http://www.jctjournals.com ISSN(ONLINE):2278 – 3814

Volume-10, Issue-3, March, 2021
JOURNAL OF COMPUTING TECHNOLOGIES (JCT)
International Journal
Page Number: 01-07

A Literature Survey of Different Data Encryption Algorithm for Secure Health Care System in Cloud

Jitendra Chouhan*, Prof. Manish Rai**,
M.Tech Scholar CSE*, Assistant professor**
RKDF College of engineering Bhopal [M.P.]
jitendrachouhan014@gmail.com*

***Abstract*— in this survey paper discuss the different type of different data encryption algorithm for secure health care system. Now a day cloud computing is providing highly potential services to IT based healthcare sector. In cloud computing model a patient can get consultancy from any doctor available in the world. There are two types of patient information i.e. protected/sensitive health information and general information. Protected information (Phone no, ATM, Security no, MR no etc.) requires more confidentiality as compared to general information. In this survey paper discuss the various method used in the health care system for secure data transmission in cloud environment. Patient data are highly secure data, which is keen required to safe and secure transmission over a public channel. For secure data transmission information encryption play an important role. In this survey paper discuss all these point and also compare the different methods of secure medical information encryption in public channel.**

Keywords*— Human Visual System (HVS), Health Care System, Cloud Computing, Information encryption and decryption etc.

I. INTRODUCTION

The IoT and cloud based medical services models are gigantic measure of medical services information is being communicated ludicrous. It is crucial for plan a capable methodology for guaranteeing the mystery and dependability of the patient's analysis data imparted from cloud technology [12]. Both of the models are foundation on internetworking between physical devices, building, educational portal, machine, robot as well as additional things placed with software, sensor and network connection that enable these object to collect and interchange information. In cloud based device communicate with each other using cloud user end device-to-server communications with the using movable node, cybernetic and instant networks that are used for direct and remote operation. PC, mobile, laptop are also a cloud device that are most commonly known by people and they are widely spread [12]. A patient can get consultation from any doctor who is available on Internet and is from any part of the world. Digital data is providing a platform to doctors who can monitor their patients. So with the invention of Internet and cloud computing, quality of IT based health care sector services are also improving day by day. This significance has been happens by stegano-realistic methodologies and information encryption models for concealing information to an image pixel. Encryption cryptography is the methodology of encoding messages so the assailants could not read it and can be decoded by a legitimate client [13][14]. At the same time, discrete wavelet change holds monstrous spatial limitation, recurrence spread, and multi goal includes that are comparable with the idea of human visual system (HVS). Not simply run of the mill figuring gadgets, cloud framework comprises of family gadgets and numerous other information gathering sensors. Using internet of thing device, people connect many household things like fan, gas, washing machine, fridge by just a touch on their smart devices. In addition, Cisco's Internet Business Expert Group had calculated that the total no of cloud device users has just doubled. They will widely spread in the world (50 billion devices) by 2020[15] [16] [17].

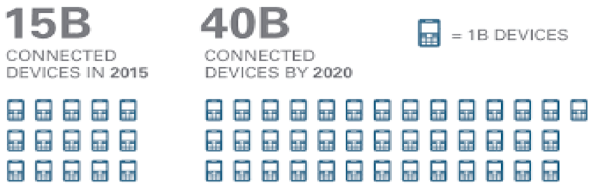

Fig.1 The growth rate of the cloud device

However, some people may still be afraid to have these devices in their homes. Although cloud devices are widely used due to its convenience. It simplify and easier people's life, security experts define various security issue and threat that concerns on the potential security problems (The Insecurity of Things), which differ the data integrity and security among various cloud devices communication device that are concern in the internet of things communication devices among top five security threats in 2015 [18]. Some expert provide a threat model based on use-cases of internet of things, which can be uses some measurement to define accurate amount of damage on data integrity by the causes of thread in cloud communication device [19]. Moreover, cloud devices with weak security level and processing power, such as servers, smart mobile handset and other home appliances are attractive points for the hackers. Therefore in an cloud device have a weak security capability that are used by hacker and authenticated person to get access of data between the transmission between two cloud based internet of things device using the various method of encryption and decryption that gives a negative impact on data integrity, security, data availability as well as steal user sensitive data. But there are a number of attacks e.g. protected/sensitive data theft, DoS, DDoS etc. exists in cloud computing environment. That's why confidentiality and privacy of patient data has more concerned in cloud environment because of it is publically available. If patient confidential information is breach out then a patient may suffer many difficulties e.g. if a celebrity personal email id is hacked then he may loss his reputation etc. Similarly, if a credit card information or account information is leaked out then patient may loss all his money. These are reasons which needs enhancement in security and protection of data [20].For the purpose of advanced level of security in a cloud network, a proposed method is stated in this thesis. Since the computer or laptop is considered as the cloud hardware, in this study, communicating the sensitive information between two computer device and home server is done using the concept of image steganography, whereas encryption as well as steganography is used when the devices are placed out of LAN. Therefore, the attackers have less effect of the transmitted data in order to eavesdrop them (sniffing)[21] [22] [23].

