ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, Vol 9(9), DOI: 10.17485/ijst/2016/v9i9/86791, March 2016 ISSN (Online) : 0974-5645

A Secure Authentication Infrastructure for IoT Enabled Smart Mobile Devices – An Initial Prototype

K. A. Rafidha Rehiman* and S. Veni

Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore - 641021, Tamil Nadu, India; rafidharahiman494@gmail.com, venikarthik@gmail.com

Abstract

Background/Objectives: Internet of Things (IoT) has made significant changes in the real world and penetrates all aspects of human life. The user acceptance of IoT is enormously high and its widespread usage is because of the availability of smart phones and tablets. Wide adoption of IoT in the applications of each field always collecting sensitive information and provide a larger surface for intruders. So privacy preserved authentication and access controls are big challenges in its research area. **Methods/Statistical Analysis:** In this paper we introduced a novel algorithm based on Zero Knowledge Protocol and Accumulated Hashing to provide secure authentication to sensor enabled mobile devices in IoT. Also for ensuring confidentiality in communication proposed a new method for key exchange using current time. **Findings:** The proposed method fulfills the requirements of resource and battery constrained mobile devices in IoT when compared with traditional authentication and access control mechanisms for other applications.

Keywords: Authentication, Accumulated Hashing, Internet of Things, Mobile Security, Zero Knowledge Protocol

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 any place. 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 enable communication[1]. So every object connected can be tracked. Each participant autonomously interacting and communicating via internet and no centralized authority is there to control the objects[2]. 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 IoT is 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

* Author for correspondence

people and other object in the network. Hence a major functional requirement of IoT is the preservation of security improvements and privacy.

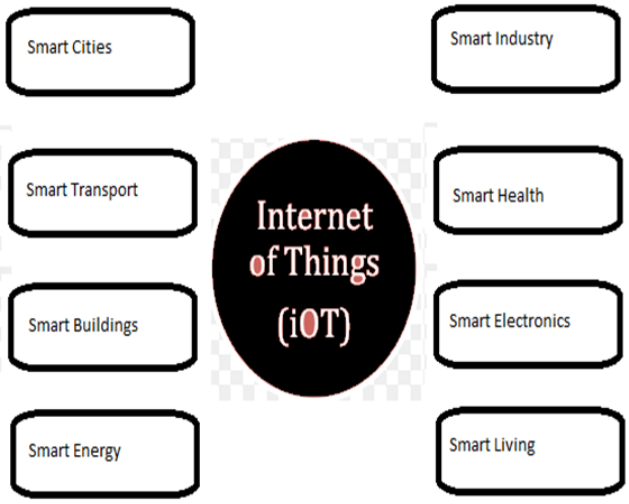

Figure 1. Internet of things in smart environment.

Protection of data is a serious issue, when devices are connected to outside world[3]. In IoT a person is always traceable and smart devices collect the data and information without their knowledge hence violate the security service let alone[4]. Almost all information collected by these smart sensors is private and confidential. So this security related challenges need to be addressed by the research community[5].

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 browsing[6,7]. 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 plain text 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 crackable within 2 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 light weight solution in small footprint with high performance and low cost for IoT environment[8,9].

Also when we analyzed 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 IoT[10]. 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 authentication[11].

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, evesdropping 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 is feasible 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 client[12].

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 IoT authentication[13].

In 2012 Manish P Gangawane 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 nodes[14].

Parikshit N Mahalle et al. in Idenity Authentication and Capability based Access Control (IACAC) for the Internet of Things tried to implement authentication and access control in Internet of Things. Paper presents a secure ECC based integrated approach for authentication and access control and claimed that method is efficient in terms of computational time. The protocol is suitable to defy Denial of Service attack, Man in the Middle attack and reply attack[15].

In 2013 Xuanxia Yao et al proposed a lightweight multicast authentication mechanism for small scale IoT applications. The authors analyzed the importance of Nyberg's fast one way accumulation in security and revised the algorithm to make it suitable for lightweight environment. Also they present an evaluation of the model based on probability theory and evaluate their design for the performance aspects. In the paper they claimed that multicast authentication algorithm meets the requirements of resource constrained applications[16].

Tuhin Borgohain et al. analyzed various authentication systems implemented to preserve the privacy of user credentials in Internet of Things. In first part of their paper they proved that Multi Factor Authentication systems are not applicable to the field of Internet of Things even though it provides greater security to user credentials. The paper suggested the importance of OAuth for IoT based security. The method results a secure experience for login to the resource server. They point out the relevance of an access token to access the resources from server[17].

In September 2014 Padraig Flood et al presented a graph theory based ZKP approach for securing the Internet of Things. The purpose of their research is to determine a security infrastructure for embedded processors in Internet of Things and a resource efficient alternative for existing standards. They summarized the study by pointing the need of future researches required in IoT[18].

Most recently in January 2015 Jitendra Kurumi and Ankur Sodhi conducted a survey of Zero Knowledge Proof for authentication, identification, key exchange and other cryptographic operations. The surveys proved that ZKP implementations solved the problems in cryptography and provide lightweight solutions within small footprint[20].

