American Journal of Agricultural Science, Engineering and Technology

TRAFFIC CONTROL PATCHING AND SECURITY SOLUTION IN IOT

Afridi Shahid[1], Md. Alam Hossain[1*], Nazmul Hossain[1]

ABSTRACT

After connecting multiple devices to a network and possessing data analysis and excerpting, the IoT is awaited to contribute to the formation of new customer value. Critical infrastructure that gets into people's lives and economic deeds will also become an area, in which way the IoT is used, so security measures for IoT systems are very important. On the other hand, a dramatic increase in the number of connected devices will create technical problems such as attacks with a broader scope of influence and attacks that last longer. So, a shortage of security operations administrators will also be a problem. The internet of things refers to a way of connecting objects to the Internet for the purpose of intelligent control and management. The objects are sensed through RFID (Radio-frequency identification) or sensors achieving the integration of human society and the information system. RFID is the core technology to implement the internet of things. So the security issue of RFID is becoming more and more important, in the past decade, a large number of research papers dealing with security issues of RFID technology have appeared. This paper deals with the security of data of RFID as IoT devices and defence against malware attacks, and DDoS attacks in IoT systems.

Keywords: Security, Privacy, Cryptographic Hardware, IoT, System on Chip, Embedded Systems, RFID

[1] Department of Computer Science and Engineering, Jashore University of Science and Technology (JUST), Bangladesh

* Corresponding Author: E-mail: alam@just.edu.bd

INTRODUCTION

Internet Technology (IT) is very pervasive today. The number of digital devices connected to the Internet, those with a digital identity, is rapidly increasing day by day. With the developments in the technology, Internet of Things (IoT) become important part of human life. However, it is not well defined and secure. Now, various security issues are considered as major problem for a full-fledged IoT environment. There exists a lot of security challenges with the proposed architectures and the technologies which make the backbone of the Internet of Things. Some efficient and promising security mechanisms have been developed to secure the IoT environment, however, there is a lot to do. The challenges are ever rising and the solutions have to be ever elevating

Literature summarized the security issues in the internet of things based on RFID, literature paid attention to the privacy models for RFID, literature explained mobile RFID network based on EPC and analyzed threats of the mobile RFID system, this is important to create a secure IOT architecture, literature analyzed RFID technology and its Applications in Internet of Things (IOT) from different layers, In this paper, we will first introduce the IOT based on RFID

then we analyze the security issues in the IOT based on RFID , and on the basis of these, we will give the current countermeasures for the security of RFID data and malware attacks..

RFID SYSTEM WORKING PRINCIPLES

a. System Composition

As per various applications, RFID frameworks maybe vary from one another on creation components. However, fundamentally, RFID framework is formed by tag, peruser and information trade and the executives framework. Electronic tag is created by coupling part and chip containing security rationale.

b. Working Principle

As a serious programmed recognizable proof innovation, RFID actualizes non-contact full duplex information interchanges through RF to get target things distinguished. RFID label comprises of chip and radio wire and each label highlights exceptional item code.

RFID framework can communicate information among transponder and sensor handset. The accompanying figure shows working guideline of RFID framework.

