International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

Integrating Lamports OTP Scheme with Elliptic Curve Cryptography (ECC)

Sunil K S[1], ShamShekar S Patil[2]

[1]*M.Tech, IVth Sem, Dept. of CSE, DR. AIT, Karnataka, India, Bangalore*

[2]*Associate Professor, Dept. of CSE, DR. AIT, Karnataka, India, Bangalore*

Abstract- *Setting up end-to-end verification amongst gadgets and applications in Internet of Things (IoT) is a testing errand. Because of heterogeneity regarding gadgets, topology, correspondence and diverse security conventions utilized as a part of IoT, existing validation instruments are helpless against security dangers and can upset the advancement of IoT in acknowledging Smart City, Smart Home and Smart Infrastructure, and so forth. To accomplish end-to-end confirmation between IoT gadgets/applications, the current validation plans and security conventions require a two-element verification component. Subsequently, as a major aspect of this anticipate we audit the reasonableness of a validation plan in light of One Time Password (OTP) for IoT and proposed an adaptable, proficient and powerful OTP plan. Our proposed plan utilizes the standards of lightweight Identity Based Elliptic Curve Cryptography plan and Lamport's OTP calculation. We assess diagnostically and tentatively the execution of our plan and watch that our plan with a littler key size and lesser framework performs keeping pace with the current OTP plans without bargaining the security level. Our proposed plan can be executed continuously IoT arranges and is the right possibility for two-variable verification among gadgets, applications and their correspondences in IoT.*

Keywords: Internet of Things, authentication, encryption

1. INTRODUCTION

Insurgency in the field of Internet of Things (IoT) is driving various applications in the range of Smart City, Smart Home, Smart Health and so forth., to upgrade the expectations for everyday comforts of the general population all inclusive. To understand this, a plenty of computerized gadgets are conveyed which speak with each other straightforwardly or through entryway or applications. From IoT application point of view (Fig. 1), we conceive IoT as interconnected Applications, Devices, Gateways and Cloud stages. Gadgets are assembled into various groups wherein bunch head is meant as door. Passage deals with the gadgets which have a place with its bunch. Gadgets inside the bunch speak with each other straightforwardly or through the entryway. Further, these portals are overseen by IoT cloud stages. These stages are conveyed topographically and speak with each other. Consequently to empower secured and coordinated interchanges crosswise over IoT, the application and gadgets need to verify each other through a cloud stage. Also, correspondence conventions contrast from one application to other and are helpless against various security dangers. Aside from this, a portion of the broadly utilized IoT correspondence conventions, for example, MQTT (Message Queue Telemetry Transport), Constrained Application Protocol (CoAP) have no inbuilt security instruments [1]. In spite of the fact that CoAP and different conventions for IoT have expanded security arrangements, for example, Datagram Transport Layer Security (DTLS), Secure Sockets Layer (SSL) and Transport Layer Security (TLS), they are powerless against known dangers [1], [2].

Consequently in IoT, existing interchanges have constrained inbuilt single-variable validation security instrument, along

these lines not adequate to moderate the dangers and requires increased confirmation plan. Thus IoT design needs to visualize a two component verification plan to meet fundamental security necessities, for example, classification, honesty and accessibility of the gadgets and their correspondences to imagine previously stated shrewd applications. The above all else prerequisite of the correspondence conventions is to set up realness between the computerized substances. In the writing, a few verification plans, for example, Message Authentication Code (MAC), signature, One Time Password (OTP), secure token and so forth., are talked about in the zone of saving money exchanges, specially appointed systems, computerized correspondence systems [3]–[8]. Because of heterogeneity as far as figuring force, stockpiling, battery power, portability, shared correspondence and usefulness (sense and activate), achievability to adjust the current verification plans should be tended to. Going ahead, the vast majority of the information from IoT gadgets are filed at IoT cloud stage (open, private) for different information investigation furthermore clients/applications are empowered to order the IoT gadgets through a stage [4]. In this manner, just validated and approved clients/applications can get to the information and solicitation/summon IoT gadgets. To encourage this, verification and approval plans for IoT should be tended to.

