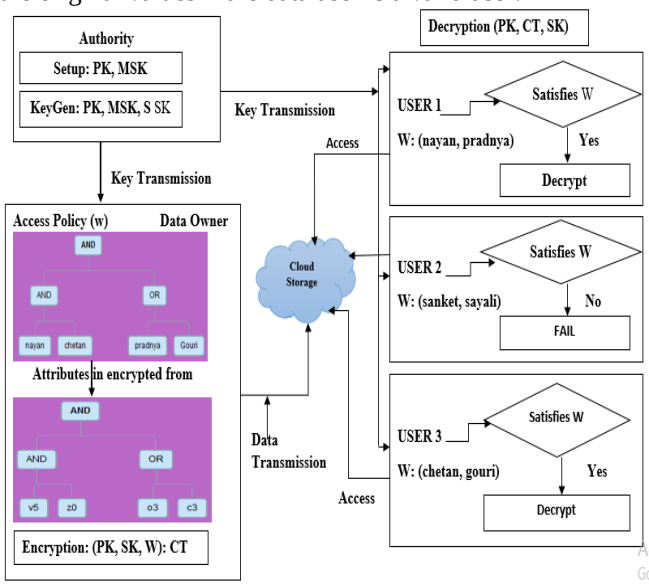

Figure 5: Predicate based hidden CP-ABE working scheme

Figure 5 shows the working scheme of proposed CP-ABE scheme. A trusted third party authority is used to generate the public key PK and master secret key (MSK) for the data owner and data users respectively. Then the data owner will decided the access policy W. Based on the replaced token values, an updated access W` would be prepared and saved on the cloud storage along with the encrypted text. When the data users wants to access the data, a request is sent to the trusted authority, using the MSK and individual secret key SK is generated and shared with the user. Once the user receives SK, then using the same the access structure us decrypted, token values are replaced and then checked whether access to ciphertext should be provided or not. If the user's secret key satisfies the access policy, then the ciphertext is decrypted and original data is shared with the data user.

2.3.3 Predicate based hidden CP-ABE algorithmic stages

The proposed methodology is implemented in four algorithmic phases as:

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

1. Setup: The setup phase is executed at the trusted authority side and is responsible for the generation of public and master secret key.
Input: Security parameters and attributes {A1, A2, A3…An} as input.
Output: public key Pk and master key MSK for each role and attribute.
2. Encryption: The encryption phase is responsible for the preparation of cipher text from the original value and access structure
Input: public key Pk, message M, access structure W.
Output: ciphertext CT along with encrypted access structure W.

3. Key Generation: The key generation algorithm would receive the request from the data users and will generate individual secret kays for each user using the trusted authority.
Input: public key Pk, master secret key MSK
Output: private key SK.

4. Decryption: The decryption algorithm will check the secret kay of each user and then based on the attribute sets, the access to the original text would be granted or rejected.
Input: public key Pk, ciphertext CT, private key Sk.
Output: message M.
To encrypt the original text, we have used AES algorithms whereas, the actual hiding of the access structure along with the message ciphertext is taken care of by Inner Product Encryption (IPE)

2.4 PERFORMANCE ANALYSIS

To evaluate the performance of the proposed scheme, the implemented application was loaded on glassfish server. Several experiments were conducted to measure time taken to encrypt the files under different scenarios. Five file sizes have been used for this purpose: 14KB, 24KB, 30KB, 39KB, and 62KB. All experiments were iterated 10 times and an average value of those ten result has been recorded. Figure 6 shows the graphical representation of the same. The graph shows that , time requierd for encryption was more as compared to decryption as encryption required encyption of original text and acess structure
also.

