# Secure And Light Weight Two-Factor Authentication For IoT Home Automation

**S.Maabuni[1], K.Venkataamana[2]**

[1] Dept of Computer Science And Engineering
[2] Associate Professor, Dept of Computer Science And Engineering
[1, 2] Seshachala Institute Of Technology, Puttur, A.P, India

***Abstract-*** *Device authentication is an essential security feature for Internet of Things (IoT). Many IoT devices are deployed in the open and public places, which makes them vulnerable to physical and cloning attacks. Therefore, any authentication protocol designed for IoT devices should be robust even in cases when an IoT device is captured by an adversary. Moreover, many of the IoT devices have limited storage and computational capabilities. Hence, it is desirable that the security solutions for IoT devices should be computationally efficient. To address all these requirements, in this article, we present a light weight and privacy-preserving two-factor authentication scheme for IoTdevices, where physically uncloneable functions (PUFs) have been considered as one of the authentication factors. Security and performance analysis show that our proposed scheme is not only robust against several attacks, but also very efficient in terms of computational efficiently.*

***Keywords***- Mutual authentication, Privacy-Preserving, Physically uncloneable functions, Fuzzy extractor, IoT device.

## I. INTRODUCTION

### 1.1 DOMAIN DESCRIPTION

Kevin A, co-founder of the Auto-ID Center at Massachusetts Institute of Technology, first mentioned the internet of things during a presentation he made to Procter & Gamble (P&G) in1999. The need to bring radio frequency ID (RFID) to the attention of P&G's senior management, Kevin called his presentation "Internet of Things" to include the cool new trend of 1999: The Internet. Massachusetts Institute of Technology professor Neil Gershenfeld's book, When Things Start to Think, also appearing in 1999, did not use the exact phrase but referenced a clear vision of where IoT was headed.

IoT is abbreviation form of Internet of Things, that refers to the exponentially-growing network of physically connected devices that feature an IPv4 or IPv6 address for internet connectivity, and also the inter-communication between the connected devices that occurs between these real world objects and the other internet-enabled devices and sub-systems.

IoT has evolved from the merger of two technologies, wireless and micro electromechanical systems (MEMS), micro services and the web. The merging has helped tear down the silos between operational technology (OT) and information technology (IT), enabling amorphous machine-generated data to be analyzed for understandings to drive improvements. Although Ashton's was one of the first reference of the Internet of Things, the primary idea of connected devices was predominantly existent around since the seventies, referenced by the names embedded internet and *pervasive computing*.

The first internet connected device, for example, was a Coke vending machine at CMU in the early eighties. The device was connected to the internet, the developerscan check the status of the vending machine and assess whether there would be a soda awaiting them, they will decide to pick the soda from the vending machine.

IoT evolved from inter-communication of machine-to-machine (M2M), i.e., machines connecting the other devicesover a network. M2M refers to connecting a device to the network, managing the device and collecting analytics data from the device.The next attempt of taking M2M communication to the next level, IoT is a sensor network with billions of smart connected devices that are connected to people, systems and other applications/appliances to collect the data and exchange the data.

As defined in the foundation, M2M extends the network connectivity that empowers IoT.

The Internet of Things is also a natural addition of SCADA (supervisory control and data acquisition), a branch of software application for process control, the collection of data in real world devices which were deployed in isolated locations to control operation of other devices. SCADA systems include physical and software components. The physical devices collect and shifts the data into a device that has SCADA software installed, the data is then processed and exported to the destination set by the users in a appropriate manner.

The growth of SCADA is such that last-generation SCADA products were reference as the first-generation IoT products. The Internet of Things (IoT) outspreads internet connectivity beyond personal devices to a wide range of devices/appliances and routine things that make use of technology to communicate, transfer/exchange data between these devices and intermingle with the external environment, all via the Internet.

The devices connectivity, networking and the device communication protocols used with-in the IoT devices largely depend on the specific IoT applications deployed.

## II. LITERATURE SURVEY

Literature survey is the predominant step in utility progress technique. Prior than setting up the appliance it may be quintessential to evaluate the time part, fiscal process n corporation stress. As speedily as these problems r satisfied, ten subsequent steps are to determine which working method and language may even be utilized for starting the application. As rapidly seeing that the programmers opening the instrument the programmers need lot of outside support. This help can also be bought from senior programmers, from e-e-e-newsletter or from web pages. Prior than starting the approach the above consideration are seen for opening the proposed system.