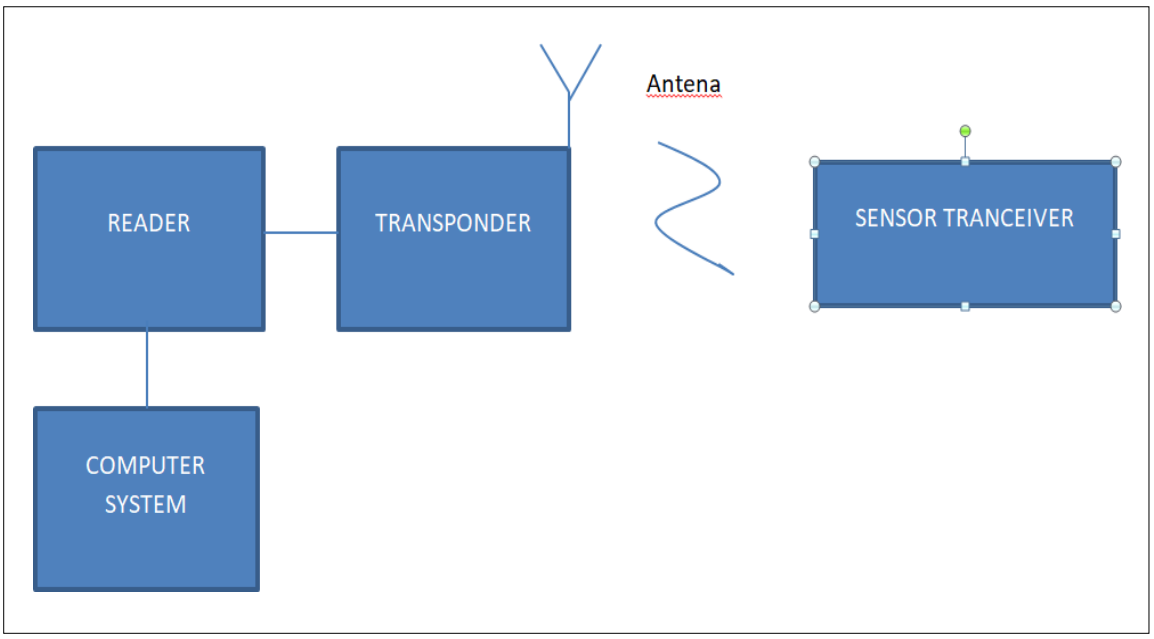


Figure 1: RFID working principle

When RFID framework is working, RF signals with a specific recurrence are initial communicated by peruser through recieving wire. As RFID label enters peruser's working field, the recieving wire will communicate actuated current so that RFID label will catch vitality that will be enacted to send their own code data to peruser. With regards to inactive frameworks, peruser will communicate RF signals at a specific recurrence through coupling segments. When RFID enters this field, vitality will be gotten through coupling segments to drive chips and peruser for correspondences. After peruser peruses self-coded data, it'll send it to information trade and the board framework. With regards to dynamic framework, after label enters peruser working region, installed battery will flexibly control so as to finish correspondences with peruser.

THE INTERNET OF THINGS BASED ON RFID

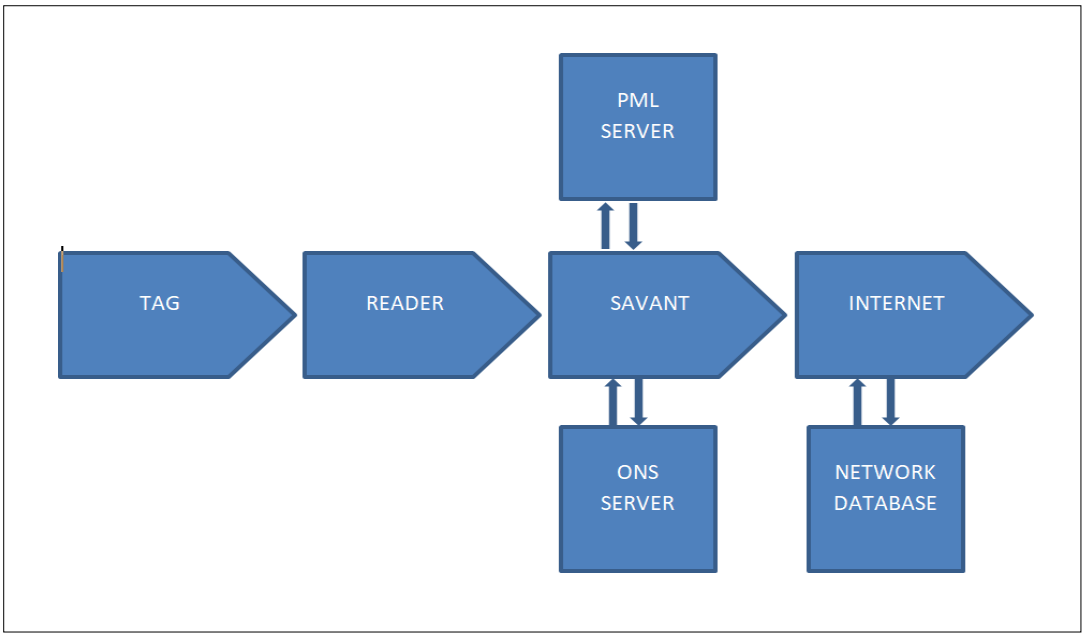


Figure 2: Structure of IOT

In the web of things dependent on RFID, RFID peruser is liable for gathering through this EPC code the middleware framework can discover relating IP address from the ONS foundation on the web, consequently the important data of the article can be gotten from this location. At that point the middleware framework (Savant framework) can measure and deal with the data. In this cycle there are neighborhood ONS worker, nearby PML worker and far off PML worker which are responsible for information stockpiling, as appeared in the Figure 2.

