IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SESSION-BASED INFORMATION SECURITY FOR IOT DEVICES USING CRYPTOGRAPHIC LEDGER

[1] Chandrappa S, [2] Darshitha K S, [3] Neha S P, [4] Spandana M, [5] Spoorthi M

[1]Assistant professor [2,3,4,5]Student

Department of Information Science and Engineering

[1,2,3,4,5]GSSS Institute of Engineering and Technology for Women, Karnataka, India.

Abstract: Internet of things (IoT) is a network that consisting of billions of devices, which provides an opportunity to an intruder to manipulate the IoT system on a large scale. It can be described as, the connection of things or devices across the internet to deliver upon an assigned function. This mainly comes in the form of devices sending or receiving data. At the hardware layer, an attacker gets access to the IoT hardware and retrieves the keys or security parameters stored inside the IoT device. The attacker can recreate a duplicate or virtual IoT device using the stolen security parameters. The duplicate IoT device can upload false data to the server and retrieve secure information about the user from the server or the network to which the IoT device is connected. The aim of this project is to provide a two-level and session-based secure data communication. To provide a secure data communication between IOT devices and cloud and between different IOT devices by creating permission based block chain and hashing the data which is being shared by different IOT devices. In this application we propose a novel cryptographic ledger based framework for IoT device data sharing and communication and planning to implement the prototype of our proposed framework using Hyper ledger Fabric and evaluate its performance.

Index Terms **– IoT, Security parameters, keys, secure information, block chain, hashing.**

I. INTRODUCTION

This project contains the design and implementation of security protocol for IoT systems. The user will send a registration request to the authority node. If the sent request is valid, the authority node will approve the request by generating a digital certificate and multiple keys. The certificate is stored in the cloud database. The user will check the status and be allowed to download the certificate and keys. After registration, the user will send a control request to the authority node. The authority node checks the sent certificate with the stored certificate, if both matches admin will grant permission to the user for accessing the IoT system.

A. INTERNET OF THINGS(IOT)

The Internet of Things is a system of interrelated computing devices, mechanical and digital machines, objects, animals, or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human to human or human to computer interaction. The Internet of Things is the network of physical objects or things embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.

The IoT allows the object to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into a computer-based system and resulting in improved efficiency accuracy, and economic benefit in addition to reduced human intervention. When IoT is augmented with sensors and actuators, the technology became an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation, and smart cities.

IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS), microservices, and the internet. The convergence has helped tear down the silo walls between operational technologies (OT) and information technology (IT), allowing unstructured machine-generated data to be analyzed for insight that will drive improvements. Practical application of IOT technology can be found in many industries today including precision agriculture, building management, healthcare, energy, and transportation.

B. CLOUD AND RASPBERRY PI

Cloud Storage is a backend as a service which provides seamless scalability and it removes the necessity of operating database which are distributed in nature. It is a fast and fully managed service. The key feature of the server is that it can store a large amount of data centrally and also it can provide access to restricted users via the internet across different geographical regions just by connecting into the same region.
The Raspberry Pi is a series of credit card-sized single-board computers developed by the Raspberry Pi Foundation. A private cloud server can be set up in a Raspberry Pi which could be used as a storage device for applications involving real-time signals. Raspberry Pi is a cheaper microprocessor in which cloud computing infrastructure can be obtained using cloud platforms.

