IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 5, Ver. IV (Sep.- Oct. 2017), PP 61-65
www.iosrjournals.org

The study of computational fuzzy extractor for providing security to IOT nodes

Prof. Pragati .Mahale ,Ms. Sonali Alwani, Ms. Vaishnavi Borade,
Ms. Shreya.Dhanbar, Ms. Pooja Suvarnakhandi
Dept. of Information Technology AISSM's IOIT,PUNE

Abstract: *With the increase in the usage over the internet over the globe ,the security regarding the confidentiality of the data that is being transferred and received while Internet is being used is the area of major concern. In the recent years, the increase in the use and development in IoT has made it necessary to facilitate keys storage that is cost efficient. The traditional methods that were used before ,proved to be expensive for key storage. An alternative solution for cost minimization, keys were being generated using the noisy entropy. The keys could be secured and made cost efficient when bounded with fuzzy extractor which also made the keys strong cryptographically. To balance the entropy loss at the time of key extraction process, the theoretical fuzzy extractors needed a enormous range of input entropy. According to the study proposed in Fuller et al the entropy loss can be minimized with the study of error problems.The server device authentication could be made more scalable and robust by using the Computational Fuzzy Extractor.The paper focuses on storage,efficiency and entropy loss and we are using lossless Computational Fuzzy Extractor,where the entropy key and the source entropy are equal to one another other.The proposed system shows how device server authentication can be provided, also we compare our work with already in use system in used on the basis of security where we are exacting to achieve zero entropy loss.*

Keywords: *IoT (internet of things),CFE(computational Fuzzy Extractor),PUF(Physical Unclonable Function),LWE(Learning with Errors),TRG(True Random Generator) Introduction*

Date of Submission: 07-10-2017 Date of acceptance: 27-10-2017

I. Introduction

Internet of things has facilitated in connecting machines to one another using the internet to represent the material world into virtual set up. The advantage of the growth in the internet and its influence over our day-to-day is the force behind the huge improvement in Internet of Things(IoT).Sensors and the camera's used for security purpose are all a fragment of the IoT devices.Billions of IoT devices are connected for the purpose of sharing information,and because so many devices linked to each other and work simultaneously,security is the main concern to protect the data being transmited. It is mandatory to sent data to the intended user and also data being received is received from a authenticated person,also that data have no chance to be modified during the process or attacked by an adversary.

The proposed systems aims in implementing the utility of a low cost IoT node and also supports lightweight mutual authentication in post-quantum world provided by the corresponding system. The goal of different algorithms was to reduce the resource requirements and also the entropy that are required for the generation of the key. Post-quantum security serves as basis for computational fuzzy extractors and also based on learning with error problem .In the areas where the environment is very restricted ,our analysis show that the these schemes can be implemented .For showing the results of feasibility ,a random number generator is constructed for a restricted environment and the use of the algorithms that reduces the area that is required for the implantation of CFE. Our system is implemented on two node platform,that is in ultra-restricted devices and powerful node.

II. Literature Survey

1. **Internet of Things:Application and Challenges in Technology and Standardization.**
Authors:-Debasis Bandyopadhyay,Jaydip Sen.

The paper states the different applications of Internet of Things(IoT) and the challenges of deploying IoT nodes. The deployment of IoT has various important technologies such as Identification technology ,IoT archietecture Technology, Networking Technology,Communication Technology, Softwares and Algorithms,Hardware,Standardization,Security and privacy Technologies etc. For successful implementation of IoT network feasibility, security and privacy are important to be maintained.The proposed paper

addresses the data security in IoT that is one of the challenges to maintain privacy.

2) Reusable Cryptographic Fuzzy Extractors Authors:Xavier Boyen
The existing model of fuzzy extractors were not adequate as it
uses multiply same fuzzy secret.The system was demonstrated with number of simple attacks and balancing privacy,protection and data quality to reuse the same fuzzy secret.To control and maintain two security models that is fuzzy sketches and extractors that assign reusable secrets.The first model allowed adversary as outsider and the other model allowed as insider.The model were selected only on particular perturbation attack.

3) Robust Fuzzy Extractor and Authenticated Key Agreement from Close secrets
Author: Yevgeniy Dodis,Jonathan Katz,Leonid Reyzin and
Adam Smith.
The paper envisions, about using noisy data for the purpose of cryptography, where the random variables generated and reproduced are not identical but a lot close to each other.It also
focuses on using non-iterative protocols. Protecting the data
from passive attacks and Robust fuzzy extractor provides us a guarantee against such passive attacks.It also proposes how short secret key helps in achieving better parameter while constructing Robust Fuzzy extactor.

4) The Learning with errors Problem Authors: Oded Regev
The paper suggests that ,The learning with errors(LWE) provide the base for the model of cryptography.The main
element that make LWE desirable is its capacity for making the worst-case lattice problem hard.There are multiple of
algorithms that facilitate LWE such as Maximum Likelihood
algorithm,and also the algorithm stated by [1] Blum et al.The algorithm suggested in [1] is considered to best for the LWE problem.The complex LWE diffculties should be broken down to smaller parts to provide simplicity and that paves ways for cryptography.LWE is flexible and extremely versatile in nature that makes it more favourable for cryptographic construction.

