Result Paper for Improve Security and Optimizing Information Leakage over Public Multi- Cloud Environment

[1] Bandgar Sunil Ajinath, [2]Hole Shubham Sunil, [3]Khajjepawar Shubham Digambar, [4]Bhosale Prajakta Anandkumar.

[5] Vinay S. Nalawade, [6] Sayyad G.G.

[123456]Student at Department of Computer Engineering SBPCOE, Indapur-413106, India.

Abstract : We propose a two-point information security protection mechanism with issue revocability for cloud storage system. Propose system allows sending an encrypted message to a destination via cloud storage server. The sender only needs to know the identity of the receiver however no different data (such as its public key or its corticated). The receiver has to possess two things to decrypt the cipher text. The primary factor is his/her secret key hold on within the pc. The second factor could be a distinctive personal security device that connects to the pc. It is impossible to decrypt the cipher text without either piece. Additional signicantly, once the safety device is stolen or lost, this device is revoked. It cannot be used to decrypt any cipher text. This could be done by the cloud server that is able to right away execute some algorithms to vary the prevailing cipher text to be un-decryptable by this device. This technique is completely clear to the sender. Moreover, the cloud server cannot decrypt any cipher text at any time. The security and potency analysis show that our system is not solely secure but additionally sensible.

IndexTerms **- Privacy preserving, Computational model, Cloud, Sensitive data, secure self-destructing, fine-grained access control**

I.INTRODUCTION

Cloud computing that has received respectable attention from analysis communities in world yet as industry, may be a distributed computation model over an outsized pool of shared-virtualized computing resources, like storage, processing power, applications and services. Cloud users square measure provisioned and unharness recourses, as they need in cloud computing setting. this type of recent computation model represents a replacement vision of providing computing services as public utilities like water and electricity. Cloud computing brings variety of advantages for cloud users. As an example, (1) Users will cut back cost on hardware, software and services as a result of they pay just for what they use; (2) Users can fancy low management overhead and immediate access to a wide vary of applications; and (3) Users will access their data where they need a network, instead of having to remain nearby their computers. However, there's a massive form of barriers before cloud computing will be wide deployed. A recent survey by Oracle referred the information supply from international data corporation enterprise panel, showing that security represents eighty-seven of cloud users' fears1. One in all the foremost security considerations of cloud users is that the integrity of their outsourced files since they not physically possess their knowledge and so lose the management over their knowledge. Moreover, the cloud server is not fully trustworthy and it is not obligatory for the cloud server to report knowledge loss incidents. Indeed, to establish cloud computing reliability, the cloud security alliance (CSA) printed AN analysis of cloud vulnerability incidents. The investigation [2] revealed that the incident of information Loss accounted for twenty fifth of all incidents, hierarchical second solely to "Insecure Interfaces & APIs". Take Amazon's cloud crash disaster as an example2. In 2011, Amazon's immense EC2 cloud services crash for good destroyed some knowledge of cloud users. The data loss was apparently tiny relative to the full knowledge keep, but anyone United Nations agency runs an internet site will instantly perceive how alarming an occasion any knowledge loss is. Typically, it is insufficient to sight knowledge corruption once accessing the info because it would be too late to recover the corrupted knowledge. As a result, it is necessary for cloud users to often check if their outsourced knowledge square measure keep properly. The size of the cloud knowledge is large, downloading the complete file to see the integrity can be preventive in terms of bandwidth value, and hence, terribly impractical. Moreover, ancient cryptographic primitives for knowledge integrity checking such as hash functions, authorization code (MAC) cannot apply here directly because of being in need of a duplicate of the first file in verification. Last, remote knowledge integrity checking for secure cloud storage may be a extremely fascinating yet as a challenging analysis topic.

Blum planned AN auditing issue for the primary time that allows data house owners to verify the integrity of remote knowledge while not explicit data of the complete knowledge. Recently, remote data integrity checking becomes additional and additional vital due to the event of distributed storage systems and online storage systems. Demonstrable knowledge possession (PDP) at untrusted stores, introduced by Ateniese et al., is a novel server. In PDP, the info owner generates some information for a file, then sends his file at the side of the information to a remote server and deletes the file from its native storage. To generate a signal that the server stores the first file correctly, the server computes a response to a challenge from the admirer. The admirer will verify if the file keeps unchanged via checking the correctness of the response. PDP may be a sensible approach to checking the integrity of cloud knowledge since it adopts a spot-checking technique. Specifically, a file is split into blocks and an admirer solely challenges tiny low set of arbitrarily chosen clocks for integrity checking. In step with the instance given by Ateniese et al., for a file with 10; 000 blocks, if the server has deleted 1 Chronicles of the blocks, then a admirer can sight server's misconduct with chance larger than 99% by asking proof of possession for under 460 arbitrarily selected blocks. Ateniese et al. planned two concrete PDP constructions by creating use of RSA-based homomorphic linear authenticators. Because of its necessity and utility, remote knowledge integrity checking has attracted in depth analysis interest in recent years.