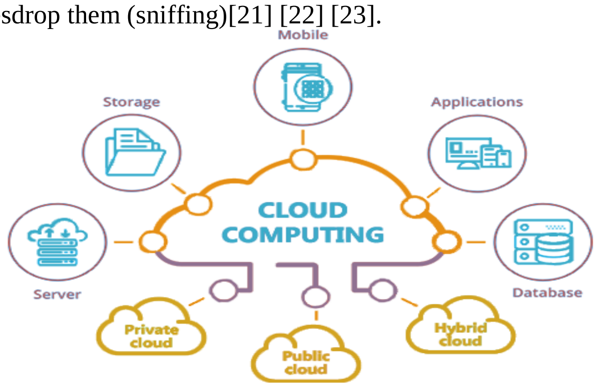

Fig. 2 various attacks at the Cloud device

A. Cloud Computing in Health Care

Cloud computing services are useful for health care sector due to following features

- Clouds computing services remain available by 24 X 7 and patient data can be access from any location wherever Internet service is available.
- Payment is according to requirement of storage and usage of patient data.
- No maintenance cost, extra payment and management cost is required e.g. Network Admin, Room, Electricity to e-Health Sector.
- Resource sharing means one server may be shared between multiple health organizations. Through this way resources utilization will be achieved maximum.
- Performance of servers will be measured by technically sound personnel.
- NIST [4] defines the five benefits of cloud computing
- On demand and Self Service the service is available at demand.
- Rapid elasticity means hardware and software requirements can be upgrade without too much effort
- Broad network Access capabilities are available on Internet and accessibilities methods are standards
- Resource Pooling means resources are shared
- Measure Services pay as you utilize like Internet usage or rent a car service [26].

Cloud computing has become the vital sign for IT technology because of its infrastructure as well as speed budget. With self-service features any users can usescalable features and upgrade the usage depending upon the requirement. This technology offers some particular types of services mentioned below which a user can gain from cloud platform [25].

- Software as a Service in Health care system
- Platform as a Service in Health care system
- Infrastructure as a Service in Health care system

II Literature Survey

PUSHPA, B.et.al. [2020], *"Hybrid Data Encryption Algorithm for Secure Medical Data Transmission in Cloud Environment",* in this research work author presented has introduced an as of late hybridization of data encryption model for defending the conclusion information in clinical pictures. The current model is introduced by the mix of 2D DWT measure with a hybridization of Blowfish and Two fish encryption calculations. The gave model starts the encryption of mystery information at that point disguised the outcome by the usage of result during a cover picture by the use of 1L and 2L 2D DWT. the shading pictures are used as cover pictures for disguising different content sizes. The presentation of the proposed model has been tried against various benchmark pictures and accordingly the outcomes are guaranteed by the use of different execution measures. It’s fascinating that the introduced model has achieved incomparable outcomes with a negligible MSE of 0.08 and most extreme PSNR of 58.96dB.[1]

Tamilarasi, et.al. [2020], ***"Medical Data Security for Healthcare Applications Using Hybrid Lightweight Encryption and Swarm Optimization Algorithm."*** In this work creator introduced information of each individual should be engraved and sent into end-client with no issues. For the most part in the medical care industry, where considerations are regularly centred around saving human’s life and which is all well and good, yet tying down admittance to interfaces and cloud server that store private information like clinical records is additionally a fundamental factor to consider. Information security is a comparing activity between controlling admittance to data while permitting free and simple admittance to the individuals who need that data. Still couple of issues are engaged by the doctor in the wellbeing area. Patient's information ought to be kept safely in clinical supplier workers with the goal that doctors can give appropriate medicines. An epic half breed lightweight encryption utilizing swarm streamlining calculation (HLE–SO) has been successfully present. HLE–SO strategy showed the upgraded execution contrasted with the current framework. This technique has been assessed utilizing recreation instrument and contrasted and existing DLCE strategy, it showed improved outcome like blunder decrease and decrease in cryptography preparing time. Secure route with no emergency. In present, specialist concentrate to diminish the encryption time and make it appropriate for likely relevance continuously applications [2]

