An Overview of Security and Privacy Aspects for Cloud Computing, IOT and Cloud Based IOT

Shubhangi N. Warkhede **Pallavi S. Rakhonde** **Gopal V. Masane** **Nilesh M. Verulkar**

***Abstract* — Now a days security and privacy is the main issue in information technology which is in cloud computing, Internet of things (IoT), cloud based IoT. Generally the data is located in different places sometime it is in cloud, IoT and cloud based IoT technologies. The designer deal with the hardware as well as software, but the data security and privacy is the main issues. Hence sharing data with consumer is a difficult task.**

This paper review different security techniquesand privacy technique in cloud computing, Internet of things and cloud based IOT. We also explore the different attacks and types of attacks present in all above technology.

***Keyword*—Cloud computing, Internet of things, cloud based IoT, Security, Privacy.**

I. INTRODUCTION

Cloud is an environment of the hardware and software resources in the data centers that provide diverse services over the network or the Internet to satisfy user’s requirements [1]. The term “cloud computing” originates from network topology.[4] Cloud computing is mainly classified into 3 segments: application, storage, and connectivity. Cloud computing environment promises lower costs, easier maintenance, rapid scaling, and service availability anywhere , anytime, a key challenge is how to ensure and build confidence that the cloud can handle user data securely.[5] One of the most significant barriers to adoption is data security, which is accompanied by issues including compliance, privacy, trust, and legal matters[1] Cloud computing can be considered as a new computing archetype that can provide services on demand at a minimal cost.

The well-known and commonly used service models in the cloud paradigm are software as a service (SaaS),platform as a service (PaaS), and infrastructure as a service (IaaS),[1] Development as a service (DaaS), Communication as service (CaaS), Network as a service (NaaS).[8] In SaaS, Ex. Google Apps, Microsoft office 365, GT Nexus, Markets and Trade Card. software with the related data is deployed by a cloud service provider, and users can use it through the web browsers. In PaaS, a service provider facilitates services to the users with a set of software programs that can solve the specific tasks. Some examples of PaaS include -Force.com, Orange’s cape, AWS Elastic Beanstalk, Cloud Foundry, Heroku, Google AppEngine, Microsoft Azure. In IaaS, the cloud service provider facilitates services to the users with virtual machines and storage to improve their business capabilities. [1] Examples of IaaSinclude: Amazon Elastic Cloud Computing,

A. Cloud deployment models:

1. Private Cloud:

Cloud is deployed, observed, and engaged for a particular distance area. However, it will be overseas through internet connection but from private branch.

2. Public Cloud:

Infrastructure is available to the public users, for example, Google-Drive service. In fact, public cloud enables a consumer to develop and deploy a service in the cloud with very little financial outlay compared with the capital usually required with other cloud computing services.

3. Hybrid Cloud:

Any cloud infrastructures have numerous clouds in different area. Only the clouds allow information, or partial information that allowed shifting between clouds. Private and public clouds can be compounded to support the requirements of retaining organizational data and offer services in the cloud.

4. Community Cloud:

This cloud is used for large infrastructure, such as government organizations that connect to one cloud to upload data with unified information or a campus server that connects one cloud computing community. [4]

The Internet of Things paradigm envisions the pervasive interconnection and cooperation of smart things over the current and future Internet infrastructure. [9] The internet was designed to allow people to communicate. The IOT takes people out of the loop letting machines talk unimpeded. But taking humans completely out of the loop with machines sensing, deciding and acting on their own brings a host of potential control and monitoring problem. [10] Privacy has been a hot research topic in different technology and application areas that are important enablers of the IOT vision, e.g. RFID, wireless sensor networks (WSN), web personalization, and mobile applications and platforms.[09]