5) Reverse Fuzzy Extractors:Enabling Lightweight Mutual Authentication for PUF-enabled RFIDs.
Authors: Anthony van Herrewege.
The paper describes the study which is focused on ,Mutual authentication which serves on the basis for PUF that is supported between the reader and the tokens of the RFID. Noise factor is present in the response that is received from PUF so we use a reverse fuzzy extractor that is used to remove the noise. The reverse fuzzy extractor is also used to provide authentication.The generate procedure and the reproduce procedure for the prover and the verifier are flipped by using the reverse fuzzy extractor.

6) Reusable Fuzzy Extractors for Low-Entropy Distribution
Authors : Ran Canetti ,Benjamin Fuller ,Omer Paneth ,Leonid Reyzin ,Adam Smith According to study of this paper, Fuzzy Extractor uses noisy parameter which is extracted from secret and convert into distributed key which is uniform in nature . They construct first Reusable Fuzzy extractor. For this construction they uses digital lockers, point Function and Hash Function. Digital lockers contain any information of the plain text from the cipher text which hard to guess by adversary .In Point Function is use for the large alphabets .It is same as digital lockers without plaintext. In proposed paper reusability is incorporated to advance and the security of computational Fuzzy extractor.

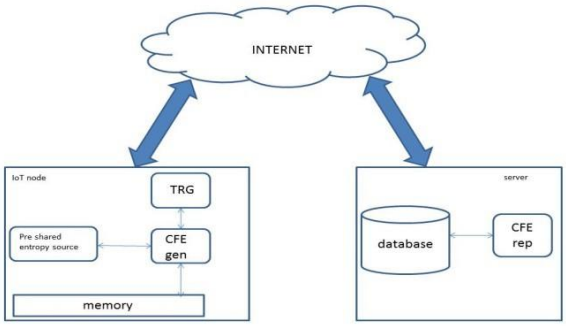
7) Attacking PUF-Based Pattern Matching Key Generators via Helper Data Manipulation.
Authors: Jeroen Delvaux,Ingrid Verbauwhede
This paper illustrates the model of PUF.PUF is accessible to calculate but crucial to conclude. PUF have a unique identification parameter,this parameter used for secret key but the result of PUF is not uniformly distributed to create high entropy keys. To overcome this drawback of non-uniformity this paper provides methodology of post-processing logic on the same parameter. To design to the fuzzy extractor the solution was parcel out with the noise which is generated from PUF.

8) Secure key generation from Biased PUF's
Authors: Roel Maes,Vincent van Der leest,Erik van der Sluis,Frans Willems According to the paper that has been studied, it shows the use of the code-offset method provide secure key generation,also that biased PUF's are possible,for the PUF's that are biased.There are many solutions that have been generated to prevent the entropy that are dealing with the noise generated through PUF. These noisy sources are in turn used for generating cryptographic keys that are mend to be secure.To supply a protected and an efficient way for protecting the non- volatile memories the PUF based key generation is adopted in the proposed system.

9) Ardrand :The Arduino as a Hardware Random-number Generator.
Authors: Benedikt Kristinsson
The study of this paper describes the increase in possibilities by using Arduino that is a type of TRNG. Randomness can be produced by making the use of TRNG ,whose source is not determined. It suggests that,there is no need of a hardware for its implementation.Freshness for each running protocol and volatile memory to store the intermediate values that are composed during the calculation is also being provided.

10) Fuzzy Extractors: How to generate Strong Keys from biometrics and other noisy data
Authors:-Yevgeniy Dodis ,Rafail ostrovsky leonid reyzin,adam smith The existing and secure techniques described how noisy information is turned into usable keys for cryptographic application and securely authenticating biometric data.
Cryptography depend on consistently provided random strings for its secret. Strings are not uniformly random not reproducible. The password authentication was described by cryptographic application where the problem of secret key in the pattern of noisy non-uniform data was described. The three models were discussed to modify and gain greater error- correction in models.

III. Proposed System Architecture



TRG:- TRG is free and also the Freshness of the system can be maintain through it. To generate numbers it uses a formula, Which behave like genuine random numbers, also they are commonly used for statistical methods and more for simulations of the random processes. A good pseudo-random number generator are used to work in most of the cases. As It's work seems like same as the Genuine random number generator. A true random number generator (hardware), is one of the piece of electronics which used to plugs into a computer so that it produces a genuine random numbers which opposed to the pseudo-random numbers, mostly this method is for amplifying the noise which is generated by a semi-conductor diode or resistor after that it is feed into a Schmitt trigger or comparator . If we take one of the sample of the output which is not too much quickly, As results we will get statistically independent series olf bits . This bits can be assembled into integers, bytes or floating point numbers.