Goyal, et.al. [2020], ***"A Hybrid Encryption Model to Lower the Complexity of Securing the Data in Cloud."*** In this research work author presented validate the outcome of the arranged strategy by means of investigation and evaluation. Cloud customers manage the difficulties of choosing proper cloud specialist organizations and evaluate security usage relying upon their security needs. A type of a novel model for offering assurance to various cloud specialist co-ops with the expectation to devise and broaden security implies for distributed computing is actualized [3]

Zhang, et.al. [2019], ***"Hybrid encryption algorithms for medical data storage security in cloud database."*** In this research work creator introduced the AES calculation and the information base external layer encryption technique have higher encryption and decoding proficiency through applicable analyses. As indicated by the qualities of clinical information, the P-AES calculation is available. It has been demonstrated by significant investigations that it has higher encryption and unscrambling productivity than the first calculation and is more appropriate for handling long information. At last, in view of this, joined with the RSA calculation, a half breed encryption calculation is available and effectively applied in the clinical data the executive’s framework. Through inquiry examination, despite the fact that information encryption will influence the proficiency of the question, it is inside the client's acknowledgment. Subsequently, the cross breed encryption calculation can give security assurance to clinical information put away in cloud data set and ensure patients' protection [4]

Le,et.al. [2018], ***"A hybrid approach of secret sharing with fragmentation and encryption in cloud environment for securing outsourced medical database: a revolutionary approach."*** In this research work author presented a cloud computing has arisen out as an ideal information sharing medium to share patient information. The idea of fracture, secret sharing and encryption expects to defend the protection of revaluated data and clients questions. Delicate credits can be ensured by parting secret qualities and conveying them with various pieces on numerous information base specialist organizations. Then, encryption upgrades the security level further. The projected framework is a novel patient-driven system with a bunch of instruments for data access the board to PHRs kept in cloud cuts off. The protection is guaranteed through classification limitations recitation the affectability of qualities and their connections. Our primary plan is to develop the framework for clients in a simple way and without introducing any applications on the client site. In our possibility work, analyst intend to carry out the current engineering to give total electronic information stockpiling frameworks for medical clinics so data have the option to be put away, kept up, rebuilt, recovered proficiently notwithstanding safely [5]

Elhoseny, et.al. [2018],***"Hybrid optimization with cryptography encryption for medical image security in Internet of Things."*** In this research work author presented from the precise discussions made above, it is important perception to elaborate on the few ideas discussed and bring further advances in medical image security process. Additionally, the current study has considered the present technique in hybrid encryption algorithm utilized as a part of IoT. The study also recommended a strategy that can enhance IoT by the hybrid encryption algorithm. This present model, i.e., ECC with PSO and GO, comes with multinomial use in encryption and decoding to accomplish a right message. This algorithm utilizes less memory on account of less financial unpredictability. While demonstrating the current work with diverse measurements, the researchers utilized the imperative measures such as PSNR and SSI which have indicated control image quality against all the tests. It is clear that the procedure is not secure enough as it never furnished great impalpability; so it needs to be investigated additionally to increment the security level. The present algorithm takes less time for both encryption and decryption process. The present work should fundamentally focus on tamper localization scheme in order to have content-based respectability as opposed to the strict-integrity functionality executed in the current algorithms.[6]

Huang,et.al. [2017], ***"Private and secured medical data transmission and analysis for wireless sensing healthcare system."*** In this exploration work creator introduced focusing on the current issues of e-/m-medical services frameworks, an unmistakable system "HES" is available in this paper. The highlights of HES can be summed up in three regions: (1) utilizing minimal effort and handily conveyed remote sensor networks as the hand-off foundation for GSRM-based secure transmission of clinical information from WBANs to WPANs; (2) tending to the issue of accomplishing direct correspondences between a client's portable terminals and installed (wearable) clinical gadgets (hubs); and (3) authorizing protection saving systems HEBM and accomplishing agreeable execution. The execution of a specialist framework that essentially addresses routine actual assessments can significantly lessen a specialist's or head's contribution and empower families and gatekeepers to get to clients' wellbeing data whenever and anyplace. Subsequently, HES can fill in as a critical segment of the data of clinical enterprises. Notwithstanding, a few issues stay strange; for instance, the conclusion unwavering quality of the master framework isn't great, and HES can't right now screen or break down abrupt illnesses. [7]