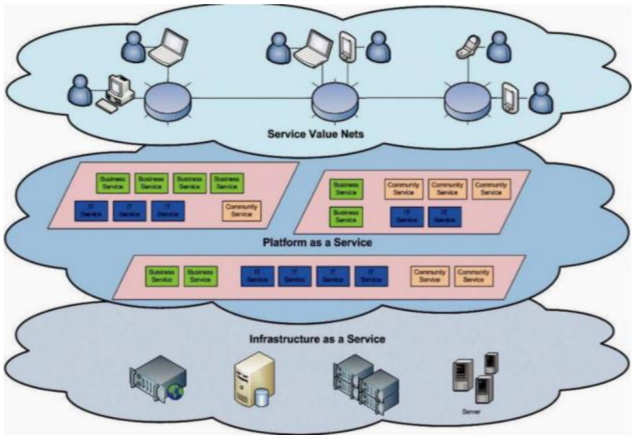

Fig 1. Service model

II. Security

The meaning of security is plentiful. Security is the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of unauthorized withholding of information.[1] There are number of security issues/concerns associated with cloud computing but these cloud providers and security issues faced by their customers.[5] There are many security threats with cloud computing because it is comprised of several technologies like databases, operating systems, different networks, transaction management, virtualization etc.[8]. Cloud services are applications running somewhere in the Cloud Computing infrastructures through internal network or Internet. [7].There is number of technology and policies to protect the data.

1. Administrative access & Data ownership:

It is very important to control administrative access to data and monitor the access to maintain protocols. Data in the cloud is globally distributed which brings the issue of jurisdiction and privacy Organizations stand a risk of not complying with government policies .There should be strong policy regarding Data ownership and organizations must comply government policies.[8]

2. Privacy of data:

Data in the cloud is globally distributed. The user doesn’t have information about the location of data and they don’t have any control over physical access mechanism to that data. [8]

3. Transmission of data:

Encryption technique is used to for data during transmission but most of the data is not encrypted in the processing time and to process the data for any application it must be unencrypted. An attacker can find a place between communication paths. The attacker can change the communication. [8].

4. Sharing of data:

The data access to one party and in turn the party can further share the data to another party. This sharing can create a serious problem like leakage of data to an unauthorized person. [8]

5. Data Integrity:

Data can corrupt at any stage and with any type of media. So, it is very difficult to check integrity of data by user because the user has no control over data and their location. [8]

6. Key Management:

A huge amount of data is stored by the user and it is difficult to encrypt large amount of data. Encryption and decryption raises the issue of key management .As the cloud providers need to maintain keys for a large number of users, key management becomes more difficult. [8]

7. Destruction of data:

Due to physical characteristics of storage medium, the data deleted may still exist and can be restored. This may result in disclose of sensitive data. [8]

A. Cloud security controls -

Cloud computing security architecture is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls. Security controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. [5]

1. Deterrent controls: Deterrent controls are set in place to prevent any purposeful attack on a cloud system. Much like a warning sign on a fence or a property, deterrent controls do not reduce the actual vulnerability of a system. [5]

2. Preventative controls: Preventative controls upgrade the strength of the system by managing the vulnerabilities. This control will safeguard vulnerabilities of system. If an attack were to occur, these controls are in place to cover the attack and reduce the damage and violation to the systems security. [5]

3.*Corrective controls:* These controls are used to reduce the effect of an attack. Unlike the preventative controls, these controls take action as an attack is occurring. [5]

4. Detective controls: These controls are used to detect any attacks that may be occurring to the system. In the event of an attack, this control will signal the preventative or corrective controls to address the issue. [5]

In short, the foremost issues in cloud data security include data privacy, data protection, data availability, data location, and secure transmission. [1]

1. Data Integrity –

Generally, data integrity means protecting data from unauthorized deletion, modification, or fabrication. Data integrity is easily achieved in a standalone system with a single database. Data integrity in the standalone system is maintained via database constraints and transactions, which areusually, finished by database management system (DBMS) Data integrity in the cloud system means preserving information integrity. The data should not be lost or modified by unauthorized users. [1].

Data integrity in the Cloud system means to preserve information integrity (i.e., not lost or modified by unauthorized users). As data is the base for providing Cloud Computing services, such as Data as a Services, Software as a Service, Platform as a Service, keeping data integrity is a fundamental task.

2. Data Confidentiality –

Data confidentiality is important for users to store their private or confidential data in the cloud. Authentication and access control strategies are used to ensure data confidentiality. The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness [1]. Confidentiality means keeping users' data secret in the Cloud systems.

The confidentiality in Cloud systems is a big obstacle for users to step into it, as many users said "My sensitive corporate data will never be in the Cloud" in the article named "Above the Cloud" [7]. Encrypted storage is another choice to enhance the confidentiality. [7].