.

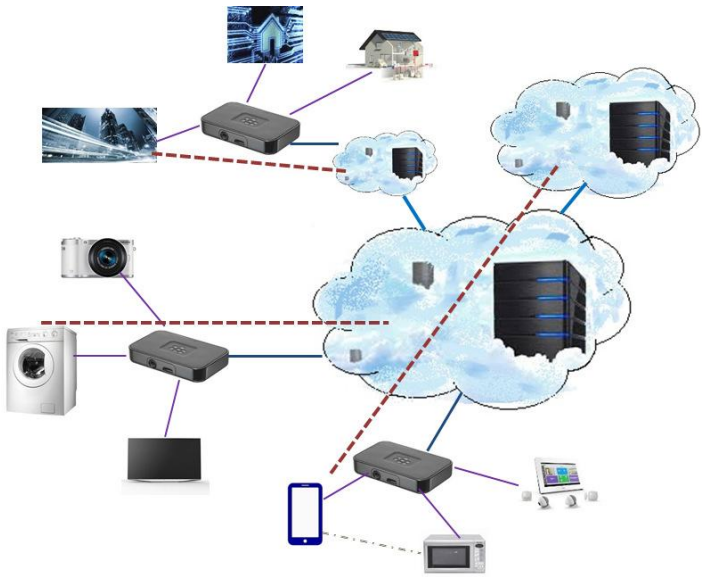

Fig. 1: IoT Architecture

We classify the authentication schemes for IoT as follows:

(a). Two party authentication through a trusted party with key exchange [5],

(b). Mutual authentication schemes [9].

(c). Directed path based authentication scheme (DPAS) [6],

(d). Session key based authentication [10],

(e). Two way authentication [7],

(f). Group authentication [11] and

(g). One time password (OTP) and SecureID Authentication Schemes [8], [12], [13].

From these plans (a-g), we construe that the vast majority of the plans are reliant on the specific kind of IoT engineering and utilized at various layers of IoT convention stack. With respect to security, they are inclined to assaults, the vast majority of these plans need neighborhood key administration and require framework for putting away the keys, consequently helpless against key burglaries [4], [5].

The paper is sorted out as takes after. Area II depicts a related work on existing OTP methods and their constraints from the IoT point of view. Our proposed OTP plan, taking into account IBE bend and Lamport's OTP calculation is depicted in Section III. In Section IV, Results and correlation of our proposed OTP

plans against the current OTP plans are broke down. At long last the paper is finished up in Section V.

2. RELATED WORK

The IoT field is quickly picking up consideration given its capacity of data accumulation and transmission by associating everything through the web. A specific number of investigates tasks are being completed at various colleges and labs to accomplish the best nature of administration in the region. The security viewpoint is among the examination points under study and more arrangements have been proposed. In this segment we show a survey on the works done around there.

Jingjun and Liangmin [14] exhibited a fast distinguishing proof confirmation convention for versatile hubs which is an advantageous sort of convention in the earth of the Internet of Things with security assurance where the mobiles hubs are required to be validated by the bunch keeping in mind the end goal to perform the correspondence. The convention outlined depends on the Veronoi [15] system model and it contains a legitimate solicitation message and an answer confirmation message, which quickly actualizes recognizable proof validation and security insurance. In addition the creators broke down the convention security lastly they formalized the convention in connected pi analytics which is a dialect for portraying simultaneous procedures and their communications. It develops the pi math adding the likelihood to display cryptographic primitives through a mark and an equational hypothesis. This is to demonstrate the security insurance properties in the convention. In examination with existing single-step conventions like the essential hash convention and OSK convention, the creators found that their convention has less correspondence overhead, is sufficiently secure and introduces more protection assurance angles contrasted with the related conventions.