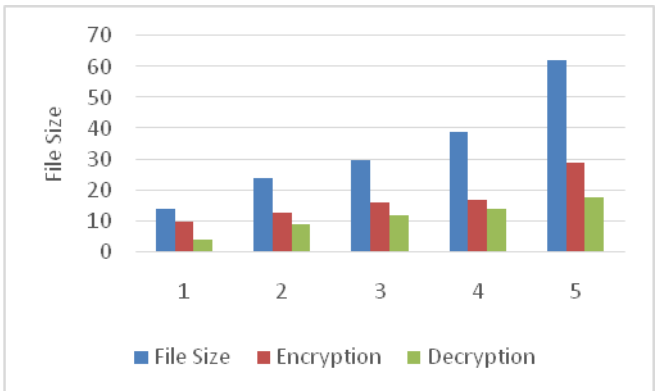

Figure 6 Performance of CP-ABE for encryption and decryption with file size

Figure 7 shows a comparison running times of the algorithms Key Generation, Encrypt and Decrypt with different number of attributes from 10 to 70

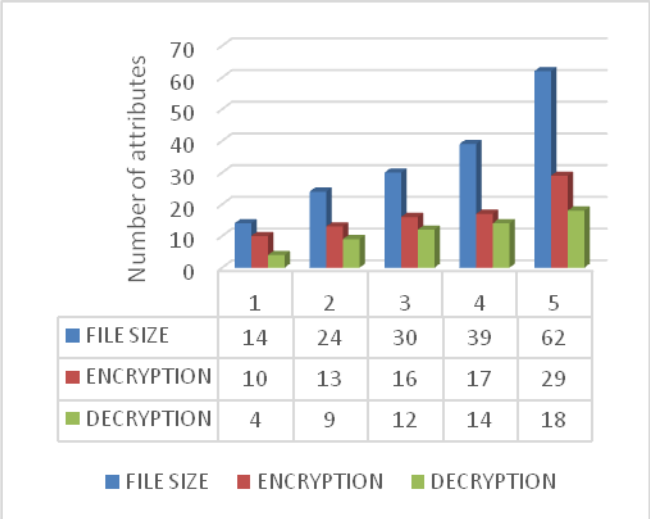

Figure 7 Performance of CP-ABE to encryption with no of attributes

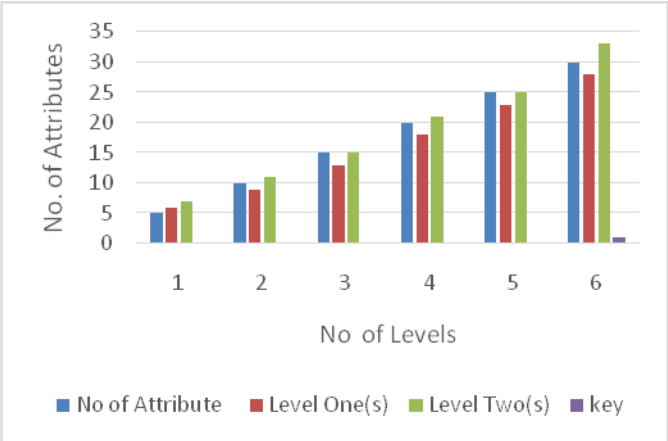

Figure 8 Performance of CP-ABE for encryption of each level of access tree

III. CONCLUSION

Digitalization of our day to day life has already commenced and human identity protection is in the hands of security and privacy technological arrangements which are currently in the developing stage. Embracement of this new digital era would completely depend upon how securely private the user would feel while using all the smart technological avatars of daily services. So it would be of prime importance to protect the personal information of the individual stakeholders from being revealed and misused by unauthorized subjects. But often, security solutions are given more importance as compared to privacy, as there is a misconception that if we secure the data it means its privacy is also taken care off. This paper mainly concentrates on the showcasing how privacy is different from security and also proposed a fine grained access control scheme to enhance the privacy preservation of cloud enabled IoT systems.

Retrieval Number: J98350881019/19©BEIESP
DOI: 10.35940/ijitee.J9835.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

