International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

Multifactor Authentication in IoT devices for ensuring secure cloud storage in Smart Banking

[1] Monaswarnalakshmi S.R, [2] Sai Aravindhan. C. P

[1, 2] *Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, Tamil Nadu, India.*

Abstract: *Internet of things is an analytics system that allow users to achieve deeper automation, analysis, and integration within a system. It has the ability to process and learn from the data provided by the sensors in real world. The data collected by the sensors are stored in cloud for processing. Cloud systems are prone to security attacks and also have less amount of privacy, so that the IoT devices can be hacked by intruders. IOT security is the area that is considered for safeguarding the the devices connected in the network. The main problem is security is not considered while designing the devices and its lead to a serious of loss in data privacy.*

This problem is solved by improving the privacy of both IoT devices and Cloud. This is done with the help of Multi-factor authentication. User who is trying to connect to the IOT device should authenticate the device first and then only the connection to that device with a network is established successfully.

Apart from authentication the data is encrypted for gaining more security. The algorithm used to encrypt the data is AES/RSA algorithm. Thus providing more secured environment to the consumers. The Multi-factor authentication is the process of securing the data stored in the cloud by means of more than two security layer patches. The user can be able to access the data and the IOT device only after authenticating the security layers.

Keywords: IOT, Multi-factor Authentication, RSA, AES.

Abbreviation:

IoT-Internet of Things

RSA-Rivest Shamir Adleman

AES-Advanced Encryption Standard

1. INTRODUCTION

IoT concept can be explained by term 'device to device communication'. The device can sense, communicate and connect to other devices which is connected to internet by recognizing the physical address assigned to the devices and can also share information between them. IoT is a rapidly developing technology on which the future life will rely upon. IoT will become the most used technology in every field around 2025. So, there is a urgent need to provide security to IoT for securing the data in cloud.

The IoT refers to the use of intelligently connected device and systems to gather large amount of data. IoT is expected to spread rapidly over the upcoming years. The IoT has the potential to deliver solution that dramatically improve energy efficiency, security, health, education, and many other aspects of our daily life clearly the internet of things is one of the most important and powerful development. The key attribute that distinguish from regular way of using internet and IOT is by using the sense framework.

Imagine that all the devices are connected in internet and programmed to share information and data, which they can perform this process automatically to make our routine life in a different way, which we had only dreamt of it. This dream can be emerged as a new upcoming technology where there is a possibility of communication between electronic devices

The most commonly used frameworks for IOT is

- OCF- Open Connectivity Foundation.
- OMA- Open Mobile Alliance
- XSF- XMPP Standard Foundation.
- FDA- Food and Drug Administration
- GS1.
- Auto- ID labs.
- EPCglobal.

1.1 Features of IoT:

- Device to device communication.
- Real-Time data management.
- Access control.
- Tele health.
- Transportation management system.
- Traffic control system.
- Environmental monitoring and control.

1.2 Advantages of IoT:

- The work load of human is reduced.
- Automation process will be helpful so that the work to be done, can be finished automatically by the End devices.
- Less man power is needed.
- Smart manufacturing.
- Smart transportation.
- Smart city.
- Smart energy buildings.

2. LITERATURE REVIEW

2.1 Technology overview

The Internet of Things is an emerging technology in a day to day daily life by making all the works easier than it already was. Tracking towards the security of this technology is not that much developed when comparing it with the performance. Thus, the security is a great threat for most of the fields in which the IOT is underplayed.

As more and more IoT devices make their way into the world, deployed in uncontrolled and complex environments, securing IoT systems presents a number of unique challenges. The top 10 challenges for IOT security are

- Secure constrained devices
- Authorize and authenticate devices
- Manage device updates
- Secure communication
- Ensure data privacy and integrity
- Secure web, mobile, and cloud applications
- Ensure high availability
- Detect vulnerabilities and incidents
- Manage vulnerabilities
- Predict and preempt security issues

Considering on the Secure Constrained Devices, Many IoT devices have limited amounts of storage, memory, and processing capability and they often need to be able to operate on lower power, for example, when running on batteries. Security approaches that rely heavily on encryption are not a good fit for these constrained devices, because they are not capable of performing complex encryption and decryption quickly enough to be able to transmit data securely in real-time.