3. Data Availability –

Data availability means the following: when accidents such as hard disk damage, IDC fire, and network failures occur, the extent that user's data can be used or recovered and how the users verify their data by techniques rather than depending on the credit guarantee by the cloud service provider alone. [1] The goal of availability for Cloud Computing systems (including applications and its infrastructures) is to ensure its users can use them at any time, at any place.

As its web-native nature, Cloud Computing system enables its users to access the system (e.g., applications, services) from anywhere. This is true for all the Cloud Computing systems (e.g., DaaS, SaaS, PaaS, IaaS, and etc.). Required to be accessed at any time, the Cloud Computing system should be severing all the time for all the users (say it is scalable for any number of users) [7]

A security and privacy framework for RFID in cloud computing was proposed for RFID technology integrated to the cloud computing [14],which will combine the cloud computing with the Internet of Things.[1]

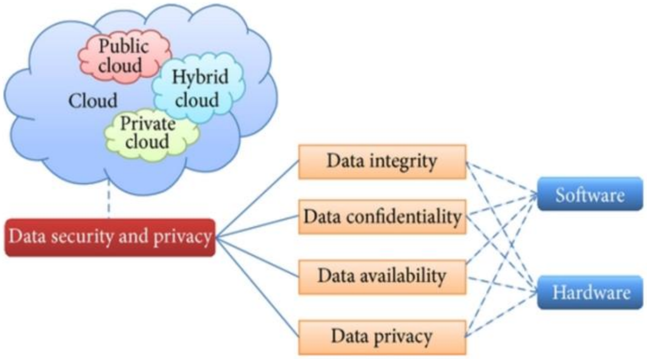

Fig 2: Organization of data security and privacy in cloud computing.

Fundamentally, securing connected devices is similar to securing other elements of your IOT infrastructure. You need to protect data at rest on the device and in transit between endpoints and other IOT infrastructure (such as hubs or other devices), or between back-end management systems. Similarly, you have to secure devices against authentication-based attacks like brute-force password guessing.

Our contributions take the form of a conceptual Reference Architecture for building a security, privacy, and trust management protocol (SPTP) that is capable of protecting private data at the time of disclosure or collection, in-transit, at-rest and for the life of a private data element even when it crosses the boundaries of the original system to be consumed by another system. In addition, we propose a logical Reference Architecture for building cloud-enabled IOT applications.[11]

3) SPTP Protocol -

As the results of our survey indicates, the savvy users of these technologies will have more trust and confidence in cloud-enabled ubiquitous solutions if they can garner some form of assurance that a third-party privacy protocol that enforces compliance standards has certified the application. Similar to the Data Security Standards (DSS) compliance requirements that often governs the Payment Card Industry (PCI) we envision that it will be useful for third-party entities to adopt our proposed protocol or a variant of it, for managing the expectations for trustworthiness among cloud-enabled ubiquitous systems and web sites. [11]

SPTP Evaluation -

To evaluate the SPTP protocol, we plan on employing a number of approaches including:

- User survey on the perceived benefits of SPTP
- Performance measurement access control
- Analysis of the SPTP protocol and its impact on Ubiquitous system adoption and trust management. [11]

III. PRIVACY

Privacy is the ability of an individual or group to seclude them or information about themselves and thereby reveal them selectively. Privacy has the following elements.

(I) when: a subject may be more concerned about the current or future information being revealed than information from the past.

(ii) How: a user may be comfortable if his/her friends can manually request his/her information, but the user may not like alerts to be sent automatically and frequently.

(iii) Extent: a user may rather have his/her information reported as an ambiguous region rather than a precise point.

In the cloud, the privacy means when users visit the sensitive data, the cloud services can prevent potential adversary from inferring the user’s behavior by the user’s visit model (not direct data leakage).[1] Finally, cloud computing providers ensure that all critical data are masked or encrypted and that only authorized users have access to data in its entirety. [5].