Liang et al. [16] proposed security-basic interactive media administration engineering in the IoT connection for mixed media applications with essential attributes, for example, activity investigation, security necessities and movement booking. As per the creators, their proposition is one of the principal security-mindful activity administration systems for such applications in the IoT. The significant parts of the proposed convention are as taking after: key administration [17–18], clump rekeying, confirmation and watermarking. The proposed plan in the validation process includes techniques running from the utilization of access control and capacity declarations to common verification between the server and client in light of the entrance control, capacity endorsements and shared confirmation [19,20]. For the most part, the capacity of watermarking is about indentifying the substance cause, to follow wrongfully conveyed materials and avoid unapproved content access [21]. To suit distinctive interactive media application needs, three methods of operation are recommended [22]: intermittent group rekeying, occasional clump leave rekeying and intermittent cluster join rekeying.

Gao et al. [23] proposed a correspondence convention for RFID frameworks in the Internet of Things and demonstrated its wellbeing by the irregular prophet strategy [24]. The proposed security model for RFID frameworks in the IoT fundamentally comprises of perusers, labels and RFID middleware. Every item in the framework has a one of a kind EPC. So as to depict the RFID framework model in the Internet of Things the irregular prophet model is connected [25]. The article proposes the SPAP convention which utilizes symmetric encryption, one-way hash capacity and XOR. As demonstrated by the irregular prophet model, SPAP can accomplish shared confirmations, interior security, possession exchange of labels; besides, can likewise oppose retransmission, following of some fundamental assaults. At last, as per the protected execution investigation comes about, the SPAP convention has great execution.

All the more as of late Ye et al. [26] have proposed a productive verification and access control plan for the observation layer of the Internet of Things concentrated on basic and proficient common confirmation and secure key foundation in light of ECC, which has much lower stockpiling and correspondence overheads. The ABC-based approval technique has been received for the entrance control approach. Their engineering configuration is predominantly in view of the idea of a base station (BS) which gathers the information and controls the sensor hubs, the client is characterized as a guest in the observation layer, including gadgets such mobiles telephones, and savvy PCs. At long last the trait power (AA) is the substance responsible for making and dealing with the characteristic data. A productive ECC-based verification and the property based access control approach were proposed keeping in mind the end goal to accomplish common confirmation amongst client and hubs and fine-grained access control. Shared verification guarantees the security of the correspondence amongst client and hubs, whose procedure is easy to take care of the asset obliged issue of the IoT observation layer. Getting to the information on the premise of client property testaments in the entrance control power can accomplish adaptable fine-grained access control. The proposed plan has better execution on the sensor hub side in examination with others reported in [27].

3. PROPOSED WORK

System Architecture Diagram

The below figure 2 shows a general block diagram describing the activities performed by this project. The entire architecture has been implemented in nine modules which we will see in high level design and low level design in later chapters.

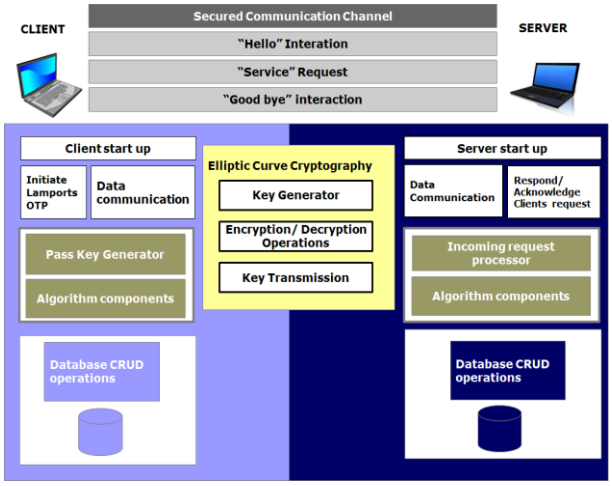

Fig 2: System Architecture

Various divisions in the project

- **Elliptic Curve Cryptography Core Algorithm**
  Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography (based on plain Galois fields) to provide equivalent security. Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization. The figure 3 shows the algorithm of ECC.