Shacham and Waters planned the notion of compact proofs of retrievability by creating use of publically verifiable homomorphic authenticators from BLS signature. This scheme conjointly depends on homomorphic properties to mixture a proof into atiny low appraiser worth and as a result, the public retrievability will be achieved.

II. LITERATURE SURVEY

1. Privacy preserving public auditing for shared data in the cloud B. Wang, B. Li, and H. Li 2014

In This paper, The identity of the signer on every block in shared knowledge is unbroken personal from public verifiers, efficiency verify shared knowledge integrity while not retrieving the whole file. Additionally it is ready to perform multiple auditing tasks at the same time rather than corroborative them one by one. The disadvantage is Ring signatures is utilize to construct homomorphic authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block. The problem with this system is 1.Traceability, which means the ability for the group manager to reveal the identity of the signer based on verification metadata in some special situations and how to prove data freshness. Batch Auditing can be used to distinguish who is the signer on each block 2.designing an efficient public auditing mechanism with the capabilities of preserving identity privacy and supporting traceability. TPA can be implemented which will be able to support batch auditing.

2. **Ensuring privacy and data freshness for public auditing of Shared data in cloud Tina Esther Trueman ,P.Narayan asamy 2012**

It uses a novel methodology for making certain privacy and data freshness of shared knowledge in cloud exploitation Homomorphic authenticable ring signature (HARS) theme to preserve the user privacy and Overlay tree rule is employed for making certain that users the information with needed level of freshness. In addition, Third Party Auditor (TPA) audits the information keep within the cloud. He should be able to verify the trustiness of the CSP while not disclosing the identity of the users within the group. The disadvantage is malicious activities Identity based integrity checking and attribute based data sharing with time constraints mechanism in cloud computing made by the user cannot get detected. The problem with this system is to extend the traceability, which means only the original user, can reveal the identity of the signer in order to preserve the malicious activity made by the user in the group. Solution can be Batch Auditing can be used to distinguish who is the authorized person signer on each block.

3. **Toward Efficient and Privacy Preserving Computing in Big Data Era Rongxing Lu, Hui Zhu, Ximeng Liu, Joseph K. Liu, and Jun Shao 2014**

Introduced an efficient and privacy preserving cosine similarity (PCSC) computing protocol in response to the efficiency and privacy requirements of data mining in the big data era. 2. The proposed PCSC protocol is not only privacy-preserving but also efficient. It is particularly suitable for big data analytics. The advantage is the computation overhead of the propos ed-PCSC protocol also increases when n is large. The disadvantage is Needs to provide unique privacy for some specific big data analytics. Introducing protocol like privacy computing to provide complete and unique security in big data era.

4. **Privacy-preserving access control model for big data cloud S. Fugkeaw and H. Sato, International Computer Science and Engineering Conference (ICSEC), Chiang Mai, 2015, pp. 1-6.**

Proposed a novel access control model combining Role-based Access Control (RBAC) model, symmetric encryption, and cipher text attribute-based encryption (CP-ABE) to support fine-grained access control for big data outsourced in cloud storage systems. We also demonstrate the efficiency and performance of our proposed scheme through the implementation.

5. **Privacy-preserving public auditing for secure cloud storage Wang, Cong, et al, IEEE Transactions on computers 62.2 (2013): 362-375.2013.**

Proposed a privacy-preserving public auditing system for data storage security in Cloud Computing. They made use of the Homomorphic authenticator and random masking to guarantee Identity based integrity checking and attribute based data sharing with time constraints mechanism in cloud computing that TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users fear of their outsourced data leakage. Authors also claim that the proposed schemes are provably secure and highly efficient.

6. **Privacy-preserving public auditing for secure cloud storage Wang, Cong, et al, IEEE Transactions on computers 62.2 (2013): 362-375.2013.**

In paper authors proposed a privacy-preserving public auditing system for data storage security in Cloud Computing. They made use of the Homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users fear of their outsourced data leakage.