### PRISM: excessive-satisfactory-Grained worthy priceless useful resource-conscious Scheduling for Map Reduce

Map Reduce has turn out to be a preferred model for working out-intensive computation in as much as the second years. By way of breaking down every job into small map and shrink duties and executing them in parallel in the path of a big wide variety of machines, Map Reduce can enormously cut back the going for walks time of understanding-intensive jobs. Nevertheless, despite trendy efforts toward designing beneficial useful resource-effective Map Reduce schedulers, present options that target scheduling on the manufacturer-stage however reward sub-satisfactory job effectively. That is because responsibilities can have surely various worthwhile resource specifications within the path of their lifetime, which makes it complex for enterprise-stage schedulers to quite simply make use of to be had property to minimize job execution time. To manipulate this obstacle, we introduce PRISM, a excessive-adequate-grained resource-aware Map Reduce scheduler that divides obligations into phases, the situation each part has a consistent useful priceless useful useful resource utilization profile, and performs scheduling on the segment stage. We first divulge the value of section-measure scheduling via exhibiting the useful priceless useful useful resource utilization variability inside the lifetime of a manufacturer utilizing a tremendous-sort of Map Reduce jobs. We then reward a section-stage scheduling algorithm that improves execution parallelism and useful resource utilization without introducing stragglers. In a ten-node Hadoop cluster going for walks normal benchmarks, PRISM presents excessive necessary useful resource utilization and presents 1.3 progress in job going for walks time compared to the reward Hadoop schedulers.

### Adaptive Workflow Scheduling on IoT with Iterative Ordinal Optimization

The scheduling of multitask jobs on clouds is an NP-hard challenge. The obstacle turns into even worse when troublesome workflows are finished on elastic clouds, paying homage to Amazon EC2 or IBM RC2. The foremost main trouble lies inside the large search subject and excessive overhead of producing satisfactory satisfactory schedules, customarily for unique-time capabilities with dynamic workloads. On this work, a company new iterative ordinal optimization (IOO) process is proposed. The ordinal optimization method is applied in each new free up to gather sub-predominant schedules. IOO ambitions at producing further effective schedules from a worldwide standpoint over a power interval. We show off by way of overhead evaluation the advantages in time and field effectively in making use of the IOO procedure. The IOO system is designed to adapt to technique dynamism to yield suboptimal effectively. In cloud experiments on IBM RC2 cloud, we execute 20,000 obligations in LIGO (Laser Interferometer Gravitational-wave Observatory) verification workflow on 128 digital machines. The IOO time table is generated in decrease than 1,000 seconds, even as making use of the Monte Carlo simulation takes 27.6 hours, one hundred activities longer to yield an main agenda. The IOO-optimized agenda results in a throughput of 1,one hundred obligations/sec with 7 GB memory demand, in comparison with 60 percentage cut back in throughput and 70 percent improve in reminiscence demand in utilizing the Monte Carlo method. Our LIGO experimental effect naturally showcase the talents of utilizing the IOO-headquartered workflow scheduling over the common blind-choose, ordinal optimization, or Monte Carlo approaches. These numerical outcomes are furthermore validated with the help of the theoretical complexity and overhead analysis furnished.

### Slick Flow: Resilient supply routing in capabilities center Networks unlocked through making use of making use of Open Flow

Up-to-the-minute proposals on abilities middle Networks (DCN) are based on centralized manipulate and a logical local material following a first-class-managed baseline topology. The architectural injury up of manipulate and capabilities planes and the organization new manipulate aircraft abstractions had been touted as application-outlined Networking (SDN), the vicinity the Open Flow protocol is one ordinary alternative for the standardized programmatic interface to working out airplane objects. On this context, give routing has been proposed so that you could furnish scalability, forwarding flexibility and ease throughout the information plane. One main caveat of source routing is regional failure hobbies, which require informing the furnish node and would take at the least on the order of 1 RTT to the controller. This paper offers Slick Flow, a resilient furnish routing method applied with Open Flow that makes it practicable for rapid failure treatment by means of combining source routing with substitute route working out carried within the packet header. Major and alternative paths are compactly encoded as a chain of segments written in packet header fields. Underneath the presence of disasters alongside a foremost route, packets may also be rerouted to replacement paths via the switches themselves without a involving the controller. We analysis Slick Flow on a prototype implementation headquartered on Open vSwitch and exhibit its effectiveness in a Mininet emulated challenge for fats-tree, BCube, and DCell topologies.