These devices are often vulnerable to side channel attacks, such as power analysis attacks, that can be used to reverse engineer these algorithms. Instead, constrained devices typically only employ fast, lightweight encryption algorithms.

Considering upon Authorize and authenticate devices, many devices offering potential points of failure within an IoT system, device authentication and authorization is critical for securing IoT systems.

Devices must establish their identity before they can access gateways and upstream services and apps. However, there are many IoT devices that fall down when it comes to device authentication, for example, by using weak basic password authentication, or using passwords unchanged from their default values.

Adopting an IoT Platform that provides security by default helps to resolve these issues, for example by enabling two factor authentication (2FA) and enforcing the use of strong passwords or certificates. IoT Platforms also provide device authorization services used to determine which services, apps, or resources that each device has access to throughout the system.

Considering on Managing the device Updates, including security patches, to firmware or software that runs on IoT devices and gateways presents a number of challenges. For example, you need to keep track of which updates are available apply updates consistently across distributed environments with heterogeneous devices that communicate through a range of different networking protocols. Not all devices support over-the-air updates, or updates without downtime, so devices might need to be physically accessed or temporarily pulled from production to apply updates. Also, updates might not be available for all devices, particularly older devices or those devices that are no longer supported by their manufacturer.

Device manager systems often support pushing out updates automatically to devices as well as managing rollbacks if the update process fails. They can also help to ensure that only legitimate updates are applied, for example through the use of digital signing.

In secure communication, Once the devices themselves are secured, the next IoT security challenge is to ensure that communication across the network between devices and cloud services or apps is secure.

Many IoT devices don't encrypt messages before sending them over the network. However, best practice is to use transport encryption, and to adopt standards like TLS. Using separate networks to isolate devices also helps with establishing secure, private communication, so that data transmitted remains confidential.

In data privacy and Integrity wherever the data ends up after it has been transmitted across the network, it is stored and processed securely. Implementing data privacy includes redacting or anonymizing sensitive data before it is stored or using data separation to decouple personally identifiable information from IoT data payloads. Data that is no longer required should be disposed of securely, and if data is stored, maintaining compliance with legal and regulatory frameworks is also an important challenge.

Ensuring data integrity, which may involve employing checksums or digital signatures to ensure data has not been modified. Block chain – as a decentralized distributed ledger for IoT data – offers a scalable and resilient approach for ensuring the integrity of IoT data.

In Securing the Application, the availability of IoT data and the web and mobile apps that rely on that data as well as our access to the physical things managed by IoT systems. The potential for disruption as a result of connectivity outages or device failures, or arising as a result of attacks like denial of service attacks, is more than just inconvenience. In some

applications, the impact of the lack of availability could mean loss of revenue, damage to equipment, or even loss of life. IoT infrastructure is responsible for essential services such as traffic control, and in healthcare, IoT devices include pacemakers and insulin pumps. To ensure high availability, IoT devices must be protected against cyber-attacks as well as physical tampering. IoT systems must include redundancy to eliminate single points of failure, and should also be designed to be resilient and fault tolerant, so that they can adapt and recover quickly when problems do arise.

Detecting Vulnerabilities and breaches include monitoring network communications and activity logs for anomalies, engaging in penetration testing and ethical hacking to expose vulnerabilities, and applying security intelligence and analytics to identify and notify when incidents occur.

Detected Vulnerabilities have to be managed and should take a respective action to manage its extent. Device managers maintain a register of devices, which can be used to temporarily disable or isolate affected devices until they can be patched. This feature is particularly important for key devices such as gateway devices in order to limit their potential to cause harm or disruption, for example, by flooding the system with fake data if they have been compromised. Actions can be applied automatically using a rules engine with rules based on vulnerability management policies.

