A Survey:

Prospects of Internet of Things (IoT) Using Cryptography Based on its Subsequent Challenges

Dhruvi Mewada[1,*], Nidhi Dave[2], Prof.Rohan Kumar Prajapati[3]
Department of Information Technology
Gandhinagar Institute of Technology
Gandhinagar, India
*Contact: dhruvimewada28@gmail.com, phone +91-99-09-147 4 12
*Contact: nidhidave1504@gmail.com, phone +91-98-79-79 2307
Contact: prajapatirohanc@gmail.com, phone +91-90-33-72 2304

Abstract—**In Today's era of information data plays vital role in communication, Security has been a ponderous affair for the professionals in any field. Security is not about only protection of assets but privacy and authority to access in legitimate terms too. Cryptography provides the functionality that protects and secures the data through its encryption algorithms and authentication to its end users. IoT has been most attractive topic/area in recent era. Privacy and security is an inseparable part of this technology. Which could affect in multi fold, so, the paper majorly focuses on four major challenges involving Security, Privacy, Compatibility and Connectivity of IOT and apprehension of IoT with its provided solution of using cryptographic algorithms.**

Keywords: - IoT, Data, Security, Privacy, Crypto graphical Algorithms, Authentication, Encryption, Compatibility, Connectivity.

Introduction

The fundamental of the Internet of Things (IoT) is the indication of every device merging with the presence of human beings. This means devices become an inseparable part of our daily routine. The victorious implementation of IoT involves consideration of huge number of aspects such as security and privacy. As the Internet of Things (IoT) has becoming more and more demanding various security issues come into consideration. So here comes the need of securing the data by means of crypto graphical algorithms. Cryptography is defined as "secret writing" which transforms the message and protects the data from the unauthorized user. The secret writing is called "cipher text". Different cryptographic algorithms are involved for security and privacy of Internet of Things. Cryptography ensures that the contents of message are confidential. In spite of using the efficient algorithms for security and privacy of data, the data are not fully secured and confidential. If the message is confidential then it may be intercepted and read by hackers.

The new invention of Internet of Things i.e. IPv6 will connect millions of devices and which breaks the limitation of IPv4 and will change the world of Information Technology by its unlimited connection establishment. The main process involving in cryptography is shown in below figure.

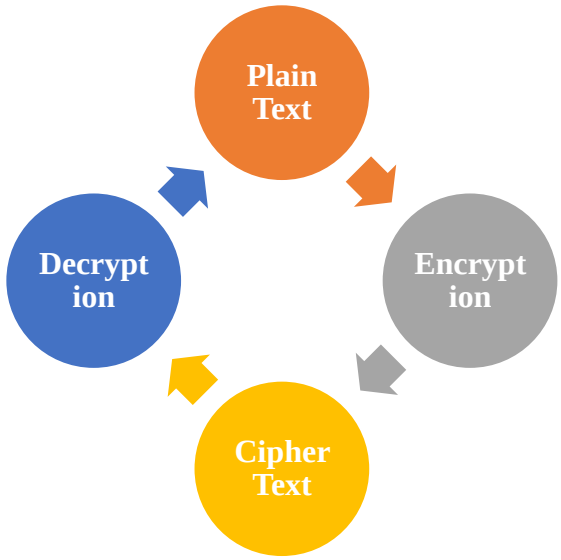

Fig:-1 Main Process involved in Cryptography

The amount of efforts necessary to discover, test, and install a new algorithm every time has become tedious and inefficient. Security issues of Internet of Things involves technological, ethical and privacy concerns. Internet of Things requires architectural solution that can manage heterogeneous states in order to work efficiently and effectively.

Now the paper discusses the survey of various IoT inventions and its drawbacks, provided with its accuracy and challenges focusing on its four major pillars namely **M2M**-, Machine-to-Machine Communication, **RFID**-Radio Frequency Identification, **WSN**-Wireless Sensor Networks and **SCADA**- Supervisory control and Data Acquisition. Internet of Things is becoming an integrated part of future internet world. So, the paper depicts the survey of Internet of Things technologies along with its securities and focuses mainly on the challenges faced by Internet of Things by using cryptography. As security issues prevails, cryptography comes into consideration. Designing a unified view of Internet of Things is difficult as it involves a wide range of applications. But a rough design can made of the structure or architecture of Internet of Things. The IoT devices

are typically thought of as "smart devices" which make work easier and quicker. An important development that showed the way for Internet of Things is the keenly and economically available computing power brought on by the present level.