SECURITY ISSUES

Correspondence security treats

a) Wireless correspondence chances In RFID framework remote correspondence is received between the RFID perusers and RFID labels. Because of the receptiveness of the remote signs, it is simple for an assailant to look, capture, screen, and jam remote correspondence signals. So encryption and confirmation are expected to secure the remote transmission between the RFID perusers and RFID labels.

b) Wired correspondence hazards Between the RFID perusers and the middleware framework, information transmission is through the web. Much the same as customary organization association, a sequential of safety efforts will be received for guaranteeing the information classification and honesty, and the typical organization association.

c) Denial of Service (DOS) In both of remote and wired correspondence, there are Denial of Service (DOS) . When assailants control countless phony perusers and labels, they can make the information

d) Network Evasdropping

Organization listening in is an organization layer assault that centers around catching little bundles from the organization communicated by different PCs and perusing the information content looking for a data. This sort of organization assault is commonly one of the best as an absence of encryption administrations are utilized

Table 1: Security target and Solution

Security target		Security Solution
IoT devices	Privacy protection	Blocking
	Anti-interference	Data coding Data coding and data integrity
Communication process	Wireless communication risks(search, intercept, monitor, and jam wireless communication signals)	the openness of the wireless signals
	wired communication risks	The openness of the internet
	Denial of Service (DOS)	Malicious attackers
	Network Eavesdropping	Encryption

EXISTING SYSTEM

System 1: The card was read by the reader. The read information was encrypted by our encrypted software and this information will save to the cloud memory. When the raw information was needed, then only the administrator, who knew the decrypted private key could get the original information. As a result, the information of the card could not be theft through an unauthenticated person. Beside no one could duplicate the card and the authenticated card holder remains save from social engineering attack. It also helped the administrator that the information will save in the cloud memory with instant time. So administrator calculates the number of the uses of the card with exact time. DES algorithm is used in this system. The procedere of methodology are depicted as follows.