REFERENCES

1. Sundmaeker, Harald, et al. "Vision and challenges for realising the Internet of Things." *Cluster of European Research Projects on the Internet of Things, European Commision* 3.3 (2010): 34-36.
2. Bandyopadhyay, Soma, et al. "Role of middleware for internet of things: A study." *International Journal of Computer Science and Engineering Survey* 2.3 (2011): 94-105.
3. Ziegeldorf, Jan Henrik, Oscar Garcia Morchon, and Klaus Wehrle. "Privacy in the Internet of Things: threats and challenges." *Security and Communication Networks* 7.12 (2014): 2728-2742.
4. Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. IEEE Internet Computing, (1), pp. 69-73.
5. Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." *Computer networks* 54.15 (2010): 2787-2805
6. Bekara, Chakib. "Security Issues and Challenges for the IoT-based Smart Grid." Procedia Computer Science 34 (2014): 532-537.
7. Mahalle, Parikshit N., Bayu Anggorojati, Neeli R. Prasad, and Ramjee Prasad. "Identity authentication and capability based access control (iacac) for the internet of things." Journal of Cyber Security and Mobility 1, no. 4 (2013): 309-348.
8. Sicari, S., A. Rizzardi, L. A. Grieco, and A. Coen-Porisini. "Security, privacy and trust in Internet of Things: The road ahead." Computer Networks 76 (2015): 146-164.
9. Stankovic, John. "Research directions for the internet of things." Internet of Things Journal, IEEE 1, no. 1 (2014): 3-9.
10. Suo, Hui, Jiafu Wan, Caifeng Zou, and Jianqi Liu. "Security in the internet of things: a review." In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3, pp. 648-651. IEEE, 2012.
11. Yan, Zheng, Peng Zhang, and Athanasios V. Vasilakos. "A survey on trust management for Internet of Things." Journal of network and computer applications 42 (2014): 120-134.
12. Aleisa, Noura, and Karen Renaud. "Privacy of the internet of things: a systematic literature review." *Proceedings of the 50th Hawaii International Conference on System Sciences*. 2017.
13. Ferrag, Mohamed Amine, et al. "Authentication protocols for Internet of Things: A comprehensive survey." *Security and Communication Networks* 2017 (2017).
14. Kim, Hokeun, and Edward A. Lee. "Authentication and Authorization for the Internet of Things." *IT Professional* 19.5 (2017): 27-33.
15. Deng, Mina, et al. "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements." *Requirements Engineering* 16.1 (2011): 3-32.
16. Appari, Ajit, and M. Eric Johnson. "Information security and privacy in healthcare: current state of research." *International journal of Internet and enterprise management* 6.4 (2010): 279-314.
17. Rao, P. Ram Mohan, S. Murali Krishna, and AP Siva Kumar. "Privacy preservation techniques in big data analytics: a survey." *Journal of Big Data* 5.1 (2018): 33.
18. Abouelmehdi, Karim, Abderrahim Beni-Hessane, and Hayat Khaloufi. "Big healthcare data: preserving security and privacy." *Journal of Big Data* 5.1 (2018): 1.
19. Huang, Qinlong, Yixian Yang, and Licheng Wang. "Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things." *IEEE Access* 5 (2017): 12941-12950.
20. Zheng, Xu, Zhipeng Cai, and Yingshu Li. "Data linkage in smart internet of things systems: A consideration from a privacy perspective." *IEEE Communications Magazine* 56.9 (2018): 55-61.
21. Ambrosin, Moreno, et al. "On the feasibility of attribute-based encryption on internet of things devices." *IEEE Micro* 36.6 (2016): 25-35.
22. Mushtaq, Muhammad Faheem, et al. "Cloud computing environment and security challenges: A review." *International Journal of Advanced Computer Science and Application* 8.10 (2017): 183-195.
23. Al-Garadi, Mohammed Ali, et al. "A survey of machine and deep learning methods for internet of things (IoT) security." *arXiv preprint arXiv:1807.11023* (2018).
24. Mehrotra, Sharad, et al. "TIPPERS: A privacy cognizant IoT environment." *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*. IEEE, 2016
25. Liu, Yuhong, et al. "A survey of security and privacy challenges in cloud computing: solutions and future directions." *Journal of Computing Science and Engineering* 9.3 (2015): 119-133.
26. Shaikh, Azharuddin, and Shruti Patil. "Role of Differential Privacy in a New Age Data Privacy Environment." *International Journal of Pure and Applied Mathematics* 118.24 (2018).
27. Dey, Sumita, et al. "A Survey of the Internet of Things." *IOSR Journal of Computer Engineering* 18.1 (2016): 80-85.