Chandu,et.al. [2017], ***"Design and implementation of hybrid encryption for security of IOT data."*** In this research work authors introduced the current calculation is demonstrated to be steady, secure and assault evidence for some conditions. This can be carried out and incorporated with all the modern plan of internet of things to get the essential data produced by the\ edge gadgets. The current calculation can be extemporized by utilizing a lot of secure awry key encryption and plan a completely fledged gadget for the equivalent. The calculation can be additionally made a lot of complex to hack by utilizing meeting key age at the solicitation time. A devoted application explicit Integrated circuit (ASIC) is to be intended for a lot quicker handling, encryption and low force. The streamlining of the plan can be completed to improve the force effectiveness and territory proficiency [8].

Khan, et.al. [2015], ***"A cloud-manager-based re-encryption scheme for mobile users in cloud environment: a hybrid approach."*****,** In this research work author presented*CMReS*, most of the encryption, decryption, and re-encryption operations are offloaded on trusted entity and cloud that improve the resource utilization on the mobile device. However, the trusted entities are under the control of the client organization and can be upgraded for gracefully handling the requests from the entire organization. Additionally, the re-encryption responsibilities of the trusted entity are also offloaded on the cloud without affecting the privacy of the user that improves the scalability of the system. The compromising of the authorized group member does not affect the security of the whole system due to the transformation of the uploaded messages with the personal private key of the data owners in the present *CMReS*. Moreover, there is no need to re-encrypt the entire data partition unlike *CReS* due to change in group members that reduces the processing burden from the trusted entities and cloud. Furthermore, the present *CMReS* consume fewer resources on the mobile device while performing encryption, decryption, and re-encryption operations as compared to the existing schemes.[9]

Sharif,et.al. [2014], ***"Online multiple workflow scheduling under privacy and deadline in hybrid cloud environment."*** In this research work author presented The problem of online multiple workflow scheduling has not received adequate attention, while becoming increasingly more complex as the cloud computing paradigm is exposed to hybrid clouds. The main motivation for this study was to address the problem of deadline and privacy constraints Researcher solved this problem by presenting two algorithms, OMPHC-PCPR and OPHC-TR, with different methods to prioritize tasks during resource allocation. Researcher designed a software-as-a-service application where patients' workflows are merged into one DAG in each scheduling interval as the input for both algorithms. OMPHC-PCPR partitions the merged DAG with regard to the privacy level of its tasks, then produces several partial critical paths. All the paths are ranked and assigned to applicable hybrid clouds' instances before their deadline. OPHC-TR, on the other hand, first ranks all tasks of the merged DAG, and then maps each task individually to the allowed instance without violating its privacy and deadline. OPHC-TR operates similarly to the existing work in this field with the addition of the privacy constraint. Researcher introduce OMPHC-PCPR as a further improvement in online multiple workflow scheduling algorithms. Researcher evaluated the performance of the two algorithms and illustrated that OMPHC-PCPR outperforms OPHC-TR by reducing the total cost by up to 50%. For present work, researcher intend to solve this challenge using discrete optimization to minimize the cost further, compared to our current approaches [10]

Tysowski,et.al. [2013], ***"Hybrid attribute-and re-encryption-based key management for secure and scalable mobile applications in clouds."*** In this exploration work creator introduced A key administration framework has been available for information rethinking applications, whereby trait based encryption specifically allows approved clients to get to get content in the cloud dependent on the fulfilment of a characteristic based strategy. The plan has been displayed so an information proprietor and a confided in power co-work in the key age and encryption cycles with the end goal that computationally-serious cryptographic tasks and demands are limited for the information proprietor; this is of significance to a populace of portable clients that should preserve their utilization of battery and use of remote correspondence. Moreover, a half breed convention is available that alternatively permits message encryption dependent on a gathering key, permitting the client participation to be additionally reined. Furthermore, it permits re-encryption to happen, and subsequently renouncement to get old without requiring existing normal cures and their limits, for example, lapse of traits special in the characteristic based strategy. The current convention in comparable in generally execution to the first code text-strategy characteristic based-encryption thought, while essentially diminishing the computational and follow trouble on the portable information proprietor [11]