**Open Flow headquartered manipulate for re-routing with differentiated flows in knowledge core Networks**

Knowledge middle Networks need densely interconnected topologies to furnish immoderate bandwidth for particularly a lot of cloud computing picks. It's required to completely make use of the bandwidth useful resource in this form of staff with various site visitors patterns. We advocate a waft-centered phase-to-phase rerouting scheme for the expertise core Networks which has the mixture of massive flows and transient flows. We center of attention on rerouting the big flows to replacement paths within the party of congestion when you consider that small flows are temporary-lived and relocating them between paths will beef up their latency and overhead. The proposed scheme has a couple of principal factors: 1) It presents adaptive re-routing of flows to fairly simply unfold the burden in retaining with the altering load stipulations. 2) It ensures mighty website on-line viewers redistribution upon hyperlink disasters. We develop a prototype and expose the effectiveness of the proposed mechanism on Open Flow scan mattress.

**Open Router: Open Flow extension and implementation centered on a commercial router**

By way of inspecting challenges of present Open Flow in building crew, we advocate three extensions of Open Flow about Flow Table, manipulate mode and Open Flow protocol. Established on these extensions, a industrial Open Flow-enabled router, named Open Router, is designed and utilized using simplest available and current hardware in a trade router. Open Router brings the capabilities of manipulate openness, integration of within/external protocols, and flexibility of Open Flow message structure, low-priced implementation and deployment. We rely on Open Router would percentage up the giant-scale utility and deployment of Open Flow in progress community.

**Ideas-established scheduling for load-balanced two-stage switches**

A framework for designing suggestions-headquartered scheduling algorithms is proposed for elegantly fixing the notorious packet mis-sequencing obstacle of a load-balanced trade. Not like reward methods, we exhibit that the efforts made in load balancing and keeping packets in order can complement every distinct. More often than not, at every core-stage port between the 2 swap substances of a load-balanced swap, most strong a single-packet buffer for every digital output queuing (VOQ) is required. Nevertheless, that packets belonging to the same go with the flow cross through character core-stage VOQs, the delays they advantage at special center-stage ports can be identical. That is made believable by means of making use of making use of safely identifying and coordinating the 2 sequences of swap configurations to kind a joint sequence with each staggered symmetry property and in-order packet furnish property. Headquartered on the staggered symmetry property, an effective feedback mechanism is designed to permit the correct core-stage port occupancy vector to be dropped on the correct enter port on the right time. Accordingly, the affectivity of load balancing as satisfactory due to the fact that the truth that the alternate throughput is extensively increased. We further extend this ideas mechanism to aid the multicabinet implementation of a load-balanced alternate; the challenge the propagation lengthens between alternate line cards and alter substances is no negligible. As compared to the gift load-balanced alternate architectures and scheduling algorithms, our options impose a modest requirement on swap hardware; however consistently yield bigger extend-throughput efficiency. Best then again now not least, some extensions and refinements are made to maintain the scalability, implementation, and fairness disorders of our picks.

## III. SYSTEM ANALYSIS

### 1.2 EXISTING SYSTEM:

Within the Open drift framework, specified capabilities forwarding add-ons and route setup add-ons are individually deployed on switches and controllers. The controllers evaluate capabilities forwarding strategies. The Open waft protocols be designated communications between switches and controllers. Reward Open waft situated scheduling schemes, nevertheless, statically established routes most amazing on the initialization stage of skills transmissions, which suffers from dynamical waft distribution and altering crew states in potential facilities and most in most cases outcomes in unsafe procedure affectivity.

### 1.2.1 Disadvantages of Existing System

- It does not help authentication ofBIoT devices over a couple of paths.
- Statically designed authentication mechanism during the initialization stage.

### 1.3 PROPOSED SYSTEM

In this paper, we recommend a novel Dynamical Authentication (DA) approach for maximizing the nearby throughput while balancing authentication dynamically. We to with formulate the DA predicament, after which raise a gaggle of strong heuristic scheduling algorithms for the two typical Open flow employees objects, FPN and FTN, we proposed and applied a collection of mighty scheduling algorithms DLBSFPN and DLBS-FTN respectively which steadiness capabilities flows time slot with the support of time slot An Open go with the flow community most likely involves multi-layer IoT devices, multi-layer waft Visors and Controllers the Open waft switches very almost ahead advantage packets; waft Visors virtualized areas of the switches; and controllers installed capabilities forwarding ideas and manipulate the regional.