7. **A secure document self destruction scheme with identity based encryption Jinbo Xiong, Zhiqiang Yao Jianfeng Ma, Ximeng Liu, Qi Li IEEE transaction (2014)**

In this paper the concept used is IBE-based secure document self-destruction (ISDS) scheme. ISDS scheme is able to resist not only traditional cryptanalysis and brute-force attack, but also Sybil attacks (e.g., hopping attack and sniffer attack) in the DHT network. ISDS scheme can also provide fine-grained access control during the lifetime of the sensitive documents, which is not guaranteed in other existing schemes. ISDS scheme Have not achieved flexible fine-grained access control The ISDS scheme should not introduce new security risks to the users. ISDS should resistance to attack.

8. **An Identity Preserving Access Control Scheme with Flexible System Privilege revocation in cloud computing Rohit Ahuja, Sraban Kumar, Mohanty Kouichi SAKURA**

Identity based integrity checking and attribute based data sharing with time constraints mechanism in cloud computing in this paper the Identity preserving access control scheme is used for cloud security. IPAC used to efficiently utilize data, scheme enables user to query CSP for desired data. This scheme achieved flexible access control by employing CPASBE and scalability is achieved by incorporating delegation with hierarchical formation of users. The computation involves in re-encryption of ciphertext to cloud servers using proxy re encryption scheme. The user is not able to modify data on cloud server as the number of data consumer increases, data owner will be overburdened with the Decentralizing the key-issuing authority at different levels of hierarchy of organization. It also allow users to modify data on cloud servers.

9. **Cipher text Policy Weighted Attribute Based Encryption for Fine Grained Access Control Jianfeng Ma, Jinbo Xiong, Qi Li, Jun Ma IEEE transaction (2014)**

In this paper the cipher text policy weighted attribute based encryption technique is used. It defines How to construct more efficient CP-ABE schemes with weighted attributes. It also defines how revocation attributes in different weights works more efficiently to design an advance CPWABE scheme to solve these problems.

III. SYSTEM DESCRIPTION

1. Data Owner: data owner will give data or les that contain some sensitive info, that are used for sharing with his/her friends (data users). Of this shared information are outsourced to the cloud servers to store.

2. Authority: An important entity is liable for generating, distributing and managing all the private keys, and is trustworthy by all the opposite entities concerned within the system.

3. Time Server: it is a time reference server with none interaction with alternative entities concerned within the system. it's liable for an explicit unleash time specification.

4. Data Users: data users are some peoples who passed the identity authentication and access to the info outsourced by the info owner. Notice that, the shared data will solely be accessed by the licensed users throughout its authorization amount.

5. Cloud Servers: It contains virtually unlimited cupboard space that is ready to store and manage all the info or les within the system. Alternative entities with restricted cupboard space will store their data to the cloud servers.

6. KDC: A typical operation with a KDC involves a call for participation from a user to use some service. The KDC can use scientific discipline techniques to certify requesting users as themselves. It will additionally check whether a private user has the proper to access, the service requested. If the genuine user meets all prescribed conditions, the KDC will issue a price ticket allowing access. The KDC generates secret keys for all the users in step with their identities. The cloud user has great deal of files to be hold on cloud while not keeping a neighborhood copy, and the cloud server has vital cupboard space and computation resources and provides information storage services for cloud users.