Privacy Strategy

A subscriber can access the requested event only if the attributes match. This clearly means that hackers follow predefined protocols. Various techniques are available through which hackers decrypt the code and gain the desired information they want. IPsec (IP security) which is a security protocol which offers end-to-end security with authentication. By working at the network layer, it can be used with any transport layer protocol. IPsec is one of the most suitable options for E2E (End to End) security. As this era is of digitalization, privacy and security comes into consideration. Many security protocols are available nowadays and one of them is WirelessHART. All traffic is secured, the data is encrypted and all messages are authenticated. WirelessHART is a bidirectional network of relatively powerful devices and has a central network manager. The network designers and device vendors have conflicts regarding the complete security architecture of the WirelessHART. A set of different security keys are used to safeguard secure communication.

Academic Survey

As portrayed in introduction cryptography is method of protecting data and network transmission over wireless networks. Internet of Things is the most emerging topic for rising generation and nowadays Internet of Things also has major security issues and many emerging challenges. Security, Privacy and confidentiality has gain traction in today's era. A survey regarding the technology issues has been done and the most common part that we found was the security issues that each of them was facing. Nowadays technology has become lifeline of our daily routine and as it is a lifeline for all of us its security and maintenance becomes an important issue for all of us. Information security is the most significant issue in providing safe transmission of data. Also security issues are now becoming significant as we are moving towards digitalized era. As more and more users associate with the internet, security comes into consideration. We need more efficient algorithms to solve the privacy issues.

Table of Survey

Sr. No	Author's Name	Fundamental concepts	Disadvantage	Interpretation
1	J. Byun, S. Kim, J. Sa, S. Kim, and Y. Shin, vol. 129, pp. 209–212, 2016. [1]	To connect more than 260 million objects according to Gartner cycle.	Focused on Smart cities, industries.	Pivoted on the functions and features of IoT.
2	E. Bertino and W. Lafayette pp. 18–20, 2016. [2]	Pre-owned algorithms used in IoT such as AES, DES Blowfish etc.	Despite of such algorithms still the security issue prevails.	Focused on Security and Privacy Issues
3	T. Borgohain, pp. 1–7.[3]	First to secure the statics of IoT and then implant Future work.	There is no infusion of the statics of IoT.	Majorly focused on Security Issues of IoT.
4	J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle [4]	Contemplate the traits of IoT to connect the enormous devices.	Fails to secure the personal data of the users.	Emphasized on the solutions of IoT.
5	N. Aleisa and K. Renaud, pp. 1–10, 2004.[5]	Majorly focused on the extended review of the security of IoT.	Still lacks some important measures.	Overview of the future of the IoT security.
6	C. Zou, E. Engineers, and Z. Caufeng, March 2015, 2012.[6]	Paper reviewed on the challenges of IoT security.	Data is not secured.	Implemented and reviewed on IoT security for future world.
7	H. Kaur, V. Verma, and J. Mishra, pp. 129–136 [7]	Extremely pivoted on the different cryptographic algorithms.	Algorithms are already used in data security of IoT.	Uses AES algorithm in which future we can store the data and get the modifications.
8	K. Lam and C. Chi, vol. 1, pp. 18–26, 2016. [8]	Relates the challenges and provides the opportunities to solve the problems of IoT.	Not all the major issues are solved.	Gives the solutions of some of the problems of IoT security.
9	IoT Security Solutions. [9]	Describes the hardware as well as software detail of IoT.	Only overview of IoT is given.	Core part is the IoT security and its authentication.
10	T. Yousuf, R. Mahmoud, F. Aloul, and I. Zualkernan, vol.	Depicts the security issues prevailing in each and every layer.	The cyber-attacks are still prevailing.	Concludes the paper describing the future work done for securing IoT.