II. LITERATURE REVIEW

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit the use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper Do not number text heads—the template will do that for you. Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar returns of the shares and estimated betas. [1] Chun Chen described distributed access control module is wireless sensor networks allows the network to authorize and allow the user access the benefits for in-network data access. In early research we mainly focuses on designing such access control modules for WSNs, but little attention to protect user's identity privacy when a user is verified by the network for accessing data. Usually a user does not want the WSN to associate his identity to request the data. In this paper, we concentrate about the design, implementation, and also we use novel approach for evaluation process, that ensure distributed privacy-preserving access control. users who have same access they get benefits are organized into the same group network owner. The user signs a query command on behalf of his group and then he able sends the signed query to the sensor node interest. The signature will be verified by its recipient as coming from someone authorized without disclosing the actual user. For theoretical analysis we adding the security properties, and distributed privacy- preserving access control in sensor networks. Token based approach in single owner multiple user sensor networks is used to preserve user's privacy with central token issuing authority. The work focused on issue with token-reusability. [2] Namhi Kang describes framework for authentication of data in IOT. Data are taken as streams with security punctuations, which get examin before the data are provided to its user. It does not give brief description about the security rules therefore MAC,apply for such solution. Nevertheless, we set some restriction to the user only not creator, which is sometime unsuitable in many applications when the sensor is just a slave of another hierarchically, a higher entity. It does not address problem of security rules duplication and consistency across different devices. key distribution system can withstand replay attacks, man-in-the-middle attacks,[3] In this paper, the author explained the use capability of tokens for granting access to services. The token is issued by the provider for a client during the initial provision of a service. It consists of URL, user/object ID, timestamp of creation, subscription period, service ID, and list of access permissions. A Secured Certificate-based authentication is not required to generate passwords or tokens, instead of that digital certificates are used to solve authentication challenges nowadays. In this paper, we are discussing the design and implementation of security protocol for the IoT and also Admin can generate a digital certificate and many keys for a valid user using SHA. The certificate and keys are downloaded by the user. The user also communicates with the admin through the digital certificate for the secured authentication of IoT. [4] the authors explained about The IoT system, which makes us suffer from a lack of reliability, security, and privacy. In this project, we have implemented the security protocol using SHA. The protocol not only covers the integrity of messages but also the authentication of each user by providing an efficient authentication mechanism for the IoT environment. here we try to resolve authorization requests for constraint devices when the user wants to access any of the device's data or services. The authorization engine is exposed through API and therefore most of the IoT devices can access it. The proposed method is a very complex framework built on top of the existing technologies. However, they deal with user device security this work does not address machine-to-machine trust.

III. METHODOLOGY

The project concentrates on the design of a Security Protocol for the IoT and the implementation of the corresponding Security Protocol on the Sensible Things Platform. The Security Protocols will not only cover the integrity of the message but also the authentication of each user by providing an efficient authentication mechanism. The functioning laboratory Prototype of the Secured Communication implemented on the Sensible Things Platform is introduced. The Sensible Things platform is an open-source platform for creating efficient and fast internet things applications. It is a common platform for communications between sensors and actuators on a Global Scale and enables a widespread Proliferation of IoT Services. This secure communication provides more efficient information for transmission mechanisms.

The Security Protocol involves:

- Registration process
- Approval process
- Certificate Generation
- Certificate Sharing
- Request to control
- Control to access

Registration Request Process: The Registration Request Process is carried out between the recently joined User and Authority Node (AN). Then the Registration Request Process is carried out between User and Admin. The user will send a request to admin, which consists of user information such as, Username, Mac ID, IP address, Machine name, Date, and Time will be auto fetched and filled into the registration form and the request is sent to admin.

Approval Process: During this process, the registration request details are stored in a cloud database and this request will be made to wait for Admin approval. The admin will take up the request from the cloud database, if it is a valid request, then the admin will approve the request otherwise the request is deleted by the admin.

Certificate Generation and Sharing: The admin will take up the combination of user information such as username, Mac ID, IP address, machine name and is given to SHA. This algorithm generates a ciphertext and is used to generate a digital certificate. The private and public keys will be generated by RSA.

The user will be provided with an option of checking his approval status. If the request is approved by the admin, he can then download the certificate and a private key from the cloud database.

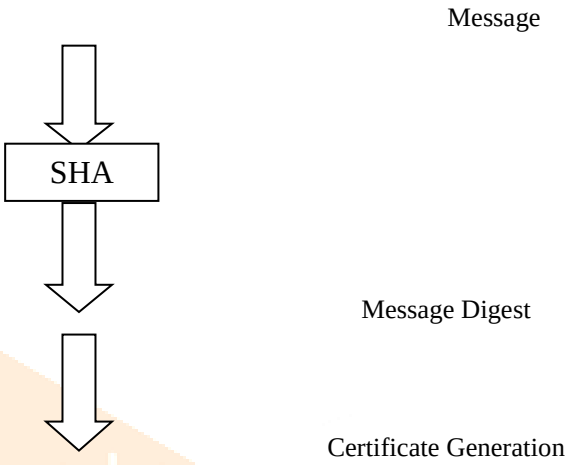

Figure 1: Generation of Certificate using SHA

Request to control: The user will then send a request to the admin along with the certificate. The cloud server will compare both the sent certificate with the stored certificate to verify whether the request is from the same user or not. If both certificate matches, it will then generate OTP, encrypted by the public key and is sent to the user. The user will then decrypt this token by a private key and he will send the OTP. If both OTP is the same, then the admin will generate a session key and it is given to the user.

