(IJIASE) 2017, Vol. No. 3, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

DEVELOPING AN AUTHENTIC BASED INTERNET OF THINGS (IOT) ENABLED SMART MOBILE DEVICE FOR SWIFT OPERATIONS

SARTHAK GARKHEL

ABSTRACT

Internet of Things (IoT) has rolled out huge improvements in reality and enters all parts of human life. The client acknowledgment of IoT is colossally high and it is far-reaching use is a result of the accessibility of advanced mobile phones and tablets. Wide reception of IoT in the utilizations of each field continually gathering touchy data and give a bigger surface to interlopers. So protection saved validation and access controls are huge difficulties in its exploration region. Techniques/Statistical Analysis: In this paper, we presented a novel calculation dependent on Zero-Knowledge Protocol and Accumulated Hashing to give secure validation to sensor empowered cell phones in IoT. Additionally, for guaranteeing classification in correspondence proposed another strategy for key trade utilizing current time. Discoveries: The proposed strategy satisfies the prerequisites of asset and battery obliged cell phones in IoT when contrasted and conventional validation and access control instruments for different applications.

1. INTRODUCTION

IoT a reality over the Internet in which things including people, objects, information and places to be connected through wireless or wired network at any time, at anyplace. With this new revolution, Internet is expanded from communication devices to the enterprise assets and consumer goods. IoT creates an intelligent environment and unique addressing is implemented to enablecommunication1. So every object connected can be tracked. Each participant autonomously interacting and communicating via internet and no centralized authority is there to control the objects2.

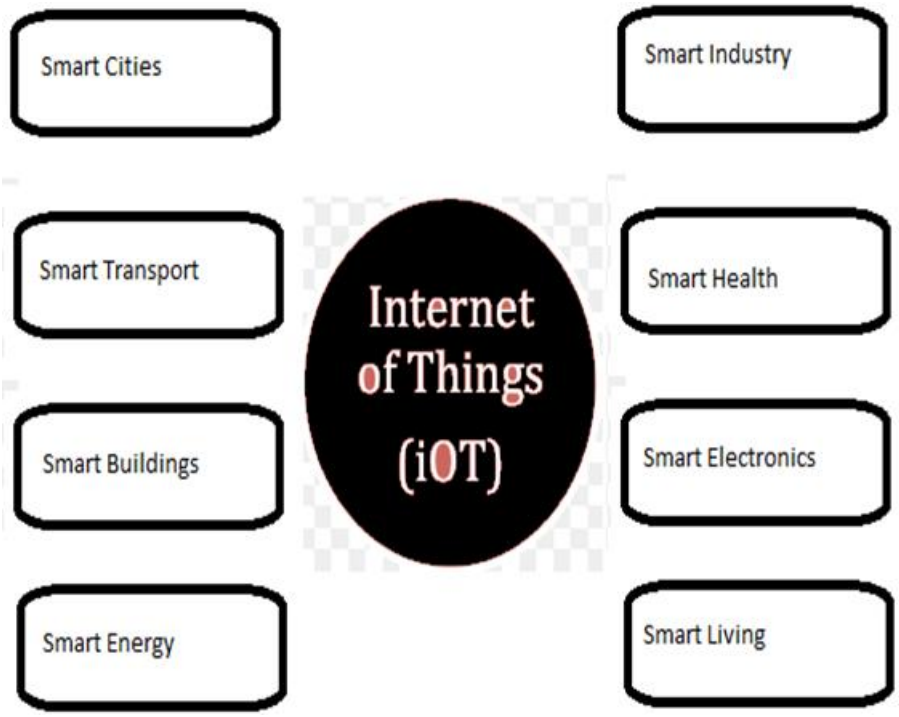

Figure 1. Internet of things in smart environment.

Figure 1 depicts the Internet of Things in Smart Environment. IoT facilitated the interaction of human with anyone over the world with a smart sensor device. IoT include technologies to acquire and process contextual information like sensors, Near Field Communicators, Global Positioning Systems etc. The IoT brings many opportunities to the society but these technologies penetrate all the aspects related to the communicator and require solution to improve security and privacy. Now billions of internet connected devices found and creates open global network connectivity for people to improve people's lives. As a result, trillions of things connected via internet and more IoT applications have been implemented. IoT brings many opportunities in business, industry, and technology to increase its performance, at the same time adding complexities to information technology. From the technology perspective the data in IoTis generated by machines and increase the density by Moore's law. A smart object with enough memory is capable to recognize and store information about people and other object in the network. Hence a major functional requirement of IoT is the preservation of security improvements and privacy.

Protection of data is a serious issue, when devices are connected to outside world3. In IoT a person is always traceable and smart devices collect the data and information without their knowledge hence violate the security service let alone4. Almost all information collected by these smart sensors is private and confidential. So this security related challenges need to be addressed by the research community5.In IoT communication enabled between smart object and social medias and is vulnerable to Trudy involvements. The mobility, dynamic nature and weak physical security of Mobile devices also made it a surface for attack. IoT connected devices lead to the privacy leakage and exposure of authentication credentials to the hackers. So a more secure authentication

mechanism from the client device itself is required for secure browsing6,7. This research presents a literature review and a promising prototype for authentication in IoT environment.