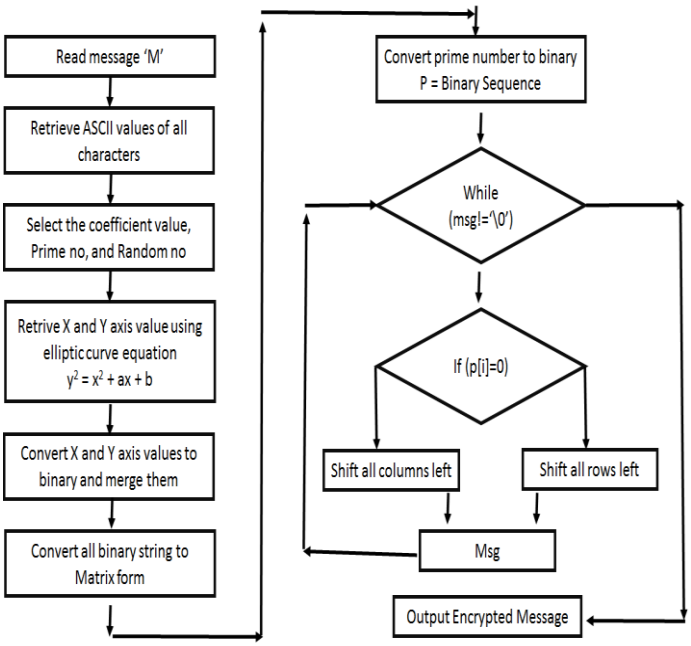

Fig 3: Algorithm of ECC

- **Lamports One Time Password Authentication Scheme**

The Lamport algorithm for generating and applying one-time passwords (OTPs) is a simple solution that provides great value in the right context. Not only can the Lamport OTP scheme provide effective security for distributed client/service interactions, but it's also simple to comprehend and implement. Louis Iacona introduces the Lamport algorithm, then describes an OTP reference implementation for an extensible, Java-based library.

There's a subtle beauty in simple things that present great value. To paraphrase Albert Einstein, a solution to a problem should be as simple as it can be, but no simpler. Applying a one-time password (OTP) scheme between distributed systems makes it more difficult for a would-be intruder to access and gain unauthorized control of restricted resources such as data, physical devices, or service end points. An OTP scheme is obviously a step up from completely open access, or access limited only by physical network barriers. But a solution based on an OTP challenge also has some advantages over static, infrequently changing passwords, because the window of opportunity to gain access to credentials is much smaller. There's a practical place for either type of authentication, or even both used in concert.

The Lamport OTP approach is based on a mathematical algorithm for generating a sequence of "passkey" values, each successor value based on the value of its predecessor. The Figure 4 shows the Lamport function and Lamport Inverse Function.

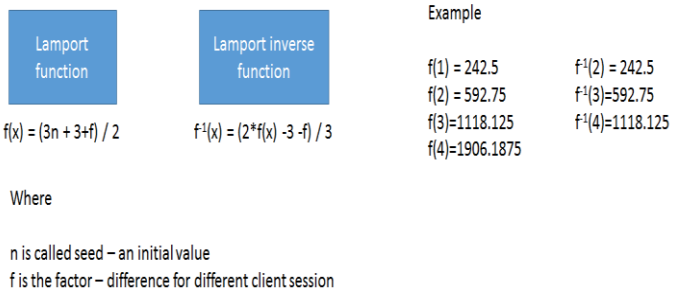

Fig 4: Lamport functions with examples

- **Client and Server applications**

These applications will be implemented as a standalone java application that will integrate the Elliptic Curve Cryptography and Lamports OTP scheme. The client and server applications will be executing in different hosts and we will show the communication between them will be encrypted using Elliptic curve cryptography. And also the clients' authentication will be established using Lamports One time password authentication scheme. The Figure 5 shows the client server account access control operation.