Table .1 Comparison of Previous Methods

Sr.No.	Author Name	Title	Year/Ref.no.	Method
1	PUSHPA, B.et.al.	"Hybrid Data Encryption Algorithm for Secure Medical Data Transmission in Cloud Environment."	[2020]/[01]	RSA method
2	Tamilarasi, et.al.	"Medical Data Security for Healthcare Applications Using Hybrid Lightweight Encryption and Swarm Optimization Algorithm."	[2020]/[02]	HLE–So method
3	Goyal, et.al.	"A Hybrid Encryption Model to Lower the Complexity of Securing the Data in Cloud."	[2020] /[03]	multi-cloudmethod
4	Zhang, et.al.	"Hybrid encryption algorithms for medical data storage security in cloud database."	[2019]/[04]	encryption method
5	Le,et.al.	"A hybrid approach of secret sharing with fragmentation and encryption in cloud environment for securing outsourced medical database: a revolutionary approach."	[2018]/[05]	encryption method
6	Elhoseny, et.al.	"Hybrid optimization with cryptography encryption for medical image security in Internet of Things."	[2018]/[06]	various methods
7	Huang,et.al.	"Private and secured medical data transmission and analysis for wireless sensing healthcare system."	[2017]/[07]	encryption methods
8	Chandu,et.al.	Design and implementation of hybrid encryption for security of IOT data.	[2017]/[08]	encryption methods
9	Khan, et.al.	"A cloud-manager-based re-encryption scheme for mobile users in cloud environment: a hybrid approach."	[2015]/[09]	cryptographic methods
10	Sharif,et.al.	"Online multiple workflow scheduling under privacy and deadline in hybrid cloud environment."	[2014]/[10]	schedule path method
11	Tysowski,et.al.	"Hybrid attribute-and re-encryption-based key management for secure and scalable mobile applications in clouds."	[2013]/[11]	Encryption method

III. Conclusions

In this survey paper discuss the cloud computing model a patient can get consultancy from any doctor available in the world. In this survey paper discuss the various method used in the health care system for secure data transmission in cloud environment. Patient data are highly secure data, which is keen required to safe and secure transmission over a public channel. For secure data transmission information encryption play an important role. In this survey paper discuss all these point and also compare the different methods of secure medical information encryption in public channel. Table 1 also discuss the comparison of different previous methods.

REFERENCES

[1] PUSHPA, B. "Hybrid Data Encryption Algorithm for Secure Medical Data Transmission in Cloud Environment." In *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 329-334. IEEE, 2020.

[2] Tamilarasi, K., and A. Jawahar. "Medical Data Security for Healthcare Applications Using Hybrid Lightweight Encryption and Swarm Optimization Algorithm." *Wireless Personal Communications* (2020): 1-22.

[3] Goyal, Mani, and Avinash Sharma. "A Hybrid Encryption Model to Lower the Complexity of Securing the Data in Cloud." *Journal of Computational and Theoretical Nanoscience* 17, no. 6 (2020): 2664-2668.

[4] Zhang, Fenghua, Yaming Chen, Weiming Meng, and Qingtao Wu. "Hybrid encryption algorithms for medical data storage security in cloud database." *International Journal of Database Management Systems (IJDMS) Vol* 11 (2019).

[5] Le, Dac-Nhuong, Bijeta Seth, and Surjeet Dalal. "A hybrid approach of secret sharing with fragmentation and encryption in cloud environment for securing outsourced medical database: a revolutionary approach." *Journal of Cyber Security and Mobility* (2018): 379-408.

[6] Elhoseny, Mohamed, K. Shankar, S. K. Lakshmanaprabu, Andino Maseleno, and N. Arunkumar. "Hybrid optimization with cryptography encryption for medical image security in Internet of Things." *Neural computing and applications* (2018): 1-15.

[7] Huang, Haiping, Tianhe Gong, Ning Ye, Ruchuan Wang, and Yi Dou. "Private and secured medical data transmission and analysis for wireless sensing healthcare system." *IEEE Transactions on Industrial Informatics* 13, no. 3 (2017): 1227-1237.