A longer-term IoT security challenge is to apply security intelligence not only for detecting and mitigating issues as they occur, but also to predict and proactively protect against potential security threats. Threat modeling is one approach used to predict security issues. Other approaches include applying monitoring and analytics tools to correlate events and visualize unfolding threats in real-time, as well as applying AI to adaptively adjust security strategies applied based on the effectiveness of previous actions.

2.2 Overview of the Secured Smart Banking

The IoT is used in banking sectors for making all the banking process easier than any time before. But the main threat in consideration of banking is the security which is dealing from the very first. The security consideration on the data and user information about the account details can be safely stored in cloud and can also be connected to any IoT devices by implementing Multi-Factor Authentication and also by encrypting the data of all the bank users. Thus by doing so, will implement a high security patch and make the intruders impossible to patch the data and user information.

The user can trust the devices and can start transaction or can carry out any other bank function with less consideration on loss of privacy data by doing that.

This process will take a external server for storing all the Authentication details in a secure way and once on successful authentication the user can access the data or devices connected in the network.

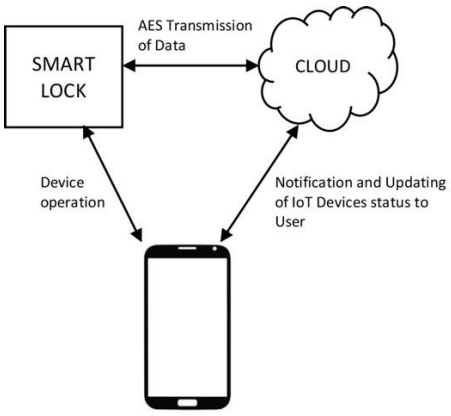

Fig - 1: Overview of secured smart banking

3. PROPOSED WORK

As illustrated above, the security in Smart Banking System is achieved by means of developing a mobile application. The functionality of the Application can be accessed only if the user authenticates all the security patch level. The data stored in the cloud will be encrypted so that if any intruders peep out of the authentication will also be made useless if the data is encrypted. This can be done with the help of AES algorithm. Firstly, the IoT devices can be accessed only after the clearance of the multi-factor authentication through mobile application. The various multi-factor includes – biometric, OTP, smart card, Strong passwords, etc. Then the user can access and operate the IoT devices safely without the intervention of the intruder.

Then the data from the devices are sent to the cloud for processing. The cloud is also prone to security and hence cloud servers and private cloud has to be secured.

Secondly, cloud servers are secured with 2 different biometric types for 2 persons at a time. As well as the private cloud can be secured with multi-factor authentication. The data that is sent for processing from IoT devices to the cloud can be transformed in a secured way with the help of AES algorithm. The AES algorithm uses has three rounds namely SubBytes, ShiftRows, Mix columns.

This project will be helpful in improving the regular banking transaction to smart and secured one. It aims to reduce the security breaches and thus providing a safe and secure banking experience to the people.

This implementation can be done with the help of mobile application for the accessing of the data from the IoT devices. This can be linked with cloud storage for knowing the current status of the data from the devices.

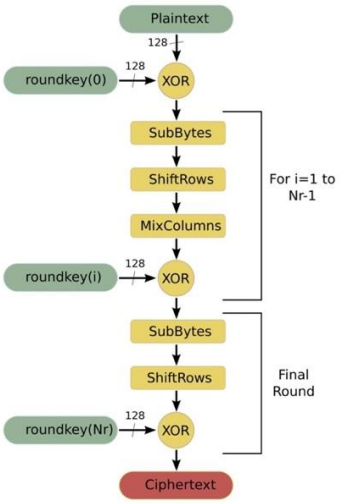

Fig - 2: AES flow diagram

3.1 Mobile app information

The mobile application can be opened only when the multi-factor authentication is successful and thus having access to the IoT devices and also the cloud. Password for the app should be entered, if the password is correct, an OTP password will be sent to the registered mobile number.