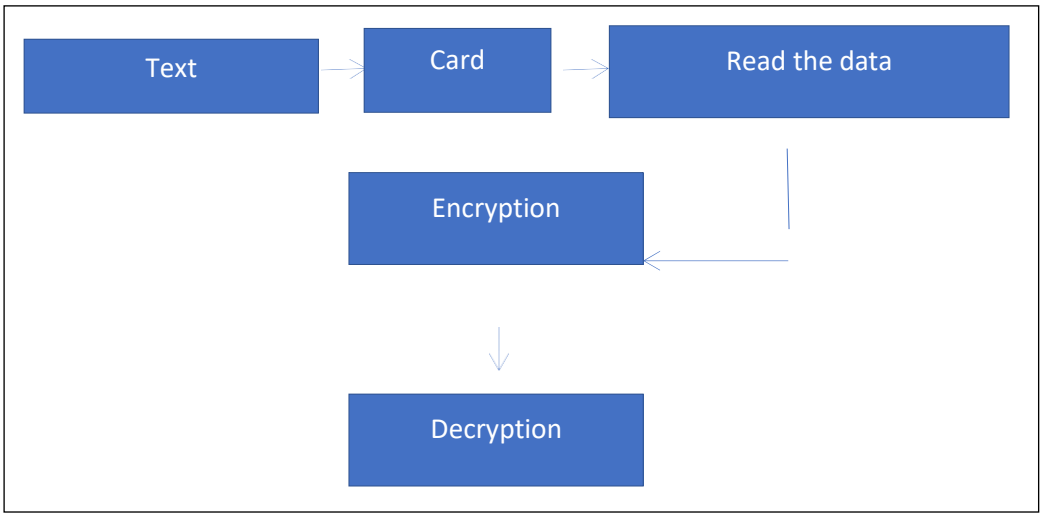


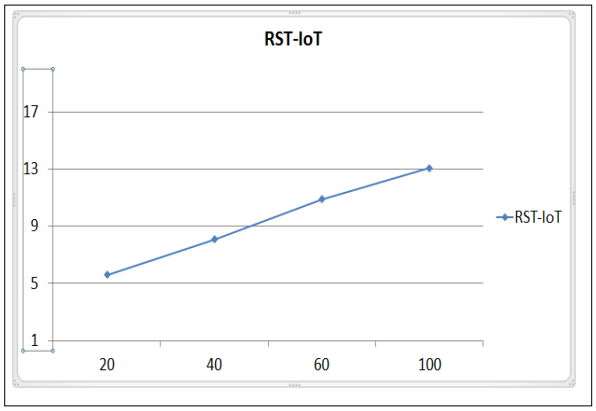
Figure 3: DES algorithm

This previous methodology could give the new technology some important security related in IOT. But it was unable to give the strong security that today's life need, because of the popularities of IOT. Besides this technology left the discussion of traffic control of data which has a major impact in encryption and decryption system.

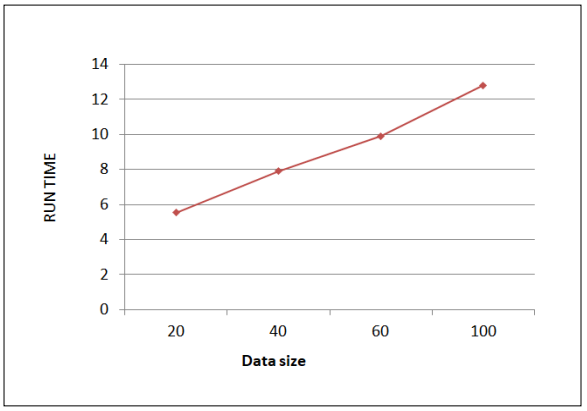
In this paper, those problems are tried to solve through acceptable performances.

System 2: There are some iot data transfer algorithm was introduced in past such as RST-IoT HCT-IoT .These algorithms are based on spanning tree theory**.**

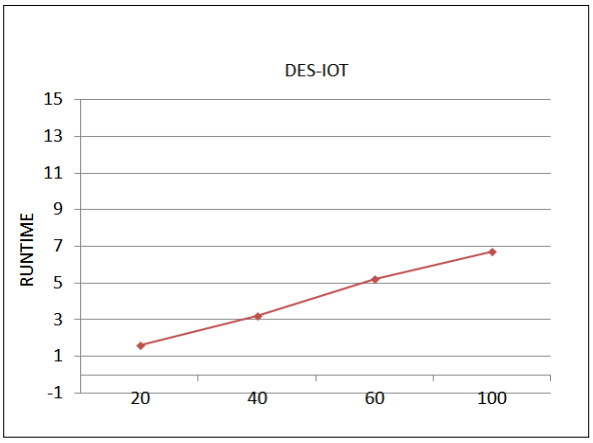
Number of devices	Avrg. Data Size (KB)	RST-IoT	HCT-IoT	DES-IoT
20	512	5.6	5.53	1.6
40	1024	8.1	7.9	3.2
60	2048	10.9	9.9	5.2
100	3072	13.1	12.8	6.7