As Cloud Computing system usually offers services (e.g. DaaS, SaaS, IPMaaS, PaaS, and so on) on the other side of the Internet in terms of its users, the secret information of individual users’ and business’ are stored and managed by the service providers, and consequently results in privacy concerns. [7]

A. Legal Issues –

1. Electronic Communications Privacy Act (ECPA):

In an electronic environment, the Electronic Communications Privacy Act of 1986 (ECPA) provides some protections against government to access the electronic information that is stored in the storage device of the third parties (e.g., Internet service providers), including electronic mail and other computer information, and so on.[7]

2. USA PATRIOT Act (UPA): The USA PATRIOT

Act, as originally enacted in 2001 and amended in 2005, includes provisions allowing the FBI to access any business record. Although a court order is required, the FBI’s authority under the USA PATRIOT Act is sufficient to extend to a record maintained by a Cloud provider, say Cloud users’ privacy can’t be protected. [7]

3. Health Insurance Portability and Accountability Act (HIPAA): The HIPAA health privacy rule imposes some limits on compelled disclosures. A legal demand by a private party to a Cloud provider for disclosure of protected health information would lead the users’ privacy information to be disclosed. [7]

4. Fair Credit Reporting Act (FCRA): The Fair Credit Reporting Act imposes limits on the use of credit reports by a user of credit report to a permissible purpose. If a creditor stores a credit report with a Cloud provider, and a third party obtains the report from the Cloud provider, the legal limit on use could be violated [7]

5·Video Privacy Protection Act (VPPA): Video Privacy Protection Act limits some disclosures of customer data. If the Cloud provider’s terms of service allow the provider to see, use, or disclose the information, the Cloud provider’s actions could result in a violation of the law. [7]

6. Gramm Leach Bliley Act (GLBA): Gramm Leach Bliley Act restricts financial institutions from disclosing a consumer’s personal financial information to a nonaffiliated third party. However, disclosure to a service provider is generally not restricted. [7]

7. Cable Communications Policy Act (CCPA): Cable Communications Policy Act protects cable television subscriber records, but not directly prevent the use of a Cloud provider. [7]

B.Multi Location Issues:

Cloud system means to offer huge computer resource to users, including infrastructure, platform, services (e.g., storage, computing power, and so on). Hence, a business has to trust the Clouds system vendor and store its private data to the Cloud system. [7]

1. Multi-location of the private data: It is rather dangerous, if the business stores its private data in the third party’s device. In this sense, the businesses’ private data are sitting in someone else’s computer, and in someone else’s facility. Then, many things can go wrong. Firstly, the Cloud service provider may go out of business. Secondly, the Cloud service provider may decide to hold the data as hostage if there is a dispute. [7]

2. Multi-location of the service provider: The Cloud service Client (e.g., business user or private user) also needs to make sure how the Cloud service provider performs their declared services. Thus, the Cloud service client is able to keep a direct relationship with the provider, and control over its own private data. [7]

3. Data combination and commingling: The Cloud Computing client (e.g., business user or private user) needs to ensure that its private data whether its private data is stored separately from others or not. If they are combined or commingled with those of other clients’ data, then it is much more vulnerable or dangerous. [7].

4. Data combination and commingling: The Cloud Computing client (e.g., business user or private user) needs to ensure that its private data whether its private data is stored separately from others or not. [7]

5. Restrictions on techniques and logistics: It might be rather difficult or even impossible for the Cloud service provider to assure the locations where the Cloud Computing client’s data will be stored. [7].

6.Data transfer across the borders: If a global company that wishes to take advantages of services hosted on Cloud Computing systems, it has to make clear which countries are hosting its private data and providing Cloud services, and the their individual laws govern its data.. [7]
The IOT system interacts with its own cloud-hosted service layer as well as external services. The IOT application user interface itself might have its own privacy and security concerns. [11].

A. Improving Privacy Concerns in this Case Study:

Some of the concerns considered in enforcing privacy and security best practices at various layers of the reference architecture include:
1. Informed Consent: We learned that **e**nd-users preferred to be notified when the Kinect sensor is collecting both sensitive and non-sensitive data in the smart environment. A visual cue by the form of a blinking green light indicator on the device while it is in recording mode proves to be useful. [11]

2. Control over Privacy Settings: The parent’s in the household may not want their children to have access to uncensored content, so the parent might want control over media content suggestions that are surfaced to the children in the household. Also, the parent might want to limit how much data is stored by the IOT App (for example, exclude geo-location information from data collection). [11]

3. Vendor Regulation: A third-party regulation body could be employed to monitor and expose gaps in the system based on the end-user’s pre-defined security and privacy preferences. Ongoing risk assessments on behalf of the end-users could prove to be useful. [11]
4. Access to User Data and Opt-Out: In some cases, participants prefer control over the data that is collected about them. End-users are also interested in how their data is used and seek to reserve the ability to opt-out and delete their data at will. [11]

5.Ongoing Reputation Access: Beyond the participant’s initial consent to allowing the IOT App access to his or her Facebook (OSN) data, it will be useful if the participant can access the privacy of the IOT solution itself at any point in time and opt-out without any loom of lock-in. [11]

6.User Identification and Authentication: If the identity management system throughout the IOT implementation is not accurate, uncensored content that might be appropriate for the parent but inappropriate for the child might be surfaced mistakenly to the child. [11]

7. Physical Security and Wireless Networks: Prevention of eavesdropping in the wireless network as well as measures to enforce security of the physical objects in the environment proves to be critical. [11].