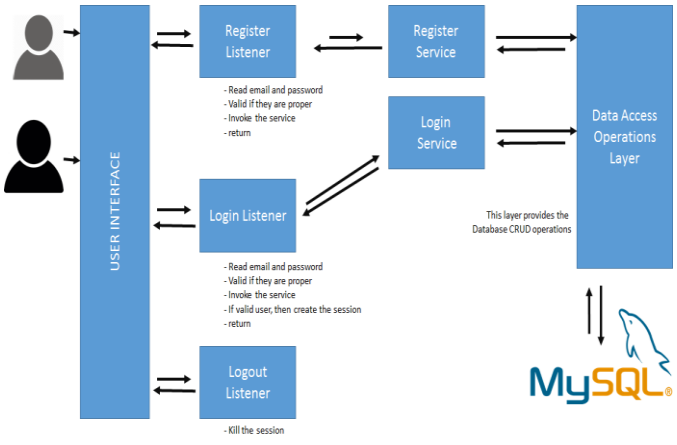

Fig 5: Account Access Control Operation

4. RESULTS AND DISCUSSION

This section is going to give the snapshots of the project which is implemented using java. The Figure 6 is going to show the client side of the project which is used for sending the message. The client clicks on the send message to send the message. The server is going to receive the message from the client and generates the key and sends it to the client, this is show in the Figure 7. The Figure 8 shows the snapshot of OTP generation and forwarding it to client.