Control to Access: The user will then send a request and session key to the IoT system. As long as the session key exists, the user can control the IoT. Once the session key expires, then he has to send a request again.

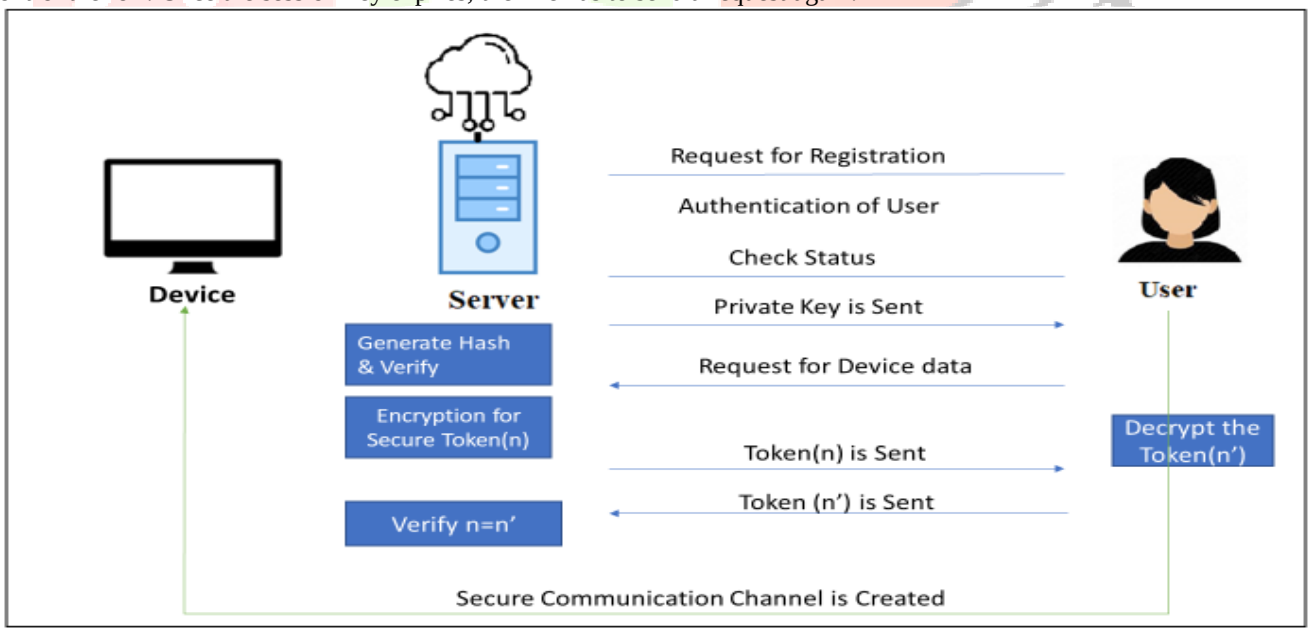

Figure 2: System Architecture

PROPOSED SYSTEM

As authentication between the IoT devices and IoT servers are mutually authenticated the essential part of the secure IoT systems will be IoT devices and the servers. In this project, we will be providing a security protocol for the embedded systems or the platforms which will serve for Internet of Things. And also, to encourage the development of the Internet of Things. The main purpose of our project is to develop a system that will not only verify the integrity of the messages but also by providing an efficient authentication mechanism.

In our project, as we will be using the multi-key authentication mechanism, even if the secret key used for ongoing authentication is recovered successfully by the attacker, the attacker will not get access to the unutilized authentication keys, and thereby the authentication system is secure from different kinds of attack The value of keys keeps changing over time as it provides session-based communication, which can prevent dictionary attack. As the Server will authenticate the user and creates a hash using User's Credentials which uses the Hashing Algorithm – Adler 32 as it trades reliability for speed and faster on many platforms.