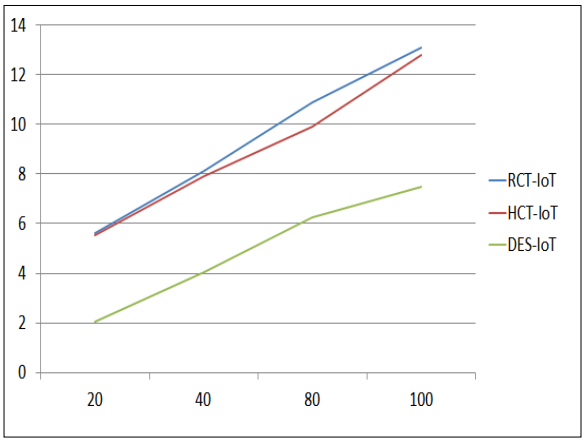
RST-IoT



HCT- IoT



DES-IoT



Comparison all IoT

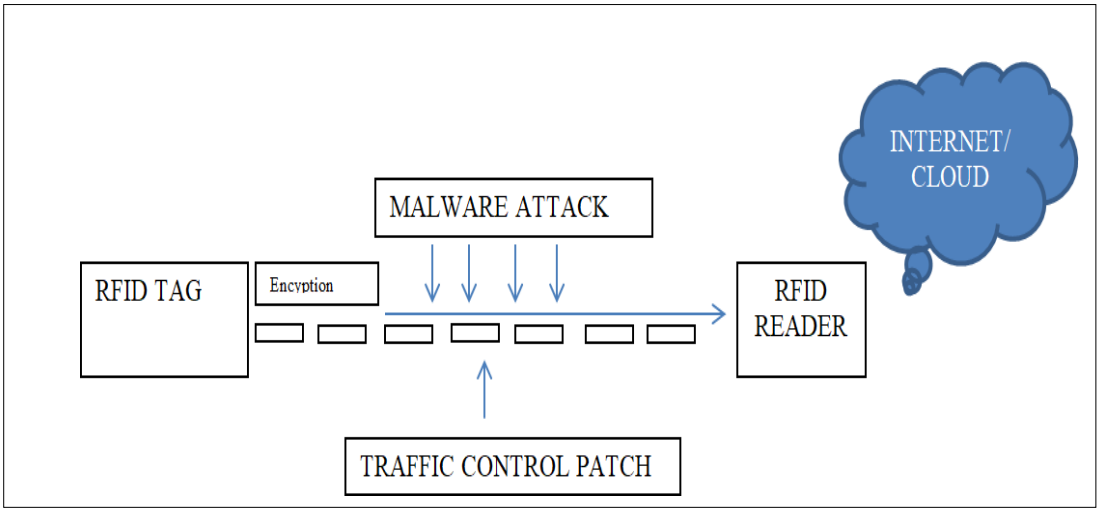


Figure 4: spanning tree theory

METHODOLOGY

When data transfer from RFID tag to destination, at first data will be encrypted for defending data cloning and eavesdropping attack. Secondly, different malicious attacks will took place at data passing time are generated by intermediate nodes could be blocked by TCP algorithm. It also control the data traffic or jam to reach the destination

TRAFFIC CONTROL PATCH

Algorithm

Here Tpr= packet pass runtime, t= present time, AP= Access point, If Tpr>t

Then select malware, generated by intermediate node in descending order based on its power by patched intermediate node (Pin)

And blocked them in run time

Else if Tpr<t

No action is needed

When Tpr=t

Always check the AP to control the traffic

Calculation 1 portrays the nitty gritty strides in fixing stage. With restricted assets and endeavors, the administrator could give a fixed measure of patches on the halfway hubs (e.g., p rate). To ease the spread from the framework connects, the Pin most significant middle hubs will be chosen for fixing. It resembles to securing the most significant hub to keep up network power . Subsequently, we present the traffic checking span for assessing the significance

of fixed halfway hubs. From the observed outcomes, the proposed traffic-control fixing plan sorts the malware in plunging request as per the intensity of traffic volumes, and the top moderate hubs are fixed.

Self-evident, the proposed volume-based fixing is powerful to the assault which produces countless traffic , e.g., DDoS assaults. The fixed middle of the road hubs could forestall the redirection of malignant traffic presented by the DdoS assault dispatched by the IoT botnets. Finally the passage are likewise consistently checked all through the run time for making sure about information passing.

Table 2: Performance Evaluation

Number of devices	Data size(KB)	Execution Time (Per Device)
20	512	1.6 sec
40	1024	3.2 sec
60	2048	5.2 sec
100	3072	6.7 sec

ACHITECTURE

An architecture was created in a simulation software (securicad) to implement the proposed network.system.Here, I use a router as an IOT device. The simulation design is given below