	5, no. 4, pp. 608–616, 2015. [10]			
11	R. Jain, pp. 1–15. [11]	A brief definition of IoT and then we will go further through more details about the current challenges of IoT.	No algorithms are used in the paper.	IoT needs to be widespread with tremendous amount of users.
12	Z. Quan, T. Chunming, Z. Xianghan, and R. Chunming, 2015. [12]	It recommends a secure user authentication protocol.	It is secured but up to some limitations.	The protocol is more appropriate to open and higher security.
13	L. Duan, Y. Zhang, S. Chen, S. Wang, B. Cheng, and J. Chen, Springer plus, 2016. [13]	The main concept is to use a two layer cooperating method to match bi-directional privacy.	Reasonable overheads are prevailing.	Future research is to make the policy implanting scheme.
14	D. Sey 2018.[14]	This paper gives a detailed study of Cryptography Techniques.	No new algorithm techniques are used.	It was concluded that Blowfish has good performance than other algorithms.
15	S. Tayal, N. Gupta, and P. Gupta, vol. 10, no. 5, pp. 763–770, 2017. [15]	This survey focuses on authentication methods for the Internet of Things (IoT).	No drawback found.	This survey has covered a wide areas of IoT which is very useful.
16	T. Borgohain, pp. 1–7. [16]	Information security is the most basic issue in providing safe transmission.	No drawback found.	This paper quickly presents the idea of PC security,

Future Work

As it is the era of digitization and information technology plays a vital role in our routine days. Internet of Things has been an emerging topic for everyone including researchers and hackers. As it is an emerging topic security has been a major concern for every technology. Although using the most efficient algorithms, security and privacy issues still prevails. So after the survey of papers we found that security and privacy are the biggest challenges of Internet of Things. We shall try our best to overcome the security challenges of Internet of Things using cryptographic algorithms. As the basic cryptographic algorithms are also not able to provide proper security as the system is updating day by day so we need higher and more efficient algorithms to provide security to our devices.

Conclusion

It is been concluded here that security is very ponderous and it is an inseparable part of every technology. Now a day's security is essential in each and every quarter. Internet of Things has a tremendous future for over upcoming 10 years but the main problem is its security. Here is survey of the IoT challenges and its issues by manipulating the cryptographic algorithms. In near future Internet of Things is going to be the most emerging technology and so security issues need to be solved quickly and rapidly.

References

[1] J. Byun, S. Kim, J. Sa, S. Kim, and Y. Shin, "Smart City Implementation Models Based on IoT Technology Smart City Implementation Models based on IoT," vol. 129, pp. 209–212, 2016.

[2] E. Bertino and W. Lafayette, "Data Security and Privacy in the IoT," pp. 18–20, 2016.

[3] T. Borgohain, "Survey of Security and Privacy Issues of Internet of Things," pp. 1–7.

[4] . J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: Threats and Challenges," no. i.

[5] N. Aleisa and K. Renaud, "Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion)," pp. 1–10, 2004.

[6] C. Zou, E. Engineers, and Z. Caufeng, "Security in the Internet of Things: A Review Security in the Internet of Things: A Review," no. March 2015, 2012.

[7] H. Kaur, V. Verma, and J. Mishra, "Survey Paper cryptography", pp 129-136.

[8] K. Lam and C. Chi, "Identity in the Internet-of-Things (IoT): New Challenges and Opportunities," vol. 1, pp. 18– 26, 2016.

[9] "IOT SECURITY SOLUTIONS White paper".

[10] T. Yousuf, R. Mahmoud, F. Aloul, and I. Zualkernan, vol. 5, no. 4, pp. 608–616, 2015. [10]

[11] R. Jain, "IoT Security: A Survey Abstract:" pp. 1–15.

[12] Z. Quan, T. Chunming, Z. Xianghan, and R. Chunming, "A secure user authentication protocol for sensor network in data capturing," 2015.

[13] L. Duan, Y. Zhang, S. Chen, S. Wang, B. Cheng, and J. Chen, "Realizing IoT service's policy privacy over publish / subscribe - based middleware," Springer plus, 2016.

[14] D. Sey, "A survey on authentication methods for the Internet of Things," 2018.

[15] S. Tayal, N. Gupta, and P. Gupta, "A Review paper on Network Security and Cryptography," vol. 10, no. 5, pp. 763–770, 2017.

[16] T. Borgohain, "Survey of Security and Privacy Issues of Internet of Things," pp. 1–7 .