IV. AUTHENTICATION ATTACKS

A. CLOUD BASED:

Research studies reveal that any authentication mechanism related to web applications and cloud should provide high security, easy to use interface and support user mobility. The customers prefer to access their applications from different locations and different devices such as desktop, laptop, PDA, smart phones, cell phones etc. Those needs pose significant requirements to the security of applications. [2] a detailed description of the attacks and the possible solutions are given.

- *Eavesdropping*:

Eavesdropping involves the act of listening to the communication channel established between two authorized users. [2]

- *Man-in-the-Middle Attack (MITM):*

MITM has become quite popular in the SaaS environment. Here the attacker intercepts the communication channel established between legitimate users and modifies the communication between client and server without their knowledge [2].

- *Wrapping Attack***:** A XML:

This attack is launched by duplicating the credentials in the login phase by modifying the Simple Object Access Protocol (SOAP) messages exchanged between the browser and the server during communication set up [2].

- *Flooding Attack*:

A successfully authorize adversary can easily send bogus request to the cloud. The cloud server before providing the requested service, checks for the authenticity of the requested jobs and the process consumes CPU utilization, memory etc. [2]

- *Browser Attack*:

This attack which results in data stealing is committed by sabotaging the signature and encryption during the translation of SOAP messages in between the web browser and web server. [2]

- *Impersonating Attack:*

Here the adversary pretends to be a valid server or user and lures a valid entity to reveal the authenticating credentials which in turn is used to gain unauthorized access to the resources. [2].

- *SSL Attacks:*

Secure Socket Layer (SSL) is a fundamental security mechanism that encrypts the information transmitted between client and server. [2]

- *Cookie Poisoning:*

In cookie poisoning, the identity related credentials stored in the cookies of an authorized user are modified by the attacker to gain unauthorized access to resources. [2]

- *Replay Attack:*

In a capture-replay attack the authentication message contains the same authentication tokens previously exchanged between an authorized user and sender and was sniffed by the attacker [2].

- *Session Hijacking:*

Session hijacking is possible, if the Session ID issued to the authenticated users is not protected properly, which in turn can be used for spoofing identity. [2]

- *Shoulder Surfing Attack:*

The attacker gains knowledge of the secret credentials such of the victim by covertly observing his entry of sensitive data via the keyboard. [2]

- *Cloud Malware Injection Attack:*

The attack aims at injecting a malicious service implementation or virtual machine instance, which appears as one of the valid service instances running in the cloud. [2]

- *Reflection Attack:*

This attack normally done by creating parallel session is launched by an unauthorized user to establish a valid session with the server. The attacker impersonates a valid user and requests a login session to the server. [2]

- *Customer Fraud Attack:*

This is a special type of attack where in the client deliberately compromises its authentication token. The attack can be done to take personal advantages or to defame the organization [2]

- *Denial-of-Service (DOS Attacks):*

The main objective of DOS attack is to overload the target machine with bogus service requests to prevent it from responding to legitimate requests.

- *Insider Attacks:*

An insider can be a current or former employee, contractor or business partner of an organization who misused his right to access the sensitive resources of the organization that negatively affected the confidentiality, integrity or availability of the organization or organizations information systems [2].

B.IOT BASED

1.Botnets:

A botnet is a network of system combine together with the purpose of remotely taking control and disturbing malware. Controlled by botnet operators via command-and-control-servers.

2.Data and identity theft:

While the news is full of scary and unpredictable hackers accessing data and money with all types of impressive hacks, we are often also our own biggest security enemy. .