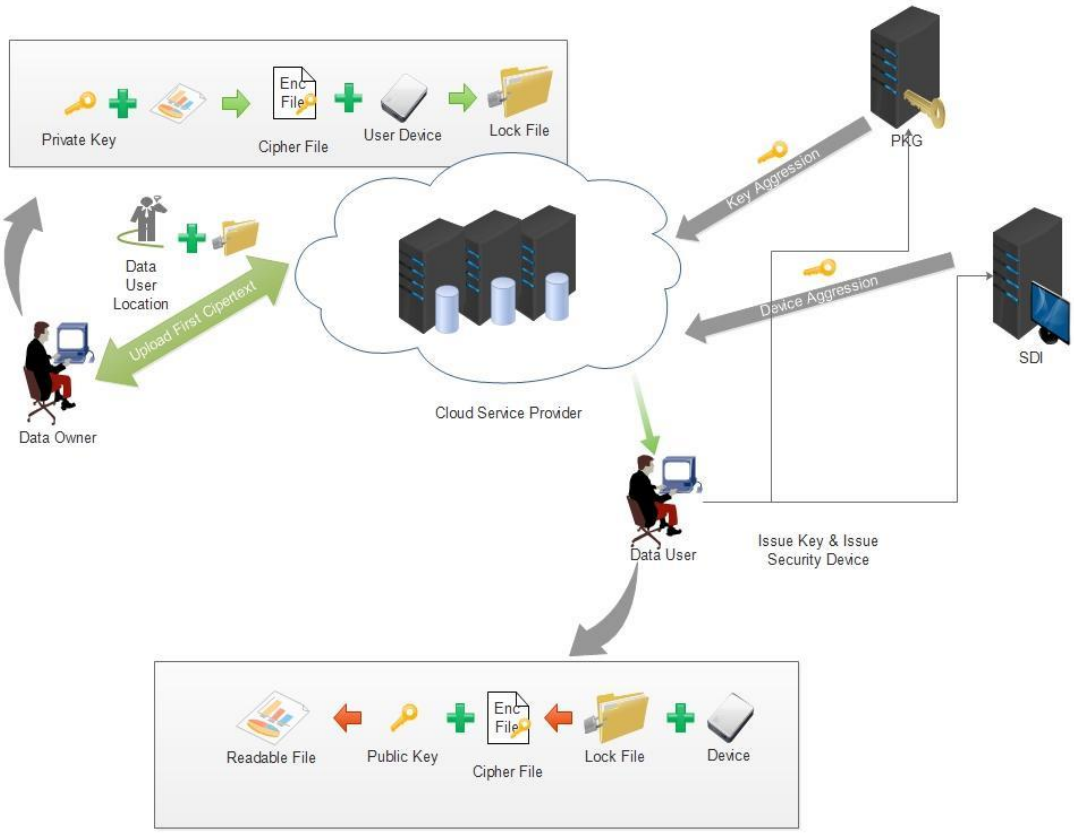

Figure 1 Architecture Diagram

7. TPA: TPA has experience and capabilities that cloud users do not have and is trustworthy to ascertain the integrity of the cloud data on behalf of the cloud user upon request. Every entity has their own obligations and advantages severally. The cloud server can be self-interested, and for his own advantages, like to keep up an honest name, the cloud server may even commit to hide information corruption incidents to cloud users. The TPAs job is to perform the info integrity checking on behalf the cloud user; however, the TPA is additionally curious within the sense that he is willing to find out some info of the users data throughout the info integrity checking procedure.

IV. RESULT AND RESULT ANALYSIS

The KP-TSABE theme is verified to be secure under the quality model. Therefore,we tend to consistently compare this theme with the prevailing self-destruction solutions (e.g., Vanish, SSDD, ISS, and FullPP) from the subsequent aspects, e.g., requirement condition, algorithm, resistance on attacks, fine-grained access management,

Security Properties	Vanish	SSDD	ISS	Full PP	KP_TBASE
Need "no attacks on VDO before it expires"?	YES	YES	YES	NO	No-Need
Leveraging what kind of algorithm?	Symmetric	Symmetric	IBE	ID-TRE	KP-TSABE
Whether cipher text is destructed or not?	NO	YES	YES	YES	No-Need
Whether the key is destructed or not?	YES	YES	YES	YES	No-Need
Resistance on the traditional cryptanalysis?	NO	YES	YES	YES	YES
Resistance on the Sybil attacks?	NO	NO	YES	YES	_
Resistance on the collusion attack?	_	_	_	_	YES
Supporting fine-grained access control?	NO	NO	YES	YES	YES
Providing full lifecycle privacy protection?	NO	NO	NO	YES	YES
Supporting user-defined time intervals?	NO	NO	NO	Half	YES
Security proof under standard model?	NO	NO	NO	YES	YES

•All the schemes of Vanish, SSDD and ISS wish the simplest assumption "no at-tacks on VDO before it expires". Since a Sybil antagonist is during a position tocrawl sufficient key shares from the DHT network to reconstruct the decryp-tion key. Once the antagonist gets the VDO from the cloud servers before itexpires, he/she will decrypt it with the reconstructed decipherion key to obtainthe plaintext.

•FullPP doesn't wish this ideal assumption as a results of the decoding key isencrypted by the ID-TRE rule. although the opposer crawls sufficient keyshares from the DHT network, he cannot reconstruct the decoding key sincehe doesn't have the ID-TRE private key. KPTSABE conjointly doesn't would like theideal assumption as a result of it does not need the DHT network. Algorithmand resistance on attacks. Since each Vanish and SSDD solely use symmetricencryption to cipher the sensitive message, they bring about complicated key manage-ment and can't achieve fine-grained access control for various users withdifferent attributes.