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 system[21] 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 a certification device. The system is based on Public key cryptography and the operators need to prepare separate certification method[22].

Traditional Authentication and Access Control solutions are not suitable for resource and battery constrained smart environment. The lack of implementation of lightweight authentication mechanism is concentrated on this research and proposes a new light weight 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. ZKP is a concept which allows a communication party to prove that he knows a secret without revealing the secret. The verifier only knows that information is true[19]. The properties of ZKP include completeness, soundness and zero knowledge.

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 number g_0 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 $Y= g_0^X$ and sends user ID and Y to the resource owner, server stores these information in its SQLite database.

In authentication module when client initiates communication then resource owner generate 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 r which is also an element of group G and calculates g_0^r and 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 $Y^C g_0^Z = g_0^{XC} g_0^{r-CX} = g_0^r$. Now the server has g_0^r, Y and OTP concatenate all these apply same hashing procedure and verify the received hash[20]. For hash preparation we propose a revised Fast – One way Accumulation suitable for IoT environment. Hash preparation algorithm explained below.

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 $P = P_1P_2P_3P_4\ldots\ldots P_n$

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

$Y_1=H(P_1),\ Y_2=H(P_2),\ Y_3=H(P_3),\ldots\ldots\ldots\ Y_n=H(P_n)$

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, Y_1), $Y_{2)}$ Y_3) ….. 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. Table 2 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

authenticate without reveling 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.

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

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 some times 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 IoT[23].

6. References

1. Vermesan O, Friess P. Internet of Things – From research and innovations to market deployment. River Publishers; 2015.
2. Peppet SR. Regulating the Internet of Things: First step towards managing discrimination. Privacy, Security and Consent, Texas Law Reviews. 2014.
3. Sen J. Privacy preservation technologies in Internet of Things. International Journal BITM Transactions on EECC. 2009 Aug; 1(4):496–504.
4. Oleshchunk V. Internet of things and privacy preserving technologies. IEEE Wireless VITAE'09; 2009. p. 336-40.
5. Huang X, et al. User interactive Internet of Things privacy preserved access control. The 7th International Conference for Internet Technology and Secured Transaction ICITST; 2012.
6. Alcaide A, Palormar E, Castillo JM, Ribagorda A. Anonymous authentication for privacy preserving iot target driven applications. Computer Security. 2013; 37:111-23.
7. Lin XJ, Sun L. Insecurity of an autonomous authentication for privacy preserving IoT target driven applications. 2013 Nov 28:1-8.
8. Kothmayr T, Schmitt C, Hu W, Brunig M, Carle G. DTLS based security and two way authentication for the internet of things. Elsevier Journal of AdHoc Networks. 2013 Nov; 11(8):2710-23.
9. Gogha R, Prateek S, Kataria N. Home automation: Access control for IoT devices. International Journal of Scientific and Research. Oct 2014; 4(10).
10. Lee JY, Lin WC, Huang YH. A lightweight authentication protocol for internet of things. IEEE 2014.
11. Hummen R, Shafagh H, Raza S, Voigt T, Wehrle K. Delegation based authentication and authorization for the IP based Internet of Things. IEEE 2014.
12. Grzonkowski S, Zaremba W. Extending web applications with a lightweight Zero Knowledge proof authentication. CSTST. 2008 Oct 27-31:1-6.
13. Jun LJ, Brandon. Implementing Zero Knowledge authentication with zero knowledge (ZKA_wzk). Proceedings of the Python Papers monograph 2:9; Pycon Asia – Pacific. 2010.
14. Gangawane MP. Implementation of in wireless sensor network for identification of various attacks. IJETAE. 2012 Aug; 2(8):124-9.
15. Mahalle PN, Anggorojati B, Prasad NR, Prasad R. Identity Authentication and Capability based Access Control (IACAC) for the Internet of Things. Journal of Cyber Security and Mobility. 2013; 1:309-48.
16. Yao X, Han X, Du X, Zhou X. A lightweight multicast authentication mechanism for small scale IoT applications. IEEE Sensors Journal. 2013 Oct; 13(10):3693-701.
17. Borgohain T, Borgohain A, Kumar U, Sanyal S. Authentication systems in internet of things. 2015.
18. Flood P. Securing the internet of things – A ZKP based approach. Sep 2014.
19. Kurumi J, Sodhi A. A survey of zero knowledge proof for authentication. International Journal of Advanced Research in Computer Science and Software Engineering. 2015 Jan; 5(1):494-501.
20. Huqing W, Zhixin S. Research on zero knowledge proof protocol. International Journal of Computer Science. 2013 Jan 1; 10(1):194-200.
21. Kumari S. Real time authentication system for RFID applications. Indian Journal of Science and Technology. 2014 Mar; 7(S3). doi no:10.17485/ijst/2014/v7i3S/48656
22. Park JK, Lee HS, Kim SJ, Park JP. A study on secure authentication system using integrated user authentication service. Indian Journal of Science and Technology. 2015 Sep; 8(23). doi no: 10.17485/ijst/2015/v8i23/79284
23. Rehiman KA, Veni S. Security, privacy and trust for smart mobile devices in internet of things – A literature study. IJARCET. 2015 May; 4(5):1775-9.