### 1.3.1 Advantages of Proposed System

- Balances regional IoT devices with a fewer connections
- At the start, our algorithms can adapt to dynamical personnel states and altering viewers requisites by way of updating load imbalance side$\delta(t)$ and as a result balancing the transmission load slot with the support of utilizing slot for the period of potential transmissions
- Our algorithms can globally steadiness transmission viewers inside the whole regional through evaluating hyperlink, route and personnel bandwidth utilization ratio proposed

### SYSTEM REQUIREMENTS

### 1.3.2 Hardware Requirements

| | | |
|---|---|---|
| Processor | - | Mobile based processors |
| RAM | - | 1GB (min) |
| Hard Disk | - | 8 GB |
| Key Board | - | Standard Windows Keyboard (optional) |
| Mouse | - | Two or Three Button Mouse (optional) |
| Monitor | - | SVGA (optional) |

### 1.3.2 Software Requirements

| | | |
|---|---|---|
| Operating System | : | Any Linux flavours |
| Application Server | : | Tomcat5.0/6.X |
| Front End | : | AngularJS and React JS |
| Scripts | : | JavaScript. |
| Server side Script | : | Not Applicable. |
| Database | : | In Memory DB |
| Database Connectivity | : | Not Applicable |

## IV. CONCLUSION

We submitted a different privacy-preserving 2 factor authentication mechanism for IoT devices, which allowsan IoT device to anonymously communicate with the Gateway or peer devices placed at the remote locations. We demonstrated that the suggested system stays secure even if an ethical hacker has direct access to an IoT device. The suggested authentication protocol offers the required security characteristics effectively by utilizing the fundamental security features of PUFs. Hence, we argue that the suggested scheme is be a feasible and encouraging solution for the security of IoT devices.

## FEASIBILITY STUDY

The feasibility of the project is investigated in this phase and business proposal is put in place with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the future system is to be carried out. This will ensure that the new system will not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

### ECONOMICAL FEASIBILITY

This study is performed to check if the proposed systems can be completed with the budget set for the project by the organization. The amount of budget that the company can spend into the R&D of the system is restricted. The costs incurred during the development of the product should be justified to the finance teams. Thus, the proposed system must be within the planned cost and for this reason most of the organization are inclined towards using the open source technologies. Only the customized products had to be purchased. employed to train the user about the system, which include proper documentation and the user guides. The user confidence level must be raised by listening to the customer for his feedback on the proposed system, which is.

## V. FUTURE ENHANCEMENTS

A new Proof of Retrievability scheme with two IoT devices. Exceptionally, one device is for auditing and the opposite for storage of knowledge. The IoT Gateway is just not required to have high storage potential. Specific from the prior work with auditing server and storage server, the user is relieved from the computation of the tags for documents, which is moved and outsourced to the cloud Gateway audit server. Moreover, the IoT Gateway additionally performs the position of auditing for the files remotely saved in the IoT Edge devices. We enhance a bolstered safety mannequin by because the reset attack towards the IoT Edge device in the upload segment of an integrity verification scheme. It's the first Proof of Retrievability model that takes reset assault into account for Authentication method. We gift an effective verification scheme for making sure far flung user Authentication in IoT Edge devices. The proposed scheme is proved secure in opposition to reset assaults within the bolstered protection mannequin even as supporting effective public verifiability and dynamic information operations at the same time.

## REFERENCES

[1] P. S. Ravikanth, Physical One-Way Functions, Ph.D. thesis, Mas- sachusetts Institute of Technology, 2001.

[2] G. Suh, S. Devadas, Physical unclonable functions for device authen- tication and secret key generation, in: Design Automation Conference, DAC ’07, 44th ACM/IEEE, 2007, pp. 9–14.

[3] V. Shivraj, M. Rajan, M. Singh and P. Balamuralidhar,“Onetimepasswordauthentication scheme based on elliptic curves for Internet of Things (IoT),” Proceedings of NSITNSW, pp. 1-6, Riyadh, KSA, February 2015.

[4] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, “Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications,” Proceedings of IEEE WCNC, pp. 2728-2733, Istanbul, Turkey, April 2014.

[5] Y. Kim, S. Yoo, and C. Yoo, “DAoT: Dynamic and Energy-aware Authentication for Smart Home Appliances in Internet of Things,” Proceedings of IEEE ICCE, pp.196-197, Las Vegas, NV, Jan 2015.