[8] Chandu, Y., KS Rakesh Kumar, Ninad Vivek Prabhukhanolkar, A. N. Anish, and Sushma Rawal. "Design and implementation of hybrid encryption for security of IOT data." In *2017 International conference on smart technologies for smart nation (SmartTechCon)*, pp. 1228-1231. IEEE, 2017.

[9] Khan, Abdul Nasir, ML Mat Kiah, Mazhar Ali, and Shahaboddin Shamshirband. "A cloud-manager-based re-encryption scheme for mobile users in cloud environment: a hybrid approach." *Journal of Grid Computing* 13, no. 4 (2015): 651-675.

[10] Jain, M., Choudhary, R. C., & Kumar, A., "Secure medical imagesteganography with RSA cryptography using decision tree", InContemporary Computing and Informatics (IC3I), 2016 2ndInternational Conference on (pp. 291-295). IEEE,.

[11] Yehia, L., Khedr, A., & Darwish, A., "Hybrid security techniques forInternet of Things healthcare applications", Advances in Internet ofThings, 2015, 5(03).

[12] Zaw, Z. M., & Phyo, S. W., "Security Enhancement System Based on the Integration of Cryptography and Steganography", International Journal of Computer (IJC), 2015, 19(1), 26-39

[13] Sharif, Shaghayegh, Javid Taheri, Albert Y. Zomaya, and Surya Nepal. "Online multiple workflow scheduling under privacy and deadline in hybrid cloud environment." In *2014 IEEE 6th International Conference on Cloud Computing Technology and Science*, pp. 455-462. IEEE, 2014.

[14] A. W. Atamli and A. Martin, "Threat-Based Security Analysis for the Internet of Things," in International Workshop on Secure Internet of Things (SIoT), pp. 35-43, 2014.

[15] L. Touati, Y. Challal, and A. Bouabdallah, "C-CP-ABE: Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things," in International Conference on Advanced Networking Distributed Systems and Applications (INDS), IEEE, pp. 64-69, 2014.

[16] A. Fragkaidakis, E. Tragos, and A. Traganietis, "Lightweight and secure encryption usingchannel measurements," in 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronics Systems, IEEE, pp. 1-5, 2014.

[17] Nadeem Akhtar, Shahbaaz Khan, Pragati Johri," An Improved Inverted LSB Image Steganography", in International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), IEEE, pp. 749-755, 2014.

[18] A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, S. Mathur, and A.Ingle, "Computational intelligence based intrusion detection systems for wireless communication &pervasive computing networks," in International Conference on Computational Intelligence& Computing Research, IEEE, pp. 1-7, 2013.

[19] B.Vasantha Lakshmi and B. Vidheya Raju, "FPGA Implementation of Lifting DWT based LSB Steganography using Micro Blaze Processor ", in International Journal ofComputer Trends and Technology pp. 6-14, 2013.

[20] S. Guicheng and Y. Zhen, "Application of Elliptic Curve Cryptography in Node Authentication of Internet of Things," in Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, pp. 452-455, 2013

[21] Zeng Bohan, Wang Xu, Zhou Kaili, and Zhao Xueyaun, "Encryption Node Design in Internet of Things Based on Fingerprint Features and CC2530," in International Conference on Green Computing and Communications, IEEE Internet of Things and Cyber, Physical and Social Computing, IEEE, pp. 1454-1457, 2013.

[22] Nitin B Naik and Mrs. Archana Nitin Naik,"Stegnographic Secure Data Communication Using Zigbee", inInternational Journal of Research in Science And Technology, 2015

[23] M. J. Covington and R. Carskadden, "Threat implications of the internet of things," in 5th International Conference on Cyber Conflict, pp. 1-12, 2013.

[24] T. Bhattasali, "LICRYPT: Lightweight Cryptography Technique for Securing Smart Objects in Internet of Things Environment." Article in CSI Communications, pp. 26-36, May 2013.

[25] Masanobu Katagi and Shiho Moriai,"Lightweight cryptography for the internet of things," Sony Corporation, pp. 7-10, 2008.

[26] R. Watro, D. Kong, S.-f. Cuti, C. Gardiner, C. Lynn and P. Kruus,"TinyPK: securing sensor networks with public key technology," in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 59-64, 2004