3. Password Discovery Attacks:

Attackers adopt several mechanisms to retrieve passwords stored or transmitted by a computer system to launch this attack. A few strategies adopted depending upon the availability of information related to the password are discussed in the following paragraphs:

i) Guessing Attack: Most often people use easy to remember passwords which make them vulnerable to guessing attack. An adversary observes some information related to the password, tries to guess, it and then verifies it by trying to login multiple times until he gets the access. [2]

ii) Brute Force Attack: This attack is launched by guessing passwords containing all possible combinations of letters, numbers and alphanumeric characters until the attacker get the correct password. Brute force attack usually carried out using automated methods demands a lot of computing power and time to be successful. [2]

iii) Dictionary Attack: Here the attacker tries to guess a password from a pre-computed dictionary of passwords. To resist this type of an attack, the password should be random and should not be a dictionary word. Even passwords in mother tongues are not secure as attackers have dictionaries of most of the regional languages [2].

iv) Video Recording Attack: In such type of attack launched in public places, the attackers with the help of camera
Equipped mobile phones or miniature camera captures the password while the victim enters the same. [2]

C.CLOUD BASED IOT:

One of Fotinet'prediction for 2017 is that the IOT will become the weakest link for attacking the cloud. That threat can come in many forms, as IoT devices have been shown to be more likely to contain easily exploitable vulnerabilities, making then a growing target for cybercriminals seeking, for example, to expand their botnets and weaponries them.

But vulnerabilities are not the only issue.as IoT devices are being developed they must also be managed, and they are increasingly being managed by cloud solution that require a communication channel between the IoT device and its master controller in the cloud.

V. Conclusion

Cloud computing and IOT is an emerging technology in current decade. But to share and transfer the data to consumer trust is necessary. There are various ways for data security and privacy in cloud, IoT, and cloud based IoT. This paper carries various ways for security, privacy and data storage in cloud, IOT and cloud based IOT. This paper also deals with authentication attack in all emerging technologies.

References

[1] Yunchuan Sun, Junsheng Zhang, YongpingXiong, and GuangyuZhu,"Data Security and Privacy in Cloud Computing, "Received 25 April 2014; Accepted 26 June 2014; Published 16 July 2014,pp.
1-7.

[2] B.Sumitra, C.R. Pethuru, M.Misbahuddin,"A Survey of Cloud Authentication Attacks and solution approaches",Vol. 2, Issue 10, October 2014,pp.6246-6252.

[3] SaˇsaRadomirovi´c, "Towards a Model for Security and Privacy In the Internet of Things".

[4] Abhishek Patel, Prof. Ashok Verma,"A Review Paper on Data Security in CloudComputing",pp.9287-9295.

[5] Chintada. SrinivasaRao1 Chinta.ChandraSekhar2, "Dynamic Massive Data Storage SecurityChallenges in Cloud Computing Environments", Vol. 2, Issue 3, March 2014,pp.3609-3615.

[6] J.M.suri, DDG (I) TEC, B.K.NathDIR (I) TEC,"security and privacy in cloud computing".

[7] Minqi Zhou†, Rong Zhang§, Wei Xie†, WeiningQian†, Aoying Zhou," Security and Privacy in Cloud Computing: A Survey", pp.105-112.

[8] Satyakam Rahul1 and Sharda2,"Cloud Computing: Advantages and Security Challenges", ISSN 0974-2239 Volume 3, Number 8 (2013).

[9] Jan HenrikZiegeldorf, Oscar Garcia Morchon, and Klaus Wehrle, "Privacy in the Internet of Things:Threats and Challenges", Security and Communication Networks 7.12 (2014): 2728-2742.

[10] Glenn A.Fink, Dimitri v.Zarzhitsky,"security and privacy grand challenges for the internet of things", pp.27-33.

[11] Ivor D. Addo, Sheikh I. Ahamed, Stephen S. Yau, ArunBuduru "Reference Architectures for Privacy Preservation in Cloud-Based Iot Applications"Vol. 2, No. 4, Oct.-Dec. 2014pp.65-76

Author's Profile

Miss. Pallavi S. Rakhonde, pursuing B.E degree in Electronics and Telecommunication at Mauli College of Engineering and Technology, Shegaon .from SGBAU, Amravati. She is a member of The Institution of Electronics and Telecommunication Engineering (IETE).

Miss. Shubhangi N. Warkhede, pursuing B.E degree in Electronics and Telecommunication at Mauli College of Engineering and Technology, Shegaon .from SGBAU, Amravati. She is a member of The Institution of Electronics and Telecommunication Engineering (IETE).