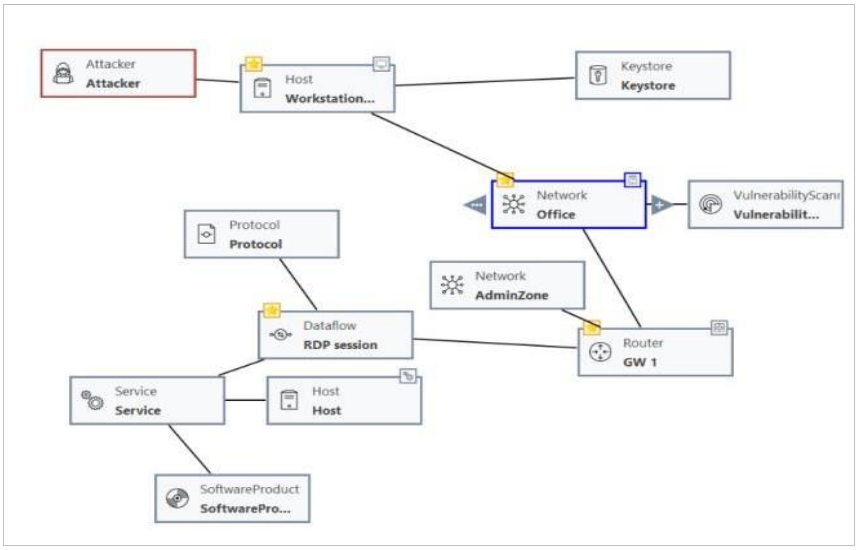


Figure 5: Simulation designed in securicad

RESULT ANALYSIS

Here necessary security steps are taken against the attack such as- DDoS, Eavesdropping, IoT device blocking, Bypass antimalware, ARP Cache Poisoning, DNS Spoof, Find Exploit etc. The output result is given below-

Table 3: Security steps against attacks

Name	Attack step	Risk probability	Risk
Network	ARP cash poisioning	0%	No
Network	DNS spoof	0%	No
Network	DoS	75%	Medium
Router	DoS	0%	No
Host	Bypass Antimalware	1%	No
Host	DoS	0%	No
Host	Find Exploit	0%	No
Dataflow	Eavesdrop	0%	No

Comparison with existing system

Conparison can be divided into two parts. i) Malware attack ii) Execution time

Malware Attack

Previous system prevented only data cloning attack but this methodology prevent other major attacks such as DDoS, Eavesdropping, IoT device blocking, Bypass antimalware, ARP Cache Poisoning, DNS Spoof, Find Exploit etc.

Table 4: Comparison by attack

Existing System	**Proposed system**
Data Cloning	DDoS,
Card cloning	Eavesdropping
Social engineering attacks	IoT device blocking
	Bypass antimalware
	DNS Spoof
	Find Exploit

Execution time: 256 KB, 512 KB, 1 MB, 2 MB,3 MB sizes are taken of data with different number of devices at a single time and find the comparison given below

Table 5: Comparison by execution time

Data size(KB)	Execution Time DES-IoT (Per Device)	Data size(KB)	Poroposed system's Execution Time (Per Device)
512	2.05	512	1.6 sec
1024	4.05	1024	3.2 sec
2048	6.25	2048	5.2 sec
3072	7.5	3072	6.7 sec

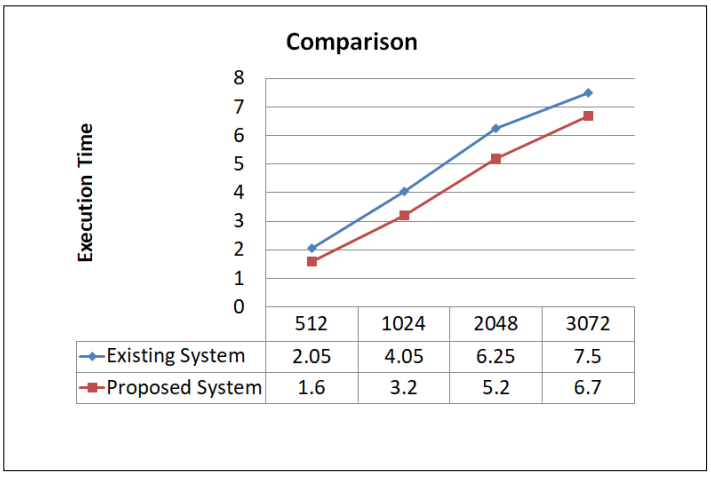


Figure 6: Comparison with existing method

Above comparison, with security attack and execution time the proposed system shows better feedback than existing. Besides it helps to minimize the data traffic by given algorithm. This proposed system creates a new era to IOT, giving combination among encryption, defend malware attacks and traffic control.

CONCLUSION

The IOT utilizes an assortment of data detecting ID gadget and data preparing hardware, for example, RFID, WSN, GPRS, and so on consolidating with the Internet to shape a broad organization so as to informationize and intelligentize the substances or articles. This paper dissects the applications and difficulties of RFID innovation, which is the significant and primary part of IOT.

REFERENCES

An ontology-based context model for wireless sensor network (WSN) management in the Internet of Things. *Journal of Sensor and Actuator Networks*, 2(4), pp.653-674. 40. Al-Turjman, F. and Malekloo, A., 2019.