ALGORITHM

Operation on Words

The following logical operators will be applied to words:
a. Bitwise logical word operations
X ∧ Y = bitwise logical "and" of X and Y.
X ∨ Y = bitwise logical "inclusive-or" of X and Y.
X XOR Y = bitwise logical "exclusive-or" of X and Y.
~X = bitwise logical "complement" of X.
Example:
01101100101110011101001001111011XOR01100101110000010110100110110111 ----------=
00001001011110001011101111001100

b. The operation X + Y is defined as follows: words X and Y represent integers x and y, where $0 \leq x<2\ 32$ and $0 \leq y<2\ 32$. For positive integers n and m, let n mod m be the remainder upon dividing n by m. Compute
$z = (x + y) \bmod 2\ 32$.
Then $0 \leq z<2\ 32$. Convert z to a word, Z, and define Z = X + Y.
c. The circular left shift operation Sn(X), where X is a word and n are an integer with
$0 \leq n < 32$, is defined by
Sn(X) = (X << n) ∨ (X >> 32-n).
In the above, X << n is obtained as follows: discard the left-most n bits of X and then pad the result with n zeroes on the right (the result will still be 32 bits). X >> n is obtained by discarding the right-most n bits of X and then padding the result with n zeroes on the left. Thus Sn(X) is equivalent to a circular shift of X by n positions to the left.

CONCLUSION AND FUTURE SCOPE

We will be providing a security protocol for Secured authentication of IoT environment which will result in high security, high efficiency ,low cost, simple and session based information security for Iot devices using cryptographic ledger. Implementing a prototype of our proposed framework using Hyperledger Fabric, and analyze the security offered by our proposed framework.

REFERENCES

[1] "Iot market size worldwide 2017-2025," [Accessed: Feb, 2020]. [Online]. Available: https://www.statista.com/statistics/976313/globaliot-market-size
[2] B. Nassi, M. Sror, I. Lavi, Y. Meidan, A. Shabtai, and Y. Elovici, "Piping botnet-turning green technology into a water disaster," arXiv preprint arXiv:1808.02131, 2018.
[3] M. G. Angle, S. Madnick, J. L. Kirtley, and S. Khan, "Identifying and anticipating cyberattacks that could cause physical damage to industrial control systems," IEEE Power and Energy Technology Systems Journal, vol. 6, no. 4, pp. 172–182, 2019.
[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [6] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 6–14, 2018.
[5] K. Fan, Y. Ren, Z. Yan, S. Wang, H. Li, and Y. Yang, "Secure time synchronization scheme in IoT based on blockchain," in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018, pp. 1063–1068.
[6] D. Merkel, "Docker: lightweight Linux containers for consistent development and deployment," Linux Journal, vol. 2014, no. 239, p. 2, 2014.
[7]. Sencun Zhu and Sammy Chan, "Distributed Access Control with Privacy Support in Wireless Sensor Networks", on 10 Oct 2011 Vol.10, No.10, in IEEE Transactions on Wireless Communication.
[8]. Pranatha," A Distributed Secure Mechanism for Resource Protection in a Digital Echo System Environment", in 2012 Vol.3, No.1, Journal of Information Security.
[9]. Seitz, "Authorization Engine as Trusted Third Party", on 29 Dec 2015 IEEE International Conference on Internet Of Things.
[10]. Namje Park and Namhi Kang, "Mutual Authentication Scheme in Secure Internet Of Things Technology for Comfortable Lifestyle", on 25 Dec 2015.
[11]. Karim lounis and Mohammad zulkernine " Attacks and Defenses in Short-Range Wireless Technologies for IoT " on May 11, 2020, IEEE, vol 8, 2020

[12]. Elias Bou-Harb, Nataliia Neshenko, "Cyber Threat Intelligence for the Internet of Things" February 2020 DOI:10.1007/978-3-030-45858-4 Publisher: Springer ISBN: 978-3-030-45857-7.
[13]. Elie Kfoury, David Khoury "Distributed Public Key Infrastructure and PSK Exchange Based on Blockchain Technology" in 2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybernetics.
[14].Sayeed Z.sajal, Israt Jahan, Kendall E.Nygard, "A Survey on Cyber Security Threats and Challenges in Modem Society",2019 Institute of Electrical and Electronics Engineers(IEEE).
[15]. Jorge Martınez Carracedo, Michael Milliken, Pushpinder Kaur Chouhan, Bryan Scotney, Zhiwei Lin, Ali Sajjad "Cryptography for Security in IoT " in 2018 Fifth International Conference on Internet of Things: Systems, Management and Security (IoTSMS) and Mark Shackleton2