Fig - 3: First step in authentication

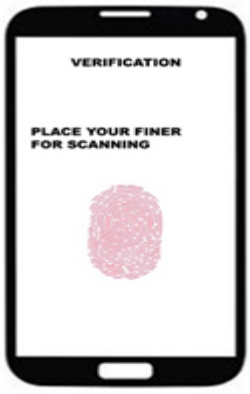

Fig - 4: Second step in authentication

The user has to enter the correct and recent OTP. The OTP generation can be done using the Transactional sms in which there is no need for the entered number to be activated DND. (Do Not Disturb) Then the next step of authentication is the biometric level, i.e. with the help of fingerprint. This can be developed by creating the instance for the Fingerprint Manager class and call the authenticate() method.

Fig - 5: Third step in authentication

Most of the device not supported in fingerprint sensor and this works on phones with the API level above 23. Once the biometric is completed then the end of multifactor authentication. This improves the security to a vast extent and difficult for the intruder to gain access to the important data.

3.2 Advantages

- By using this application, the hackers who seek for the privacy data of others can be stopped.
- The decryption will be not a easy process unless the private key is available.
- The data will be securely accessed only by successful authentication of multi-factor process.

4. Conclusion

This system will be useful in safeguarding the bank account details and the transaction details of a user from many intruders in the network. This system will also take the security level of IoT devices to a next level, that by making the security of the devices stronger than before and giving consideration to IoT devices to be manufactured with security updates for many future purposes.

5. References:

[1] Rohan H.Shah, D.P.Salapurkar,"A Multifactor authentication system using secret splitting in the perspective of Cloud of Things",IEEE International conference on Emerging Trends & Innovation in ICT,2017.

[2] Prachi Garg, Sandeep Goel, Avinash Sharma, "Security techniques for cloud computing environment", IEEE conference on computing, communication and automation,2017.

[3] N.Venkatesh, M.Rathan Kumar, "Fingerprint authentication for improved cloud security", IEEE international conference on computing system and information technology for sustainable solutions,2016.

[4]N.Jayapandian, A.M.J.Md.Zubair Rahman, S.Radhikadevi, M.Koushikaa,"Enhanced cloud security framework to confirm data security on asymmetric and symmetric key encryption", IEEE world conference on Futuristic Trends in Research and Innovation for Social welfare,2016.

[5] Xin Pei, Yongjian Wang, Wei Yao, Jiuchuan Lin, Ruxiang Peng, "Security Enhanced Attribute Based Signcryption for Private Data Sharing in Cloud", IEEE Trustcom/BigDataSE/ISPA,2016.

[6] Dimitris Schinianakis, "Alternative Security Options in 5G and IoT Era",IEEE circuits and system Magazine,2017.

[7] Elias Tabane, Tranos Zuva, "Is there a room for security and privacy in IoT?", IEEE International conference on Advances in Computing and Communications Engineering(ICACCE),2016.

[8] Kan-Siew-Leong, Paul Loh Ruen Chze, Ang Khoon Wee, Elizabeth Sim, Kan Ee May,"A multi-factors security key generation mechanisms for IoT",IEEE 9th International Conference on Ubiquitous and Future Networks(ICUFN),2017.

[9] Ritambhara, Alka Gupta, Manjit Jaiswal,"An enhanced AES algorithm using cascading method on 400 bits key size used in enhancing the safety of next generation internert ofthings(IOT)",IEEE International Conference on Computing,Communication and Automation(ICCCA),2017.

[10] Afsoon Yousefi, Seyed Mahdi Jameii,"Improving the security of internet of things using encryption algorithms",IEEE International Conference on IoT and Application(ICIOT),2017.

[11] rafiullah khan,sarmad ulla khan,rifaqat zaheer,shahid khan,"future internet: the internet of things architecture, possible applications and key challenges".