An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. *IEEE Internet of Things Journal*, 5(5), pp.3758-3773.

Benaissa, S., Plets, D., Tanghe, E., Trogh, J., Martens, L., Vandaele, L., Verloock, L., Tuyttens, F.A.M., Sonck, B. and Joseph, W., 2017.

Brown, Eric (13 September 2016). "*Who Needs the Internet of Things?*". Linux.com. Retrieved 23 October 2016.

Dr. S. S. Manikandasaran, 2016,"*Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage*" (IJCSITS),

E. Ronen and A. Shamir, "*Extended Functionality Attacks on IoT Devices: The Case Of Smart Lights*", Proc. IEEE S&P Europe 2016, Mar. 2016.

Floerkemeier, C., Roduner, C. and Lampe, M., 2007. RFID application development with the Accada middleware platform. *IEEE Systems Journal*, 1(2), pp.82-94. Liu, Y., Seet, B.C. and Al-Anbuky, A., 2013.

"Internet of Things: Science Fiction or Business Fact?" (PDF). *Harvard Business Review*. November 2014. Retrieved 23 October 2016.

Internet of animals: characterisation of LoRa sub-GHz off-body wireless channel in dairy barns. Electronics Letters, 53(18), pp.1281-1283. 43. García-Lesta, D., Cabello, D., Ferro, E., López, P. and Brea, V.M., 2017.

IOT for smart farm: A case study of the Lingzhi mushroom farm at Maejo University. In 2017 14th *International Joint Conference on Computer Science and Software Engineering (JCSSE)* (pp. 1-6). IEEE. 45. Viani, F., Bertolli, M., Salucci, M. and Polo, A., 2017.

J. Granjal, E. Monteiro and J. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues*", IEEE Commun. Surveys & Tutorials*, vol. 17, pp. 1294-1312, July 2015.

Low-cost wireless monitoring and decision support for water saving in agriculture. *IEEE Sensors Journal*, 17(13), pp.4299-4309.

M. Miettinen et al., *IoT Sentinel*: Automated Device-Type Identification for Security Enforcement in IoT, CoRR, 2016.

P.-Y. Chen et al., "Decapitation via Digital Epidemics: A Bio-Inspired Transmissive Attack", *IEEE Commun. Mag*., vol. 54, no. 6, pp. 75-81, June 2016.

P.-Y. Chen, S.-M. Cheng and K.-C. Chen, "Optimal Control of Epidemic Information Dissemination over Networks", *IEEE Trans. Cybernetics*, vol. 44, no. 12, pp. 2316-28, Dec. 2014.

P. Wang et al., "*Understanding the Spreading Patterns of Mobile Phone Viruses*", Science, vol. 324, no. 5930, pp. 1071-75, May 2009.

P.-Y. Chen et al., "Decapitation via Digital Epidemics: A Bio-Inspired Transmissive Attack", *IEEE Commun. Mag*., vol. 54, no. 6, pp. 75-81, June 2016.

P.-Y. Chen et al., "Decapitation via Digital Epidemics: A Bio-Inspired Transmissive Attack", *IEEE Commun. Mag*., vol. 54, no. 6, pp. 75-81, June 2016.

R Khan,2012,*Future Internet*: The Internet of Things Architecture,Possible Applications and Key Challenges,

S. Babar,2011,Proposed Embedded Security Framework for Internet of Things (IoT), 978-1-4577-0787-2/11/$26.00 2011 IEEE

S. Tanachaiwiwat and A. Helmy, "*Encounter-Based Worms: Analysis and Defense*", Ad Hoc Net., vol. 7, no. 7, pp. 1414-30, Sept. 2009.

Smart parking in IoT-enabled cities: A survey. *Sustainable Cities and Society*, p.101608. 41. Elijah, O., Rahman, T.A., Orikumhi, I., Leow, C.Y. and Hindia, M.N., 2018.

Springer International Publishing AG 2017G. *Wang et al. (Eds.):* SpaCCS 2017 Workshops, LNCS 10658, pp. 607–616, 2017.

Wireless sensor network with perpetual motes for terrestrial snail activity monitoring. *IEEE Sensors Journal*, 17(15), pp.5008-5015. 44. Chieochan, O., Saokaew, A. and Boonchieng, E., 2017, July.