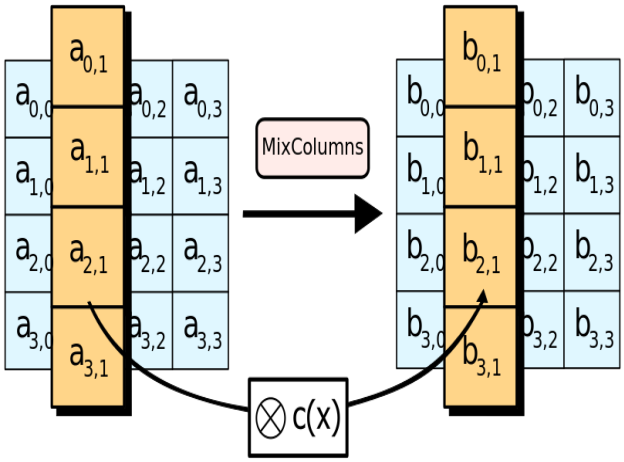

Figure 3: MixColumns module

d) AddRoundKey: In this step, each byte of the state is combined with a byte of the round subkey using the XOR operation

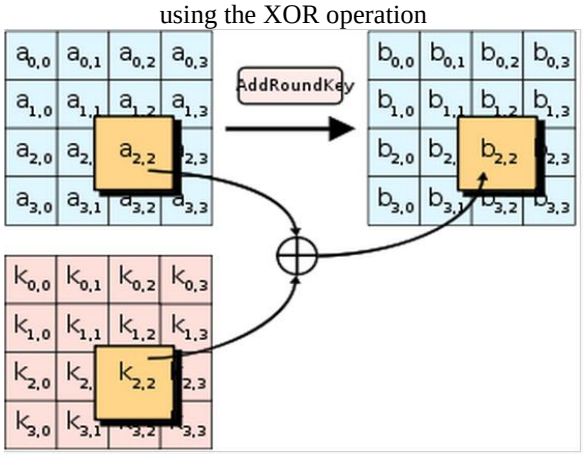

Figure 4: AddRoundKey module

5. Conclusion

In this paper, a novel authorized accessible privacy model (AAPM) and a patient self controllable multi-level privacy preserving cooperative authentication scheme (PSMPA) realizing three different levels of security and privacy requirement in the distributed healthcare cloud computing system are proposed, followed by the formal security proof and efficiency evaluations which illustrate our PSMPA can resist various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead.

References

[1] E. Villalba, M.T. Arredondo, S. Guillen and E. Hoyo-Barbolla, A New Solution for A Heart Failure Monitoring System based on Wearable and Information Technologies, In International Workshop on Wearable and Implantable Body Sensor Networks 2006-BSN 2006, April, 2006.

[2] J. Zhou and M. He, An Improved Distributed Key Management Scheme in Wireless Sensor Networks, In WISA 2008.

[3] S. Yu, K. Ren and W. Lou, FDAC: Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks, In IEEE Infocom 2009.

[4] J. Sun and Y. Fang, Cross-domain Data Sharing in Distributed Electronic Health Record System, IEEE Transactions on Parallel and Distributed Systems, vol. 21, No. 6, 2010.

[5] D. Slamanig, C. Stingl, C. Menard, M. Heiligenbrunner and J. Thierry, Anonymity and Application Privacy in Context of Mobile Computing in eHealth, Mobile Response, LNCS 5424, pp. 148-157, 2009.

[6] J. Zhou and Z. Cao, TIS: A Threshold Incentive Scheme for Secure and Reliable Data Forwarding in Vehicular Delay Tolerant Networks, In IEEE Globecom 2012.

[7] F.W. Dillema and S. Lupetti, Rendezvous-based Access Control for Medical Records in the Pre-hospital Environment, In HealthNet 2007.

[8] J. Sun, Y. Fang and X. Zhu, Privacy and Emergency Response in Ehealthcare Leveraging Wireless Body Sensor Networks, IEEE Wireless Communications, pp. 66-73, February, 2010.

[9] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, SAGE: A Strong Privacy-preserving Scheme against Global Eavesdropping for Ehealth Systems, IEEE Journal on Selected Areas in Communications, 27(4):365-378, May, 2009.

[10] J. Sun, X. Zhu, C. Zhang and Y. Fang, HCPP: Cryptography Based Secure EHR System for Patient Privacy and Emergency Healthcare, ICDCS'11.

[11] L. Lu, J. Han, Y. Liu, L. Hu, J. Huai, L.M. Ni and J. Ma, Pseudo Trust: Zero-Knowledge Authentication in Anonymous P2Ps, IEEE Transactions on Parallel and Distributed Systems, Vol. 19, No. 10, October, 2008.