•Vanish sends the whole ciphertext to the cloud server, therefore it cannot resist against the traditional cryptanalysis. Since the SSDD scheme distributes an element of the ciphertext and also the decoding key to the DHT network, each of which will be self-destructed once expiration, therefore the cloud server stores incomplete cipher text. Therefore, SSDD will resist against the standard cryptanalysis. 2 However, Vanish and SSDD cannot resist against the Sybil attackers who can continually crawl the key shares from the DHT network to recover the de-cryption key.

•In distinction, every ISS and FullPP won't exclusively resist against the conventional cryptography and also the Sybil attacks but to boot implement versatile ac-cessmanagementowingtotheIBEandID-TREalgorithms. KP-TSABE doesn'thave the matter of the Sybil attacks as a results of there's no use of the DHT network. what's a lot of, it'll provide fine-grained access management through combining fully totally different attributes with variance time intervals. User-defined authorization quantity.

•Vanish, SSDD, ISS and FullPP leverage the DHT network to store the keyshares or the hybrid ciphertext shares, that area unit self-discarded by the DHT nodes once an quantity of some time. That the expiration time is proscribed by the update amount of the DHT network and it can't be controlled by the sensitive data owner. above those schemes, inside the KPTSABE scheme,each attribute inside the attribute set related to the ciphertext is matched with a time interval, that's that the authorization amount of the sensitive information and is predefined by the knowledge owner.

•Therefore, the authorization amount and thus the expiration time don't seem to be restricted by the system constraint, however flexibly to be made public by the owner. Security proof. Vanish, SSDD, and ISS don't offer the protection proof. The ID-TRE within the FullPP theme is verified to be secure below the additive Diffie-Hellman (BDH) assumption. moreover, the KP-TSABE

theme is verified to be secure below the standard model with the selection l-Expanded BDHI assumption to resist against the traditional cryptography and therefore the collusion attack. in conclusion, the KP-TSABE theme is superior to theprevailing self-destruction solutions from several security properties.

•The Execution times for each the Elgamal and RSA algorithms space unit shown on the Tables and Figures. The day's square measure measured in milliseconds, however regenerate to seconds as displayed on the result templates. we have a tendency to tend to watch and deduce as follows from the results obtained.

•In the secret writing and communication methodology, theRSAperformshigherthan Elgamal altogether cases. within the secret writing methodology, the Elgamal out performs RSA; that means that text messages area unit decrypted faster by Elgamal than will the RSA technique. At intervals the signature verification methodology, the RSA over again performs over the Elgamal approach. once viewed along tool, the RSA is superior to the Elgamal formula in terms of method speeds. This, in part, explains why the RSA formula has been and remains obtaining utilized in springing up with several security protocols for information communication.