CFE:- This CFE make system lossless. To derive keys from noisy measurements mostly the Fuzzy extractors (FE) is used. A Fuzzy extractors (FE) contain two procedures Gen and Rep .A public helper data generated by Gen from a measurement, from noisy measurement as well as helper data Rep tries to reproduce a shared secret. Here CFE used to derive longer keys compared to information-theoretical secure fuzzy extractors when input entropy remains the same at the cost of achieving only computational security. On LWE problem their construction is mostly based which is achieved by using variant LWE.

Reverse and Robust Fuzzy Extractor:- The secret is removed from public key by applying various computations, here public key is carried within data also in between the network where the data is going from source to destination the secret is generated and which is used to verify the users or node identity on server side which is hosted in the dynamic networks.

Generate Procedure:-In this the random variables are allowed to calculate the generate procedure efficiency so that the secret and encoding which is done to provide the security to adversary should be optimized in his path. The output of the TRG is measured element by element by using distribution of values which we have considered i.e if we consider xyz for TRG then the xyz computations are formed using the pseudo code of the GEN. It includes many sub process within it such modular reduction, multiplication Matrix etc. for authentication and enhancing it to a robust fuzzy extractor making secure against outsider chosen perturbation attacks.

The reverse fuzzy extractor effectively flips the Gen and Rep procedures for a prover and a verifier, here device and server respectively. Server used to transmits a challenge to the device holding a pre-shared entropy sources. Generate procedures and the Decode function are the two most useful and important algorithms is our system.

PUF:-A physical entity is a Physical unclonable function which embodied in physical structure easy for evaluate and hard to predict.PUF depend on thier physical unlikeness and these physical factors are unpredictable and uncontrollable which actually makes it different and doesnt duplicate with other clone.Using fuzzy extractor or key extractor puf concentrate a unique and strong cryptographic key.Different environmental variations like a temperature supply voltage affect the performance of PUF.PUF assure that if some how its used in any of the cryptographic application for key extraction then the output is stable and there also will be error correction.

Shared Entropy type 1)MD5:
Hashing function is also recognized as MD5. A hash value of 16 bytes is generated as well as 32 bit hexadecimal number.
MD5 hash function loses its properties during security.
Pentium 4 processor, within a second computer can detect collisions by collision attack, collision attack is generate the same hash value nothing but MD5 hash function is used for generating high entropy keys in fuzzy extractor.

2)SHA-1
Secure hash function is the clan of cryptographic hash functions which has a special branch of hash function also includes properties which make it relevant for adopt the methods in cryptography. Cryptographic hash functions have security applications, like digital signatures, MACs(message authentication codes) and further forms of authentication.SHA-1 is the 160 bit hash function and is part of digital signature algorithm.It has limited message size bits and output size is 160bits so called as 160bit hash function.

IV. Conclusion

We have studied how, client to client and client to server authentication can be provided using methodology such as, Computational Fuzzy Extractor, True Random Generator, Robust and Reverse Fuzzy Extractor and in turn provide zero entropy loss. The analysis done on the existing work, suggests that for lossless entropy ,Computational Fuzzy Extractor helped in achieving the objective rather than by using the theoretical Fuzzy Extractor. LWE methodology has been study and is observed to provide hard to crack and cryptographically strong keys used to data more secure. The designed system can be demonstrated to be more fast in data transmission with the use of ARM processor, as compared to the existing system. We also studied the methods to provide device and server authentication with adequate accuracy.

Reference

[1] A.Blum, A. (2003). "Noise-tolerant learning the parity problem and the statistical qyery model". *ACM(JACM) , 50*, 506-519.
[2] A.Van Herrewege, S.-R. (2012). "Reverse fuzzy Extractor:Enabling lightweight mutual authentication for puf-enabled rfids ". *Springer* , 374-389.
[3] B.Fuller, X. (2013). "Computaional Fuzzy Extractors". *Springer* , 174- 193.
[4] D.Bandyopadhyay, J. (2011). "Internet of things:Application and challenges in Technology and Standardization". *Springer , 58*, 49-69.
[5] D.Kristinsson. (2011). "Ardrand:The arduino as a hardware random- number generator".
[6] I.Delvaux, I. (2014). "Attacking puf-based pattern matching key generators via helper data manipulation". *CT-RSA* , 106-131.
[7] O.Regev. (2010). "The learning with errors problem". *CCC* .
[8] R.Maes, V. d. (2015). "Secure key generation from biased pufs". *CHES* , 517-534.
[9] Sen, D. B. (2011). "Internet of things: Applications and challenges in technology and standardization". *Springer , 58*, 49-69.
[10] X.Boyen. (2004). "Reusable cryptographic fuzzy extractor". *ACM* , 82- 91.
[11] Y. Dodis, R. O. (2008). "Fuzzy Extracters How to generate strong keys from biometrics and other noisy data". *SIAM , 38*, 97-139.
[12] Y.Dodis, B. K. (2012). "Rubust fuzzy extracters and authenticated key agreement from close secrets". *IEEE , 58*, 6207-6222.

Prof. Pragati .Mahale The study of computational fuzzy extractor for providing security to IOT nodes." IOSR Journal of Computer Engineering (IOSR-JCE), vol. 19, no. 5, 2017, pp. 61-65.