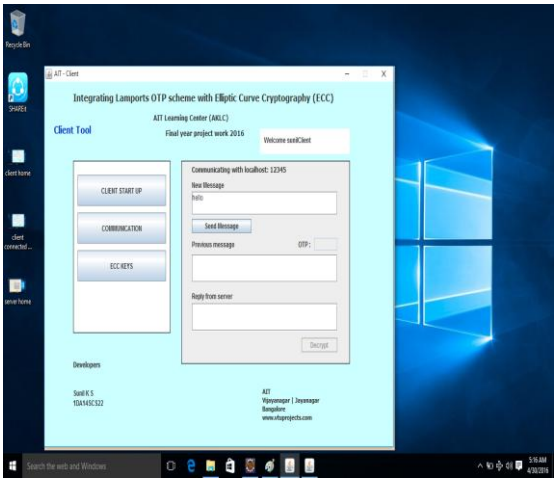

Fig 6: Client Side

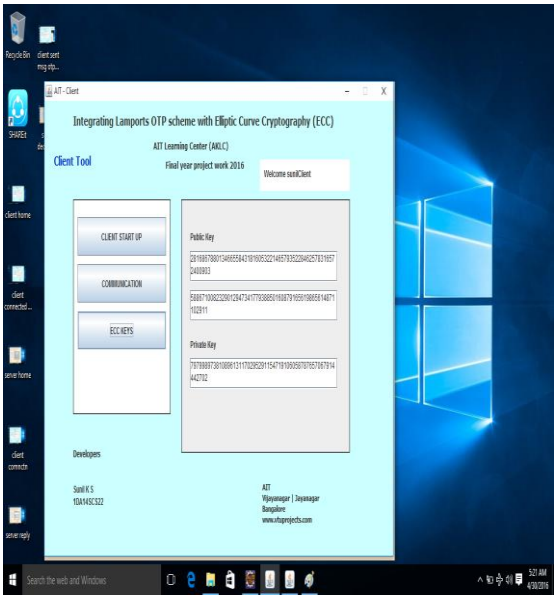

Fig 7: Server Generating the Key

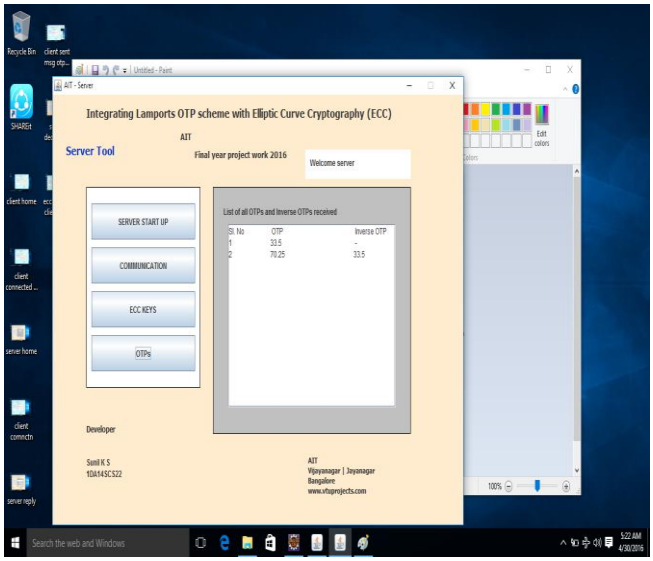

Fig 8: Client receiving the OTP

5. CONCLUSION

In this anticipate we have investigated the current OTP plans utilized for end-to-end confirmation in IoT and have proposed a lightweight, strong and versatile OTP plan by utilizing the standards of IBE-ECC. Since we don't store the keys, key size is little and don't rely on upon the past keys (memory less),our plan requires lesser assets for operation when contrasted with the current plans, for example, HOTP, TOTP, Bicakci et al.,Yeh et al., Lamport's hash based calculation and Chefranov and Goyal et al, and so on. We have exhibited that our proposed plan with a littler key size and lesser framework performs comparable to the current OTP plans, without trading off the security level. Since our plan requires less assets and the key size is littler when contrasted with the current plans, it can be seen as an unmistakable possibility for expansive and differing IoT frameworks, for example, Smart City, Smart Home and Smart Infrastructure arrangements. As a component of our future work, we are currently conveying our proposed plan on a genuine IoT stage such that constant execution assessment can be acquired.

REFERENCES

[1] J. Antonio J, L. Latif, and S. Antonio, "The internet of everythingthrough ipv6: An analysis of challenges, solutions and opportunities,"in Journal of Wireless Mobile Networks, Ubiquitous Computing, andDependable Applications, ser. JoWUA '13. Innovative Information Science & Technology Research Group, 2013, pp. 97–118.

[2] G.-M. Oscar, K. Sandeep S, H. Sye, Loong Keoh Rene, and S. Rene,"Security considerations in the ip-based internet of things," in IETFDraft-garcia-core-security-06, ser. Internet Draft '14. IETF, 2014, pp.1–45.

[3] A. Hiltgen, T. Kramp, and T. Weigold, "Secure internet bankingauthentication," in IEEE Security and Privacy, 2006, pp. 21–29.

[4] M. Parikshit N, A. Bayu, P. Neeli R, and P. Ramjee, "Identity authenticationand capability based access control (iacac) for the internet ofthings," in Journal of River Publications. River Publishers, 2013, pp.1–40.

[5] L. Chen-Xu, L. Yun, Z. Zhen-Jiang, and C. Zi-Yao, "The novel authenticationscheme based on theory of quadratic residues for wireless sensornetworks," in International Journal of Distributed Sensor Networks.Hindawi, 2013.

[6] N. Huansheng and L. Hong, "Directed path based authentication schemefor the internet of things," in Journal of Universal Computer Science,2012, pp. 1112–11 131.

[7] C. Schmitt and B. Stiller, "Two-way authentication for iot," in IETF,ser. ACE Working Group '14. IETF, 2014, pp. 1–19.

[8] L. Leslie, "Password authentication with insecure communication," inCommunications of the ACM, ser. J.UCS '12. New York, NY, USA:ACM, 2012, pp. 770–772.

[9] G. Zhao, X. Si, J. Wang, X. Long, and T. Hu, "A novel mutual authenticationscheme for internet of things," in Modelling, Identificationand Control (ICMIC), Proceedings of 2011 International Conferenceon, June 2011, pp. 563–566.