2. AUTHENTICATION

For implementing trust in IoT communications and ensuring the goals of information security, we are required to take necessary care for server authentication and user authentication. Authentication is the process of validating one's identity in communication and ensures the reliability of origin of communication. It is one of the primary goals of security and acts as a gateway in front of a secure system to prevent the malfunctions. When more devices are connected, then a new mechanism need to be developed to authenticate the users and devices. The authentication mechanisms used in commercial applications categorized into four – something you know, something you have, something you are and some place where you are. Among these most common authentication scheme used is user ID and password submission mechanism over a Secure Socket Layer connection. Sometimes the systems calculate the cryptographic hashes and avoid the transmission of plaintext password. But the credentials are sent via the internet and the availability of wireless hotspots are growing so vulnerable to access by the intruders even if it is hashed. Also 3G GSM connection is unsafe and crack able within2 hours. Hence we require a solution without revealing our secret for authentication. Conventional authentication to a system always results overhead to the server and time consuming procedure at end user machine. So to overcome this issue, current researches focus on a solution for Memory and Battery constrained Smart devices. This research extends a lightweight solution in small footprint with high performance and low cost for IoT environment8,9. Also when we analysed the IoT devices, it is found that majority of devices lack password and authentication mechanisms. The use of weak passwords and traffic encryption is a major issue in IoT10. Now a day people increasingly used their hand held mobile devices for banking, payment, shopping etc. hence it will be beneficial to protect their identity and ensure authentication11.In IoT the possible communications are device to device, device to human, human to human and hence support heterogeneous entities and networks. As devices have no prior knowledge about other entities and no SSL communication is enabled, eavesdropping is possible. Moreover, IoT smart devices with sensors and actuators exchange and collect the personal data for authentication and chance to have unauthorized revelation of identity. So for personal data protection and anonymity we require an entirely different access control, authorization and attack detection mechanisms. The discrimination from sensor output is a big problem and the privacy law is still unprepared for IoT. In traditional authentication process client submits its user id and password, client machine creates the hash of the password then transmit the user id and password hash via network. The reply packets from the server are also transmitted via network. A public Wi-Fi or 3G mobile broadband is used to transmit these credentials and is vulnerable to attacks. A hacker can sniff the credentials and can use it later to avail services from the server or he can use some software's to recover the password from the hashes. The authentication mechanisms are mainly classified into private key based, public key based and one-time signature based. Public key based systems require high computation, communication and

storage overhead. Also existing private key mechanisms are not feasible for resource constrained devices and an internet security standard like TLS does not support small embedded units. Due to portable nature, wireless connections and devices connected together in network access layer, IoT require a specific security concern. Hence Zero Knowledge proof is a best choice for such devices. Slawomir et al extends web applications with Zero Knowledge Proof (ZKP) algorithm based on isomorphic graphs. There experimental evaluation shows ZKP isfeasible with existing web standards with advantages of asymmetric key cryptography. This solution allows server to verify the authenticity of web client without directly checking the secret credential of client12.In Implementing Zero Knowledge Authentication with Zero Knowledge (ZKA_wzk), Lum Jia Jun and Brandon provide a practical web/python implementation of Zero Knowledge authentication protocol. This implementation is used to prove that it is able to prove the password is correct without revealing the password. The simplicity and ease of their implementation prove that Zero Knowledge Protocol is suitable choice for IoTauthentication13.In 2012 Manish P Gang wane finds the importance of Zero Knowledge Proof in wireless sensor network for identification of attacks. IoT devices attach with a variety of sensors and connected to wireless networked environment. These sensors are automatically controlled and there is an issue of security. In this he implemented Zero Knowledge Proof for the verification of sender sensor nodes14.In Real time authentication system for RFID applications, Swathi Kumari introduced a new security layer for authentication. The application captures location information then matches it with predefined authorized location for granting access to the system21 In Real. This method suitable for RFID devices and offer secure authentication using back end servers when compared with previous methods for RFID authentication. Jae-Kyung Park et al. proposed authentication service to resolve the existing certificate problems and presents certification device. The system is based on Public key cryptography and the operators need to prepare separate certification method22.Traditional Authentication and Access Control solutions are not suitable for resource and battery constrained smart environment. The lack of implementation of lightweight authentication mechanisms concentrated on this research and proposes a new lightweight method for trust management specifically for smart mobile devices. Smart Mobile devices are manufactured by consumer goods makers and lack the data security in many cases. At the same time intelligent objects in these devices are prawn to security flaws. So an Authentication module with at most care is a requirement for these devices.