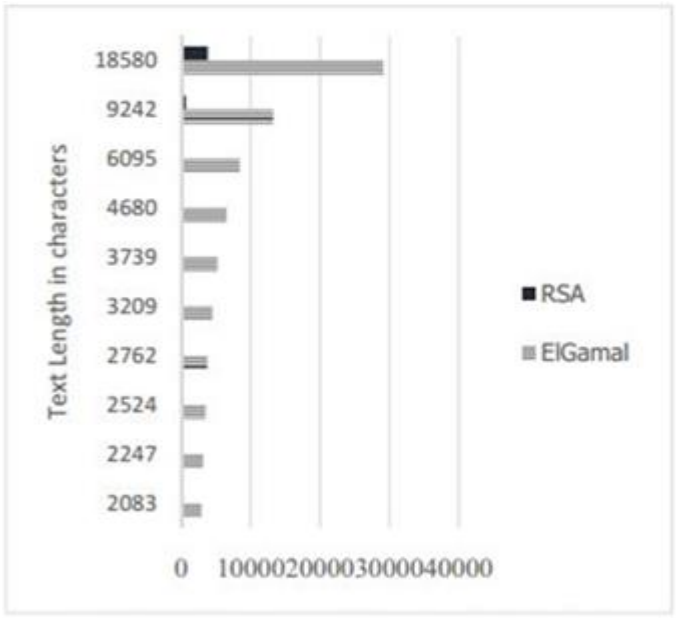

Chart 1: Execution Time for Encryption and Signing

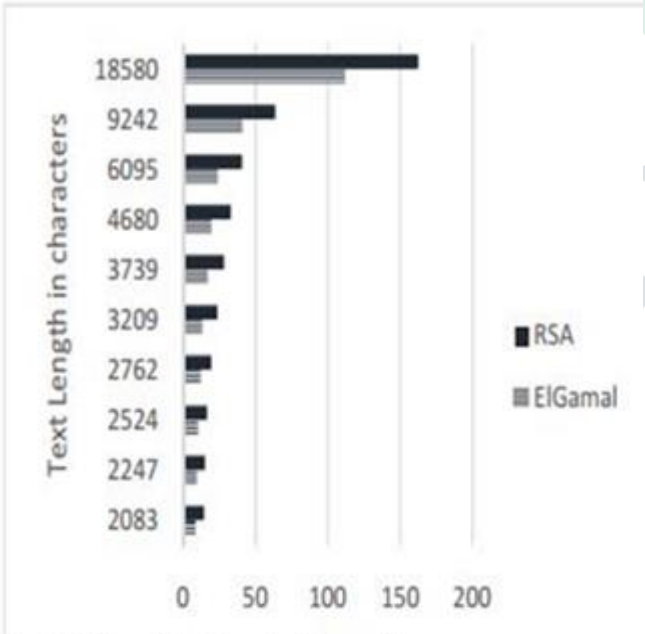

Chart 2: Execution time for Decryption

V. CONCLUSION

we study the matter of class data collection during a multi-category RFID system.Considering the new options of the matter, we propose a two-phase sampling protocol(TPS) that 1st quickly zooms into a class and then isolates an arbitrary tag from the class by victimization the pure mathematics distribution of tags. we the critically analyze the protocol performance and discuss the optimum parameter settings that minimize the general execution time. Extensive simulations show that TPS is ready to shorten the length of the polling vector to solely 7.5 bits, that is incredibly efficient compared with 96-bit tag IDs.

VI. Acknowledgment

We study the matter of class data collection during a multi-category RFID system. Considering the new options of the matter, we propose a two-phase sampling protocol (TPS) that 1st quickly zooms into a class and then isolates an arbitrary tag from the class by victimization the pure mathematics distribution of tags. We theoretically analyze the protocol performance and discuss the optimum parameter settings that minimize the general execution time. Extensive simulations show that TPS is ready to shorten the length of the polling vector to solely 7.5 bits that is incredibly efficient compared with 96-bit tag IDs.

References

[1] R. Li, Z. Huang, E. Kurniawan, and C. K. Ho, AuRoSS: an autonomous robotic shelf scanning system, in Proc. of IEEE/RSJ IROS, 2015, pp. 61006105.J.

[2] Liu, F. Zhu, Y. Wang, X. Wang, Q. Pan, and L. Chen, RF-Scanner: Shelf scanning with robot-assisted RFID systems, in Proc. of IEEE INFOCOM, 2017.

[3] L. Xie, H. Han, Q. Li, J. Wu, and S. Lu, Efficiently collectiing histograms over RFID tags, in Proc. of IEEE INFOCOM, 2014, pp. 145153.

[4] J. Lang and L. Han, Design of library smart bookshelf based on RFID, Applied Mechanics and Materials, vol. 519, pp. 13661372, 2014.

[5] P. Benavidez and M. Jamshidi, Mobile robot navigation and target tracking system, in System of Systems Engineering (SoSE), 2011 6th International Conference on. IEEE, 2011, pp. 299304.

[6] L. Xie, J. Sun, Q. Cai, C. Wang, J. Wu, and S. Lu, Tell me what I see: Recognize RFID tagged objects in augmented reality systems, in Proc. of ACM UbiComp, 2016, pp. 916927.

[7] J. R. Smith, Wirelessly Powered Sensor Networks and Computational RFID. Springer-Verlag New York, 2013.

[8] S. Chen, M. Zhang, and B. Xiao, Efficient information collection protocols for sensor-augmented RFID networks, in Proc. of IEEE INFOCOM, 2011, pp. 31013109.

[9] H. Yue, C. Zhang, M. Pan, Y. Fang, and S. Chen, A time-efficient information collection protocol for large-scale RFID systems, in Proc. of IEEE INFOCOM, 2012, pp. 21582166.

[10] K. Bu, M. Xu, X. Liu, J. Luo, S. Zhang, and M. Weng, Deterministic detection of cloning attacks for anonymous RFID systems, IEEE Transactions on Industrial Informatics, vol. 11, no. 6, pp. 12551266, 2015.