[10] V. Cakulev, G. Sundaram, and I. Broustis, "Ibake: Identity-based authenticatedkey exchange," in RFC 6539, ser. Informational '12. IETF,2012, pp. 1–13.

[11] M. Parikshit N, A. Bayu, P. Neeli R, and P. Ramjee, "Novel thresholdcryptography-based group authentication (tcga) scheme for the internetf things (iot)," in 7th IEEE ANTS. IEEE, 2013, pp. 1–6.

[12] D. M'Raihi, S. Machani, and J. Rydell, "Hotp: An hmac-based onetimepassword algorithm," in IETF RFC 4226, ser. Network WorkingGroup '05. IETF, 2005, pp. 1–37.

[13] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen,"Totp:time-based one-time password algorithm," in IETF RFC 6238,ser. Informational '11. IETF, 2011, pp. 1–16.

[14]. Miao J., Wang L. Rapid Identification Authentication Protocol for Mobile Nodes in Internet of Things with Privacy Protection. J. Netw. 2012;7:1099–1105.

[15]. Du X., Xiao Y., Mohsen G. An effective key management scheme for heterogeneous sensor network. Ad Hoc Networks. 2007;1:24–34.

[16]. Liang Z., Chao H. Multimedia Traffic Security Architecture for the Internet of Things. IEEE Netw.2011;25:35–40.

[17]. Zhao H.V., Lin W.S., Liu K.J.R. A Case Study in Multimedia Fingerprinting: Behavior Modeling and Forensics for Multimedia Social Networks. IEEE Signal Proc. Mag. 2009;26:118–139.

38. Chen M., Gonzalez S., Zhang Q., Leung M.V.C. Software Agent-based Intelligence for Code-centric RFID Systems. IEEE Intell. Syst. 2010;25:12–19.

[18]. Kundur D., Luh W., Okorafor U.N., Zourntos T. Security and Privacy for Distributed Multimedia Sensor Networks. Proc. IEEE. 2008;96:112–130.

[19]. Zhou L., Xiong N., Shu L., Vasilakos A., Yeo S. Context-Aware Multimedia Service in Heterogeneous Networks. IEEE Intell. Syst. 2010;25:40–47.

[20]. Zhou L., Wang X., Tu W., Muntean G., Geller B. Distributed Scheduling Scheme for Video Streaming over Multi-Channel Multi-Radio Multi-Hop Wireless Networks. IEEE J. Sel. Area. Commun. 2010;28:409–419.

[21]. Eskicioglu A.M. Multimedia Security in Group Communications: Recent Progress in Key Management, Authentication, and Watermarking. Multimed. Syst. 2003;9:239–248.

[22]. Susanto H., Muhaya F. Multimedia Information Security Architecture Framework. Proceedings of the FutureTech; Busan, Korea. 21–23 May 2010.

[23]. Gao D., Guo Y.J., Cui J.Q., Hao H.G., Shi H. A Communication Protocol of RFID Systems in Internet of Things. Int. J. Secur. Appl. 2012;6:91–102.

[24]. Martin G. Ph.D. Thesis. University of California at Davis; California, CA, USA: 2008. A Study of the Random Oracle Model.

[25]. Alomair B., Clark A., Cuellar J., Poovendran R. Scalable RFID systems: A privacy-preserving protocol with constant-time identification. Proceedings of the International Conference on Dependable Systems and Networks; Chicago, IL, USA. 28 June–1 July 2010.

[26]. Ye N., Zhu Y., Wang R.C., Malekian R., Min L.Q. An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things. Int. J. Appl. Math. Inf. Sci. 2014;8:1617–1624.

[27]. Hsiu Y.L., Chen T.H., Liu P., Kim T., Wei H. A secured authentication protocol for wireless sensor networks using Elliptic Curves Cryptography. Sensors. 2011;11:4767–4779.