3. PROPOSED SYSTEM AND METHODOLOGY

A strong authentication and access control module suitable for available footprint is designed based on Zero Knowledge Protocol. A device wish to connect to a resource owner must require registering with the resource owner. Resource owner select a group G and select a random numberg0 belongs to the group G. The clients who wish to communicate with the owner must agree with these global public elements. In registration process the client inputs user ID and password. An authentication application at client side generates the hash of the password X and compute Y= g0X and sends user ID and Y to the resource owner, server stores this information in

(IJIASE) 2017, Vol. No. 3, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

its SQLite database. In authentication module when client initiates communication then resource owner generates a onetime token OTP by applying Pseudo Random Number Generation algorithm and save in data base with Clients user ID. The server then encrypts the OTP with a 4-digit key generating from system clock by combining current hour and minute. Resource owner send this encrypted OTP via Short Message Service. The authentication module installed in client device decrypt it by current time and retrieves the OTP for authentication. The client is only able to decrypt it within 60 seconds, now all devices used the standard time from satellites so no synchronization is required. After decrypting the OTP user select a random key which is also an element of group G and calculates g0rand concatenates this with Y and token. Next procedure is to apply hashing algorithm to prepare the digest C from the concatenated result and compute Z=r-C.X. Finally, the client sends C and Z to the resource owner. When C and Z from the client received, server calculate

Step 1: Read and separate the plain text password/ characters from the text from which the system need to produce the hash.
Hence password P is treated as P = P1P2P3P4…… Pn
Step 2: Map each character in the plaintext to another set of values by applying a simple mathematical function and we can designate them as
Y1=H(P1), Y2=H(P2), Y3=H(P3),…… Yn=H(Pn)
Step 3: Use encrypted OTP received from the resource owner as the initial key value for hashing.
Step 4: Prepare an HMAC with OTP by applying cumulative hashing
H (……H (H (H (OTP, Y1), Y2) Y3) ….. Yn)

For preparing and verifying the hashes both resource client and resource owner need to agree with a hash function and seed value. Here we use the same OTP received in encrypted format from the server for ZKP implementation. Also a secure way is identified for symmetric key exchange. Finally, we evaluated our algorithm by a prototype implementation in mobile operating system. The main functionalities included in the prototype summarized in Table 1

Table 1. Functionalities of prototype model

Agreement of Global Public Elements
Registration with Resource Owner
Token Generation and Encryption
Retrieval of Token by Decryption
Hash Preparation and Verification

4. RESULTS AND DISCUSSION

Based on the initial prototype model, we proposed a light weight power efficient authentication and access control algorithm for smart mobile devices in IoT. Table2 depicts the computational and memory requirements of the cryptographic protocols as per the theoretical considerations.

Table 2. Requirements of cryptographic protocols

Protocol	Message size supported	No of Iterations	Amount of Calculation	Memory Requirements
ZKP	Large	Many	Large	Large
Public Key	Large	One	Very Large	Large
Private Key	Large	One	Small	Small

Table 3. The performance matrix

Function	Time Requirement (ms)	Memory Requirement (bytes)
Key Agreement	1.07	64 bytes
Registration with Resource Owner	2.03	320 bytes
Token Generation and Encryption	25 KB encryption 3 ms	12 bytes
Retrieval of Token by Decryption	3 ms	---
Hash Preparation and Verification	119	16 bytes

User authentication is very crucial requirement for accessing sensitive information from IoT enabled environment. For secure banking and online shopping applications, now we trust HTTPS based on asymmetric key cryptography but not suitable for IoT. Asymmetric key algorithms are more secure than private key algorithms but additional cost and power will be required. So for IoT environment we choose symmetric key system. The computation overhead of proposed scheme is very low because we use simple mathematical functions to prepare the hashes and require less memory and clock cycles when compared with existing MD5 and SHA algorithms. Proposed authentication method use an algorithm based on Zero Knowledge Proof so an entity can authenticate without revelling the secrets to the resource servers and all computations carried out at user's browser. Zero Knowledge Protocols require small computations and are light weight hence less memory is required for its operations, suitable for memory and power constrained smart mobile devices. We measured the computation time required for a secure authentication and calculate the memory requirement. The performance matrix for the proposed scheme in terms of computational time and memory requirement is summarized in Table 3. Low communication overhead is required by the proposed scheme because the length of the message exchanged between user and server is too short. The proposed method fulfils the properties of Zero Knowledge proof and provides solutions against various threats in network.

(IJIASE) 2017, Vol. No. 3, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

5. FUTURE ENHANCEMENT

We extended an approach for Zero Knowledge Proof for authentication on mobile devices in IoT to reduce computation and communication overhead. In this work we use same OTP for verification and hash preparation, and plan to develop an algorithm for key exchange in IoT. With the introduction of GPS, NFC and RFID, location of the devices are traceable but sometimes the user need to hide their location from services. We propose a context based filter to preserve privacy based on situation. The future work also concentrates on the design of a small server to act like a firewall in between server and requester and hence develop a complete attack resistant and resilient solution for mobile devices in IoT23.