IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 84-89

Fingerprint Based Authentication of Internet of Things Users

Kalaivani S[1] Shalini Dhiman[2]
[1](Computer Science Department, Kathir College Of Engineering, India)
[2](Computer Science Department, Kathir College Of Engineering, India)

Abstract: *Internet of Things (IoT) can be seen as a pervasive network of networks: numerous heterogeneous entities both physical and virtual interconnected with any other entity or entities through unique addressing schemes, interacting with each other to provide/request all kinds of services. Given the enormous number of connected devices that are potentially vulnerable, highly significant risks emerge around the issues of security, privacy, and governance; calling into question the whole future of IoT. During the data exchange, it is mandatory to secure the messages between sender and receiver to handle the malicious human based attacks. The main problem during Fingerprint based approaches is the computational overhead due to large real numbers required for Fingerprint and verification processes. This paper presents a light weight Shortened Complex Digital Fingerprint Algorithm (SCDSA) for providing secure communication between smart devices in human centered IoT. We have used less extensive operations to achieve Fingerprint and verification processes like human beings do Fingerprints on legal documents and verify later as per witness. It enhances the security strength to guard against traffic analysis attacks.*

Keywords: *Confidentiality, Complex Numbers, Digital Fingerprint, Internet of Things*

I. Introduction

Internet is the largest public data network to facilitate social, military and commercial information exchange. In current era, Internet of Things (IoT) is getting a vastly growing interest due to its applicability in a wide range of innovative applications. IoT comprises of a large number of smart devices to share sensed data over internet to ultimately save at cloud repositories. Human centered IoT is an emerging area in every field of life, especially in business, online bank transaction, smart cards, healthcare, online correspondence and exchange of sensitive personal information [1][2]. A number of smart systems prefer the human intervention for initiating the automated tasks. A number of smart devices involve the social impact where the devices should be capable of transforming its functional model as per behavior of different human beings. It has boosted the growth of information exchange over the IoT and enabling networks. It includes cellular, vehicular and healthcare for human beings by supporting middleware [3]. However, the information exchanged in these applications is at risk due to fraudulent activists like hacking, viruses and individual or human error to change, duplicate or intercept the data. Due to this perception some questions arises that need proper attention. How secrecy can be maintained during transmission such that no human get unauthorized access to the information of transmitted message? How can the sender of the message ensure that the transmitted message exactly received by the intended recipient?

Digital Fingerprint Algorithm (DSA) has been used for transmission of electronic funds, interchange of data, distribution of software, storage of data Digital Fingerprint's security depends upon the private key of the signer. Digital Fingerprint consists of the Fingerprint generation and verification algorithms. Private Key of the signer is used for signing and Public key of the signatory is used to verify the Fingerprint by the recipient. Comparing with the physical Fingerprint, digital Fingerprint has the capability that, it cannot be changed nor copied by someone else, and also the signers of the Fingerprint cannot repudiate Fingerprint later. The process of Digital Fingerprint generation and verification is shown in figure 1 [5].

Digital Fingerprint are mainly applicable in following two scenarios. 1) Direct Digital Fingerprint Scheme where message is sensitive to the receiver, like Fingerprint on tax information, personal and business transactions are such type of situations in which user A signs a message and transmits to user B that can verify the Fingerprint or prove the Fingerprint validity to any other users. 2) Arbitrated Digital Fingerprint Scheme, the signed message firstly send to a trusted third party called arbiter to check the authenticity and integrity of that message. After complete verification it is forwarded to intended receiver [5]. An improved speed digital Fingerprint algorithm titled as "isDSA" that presents lightweight scheme where the complex modular inverse operation is eliminated. It uses modified *s* parameter of Fingerprint (r, s) by removing *w* component during verification. Moreover, the *u1* and *u2* sub-components used during verification are modified. It also pre-calculates and memorizes the redundant operations to improve computational cost by using modulo *p* as 1024

II. Existing solution

Digital Fingerprints are considered to be the reliable option in asymmetric cryptography to ensure the ownership and authenticity of the communication parties. This paper presents a Shortened Complex Digital Fingerprint for securing communication in human-centered IoT scenario. We have also presented a multi-option parameter selection mechanism where the Fingerprint-verification pairs of expression at particular index can be selected to calculate security credentials. It improves the security against traffic capturing attacks. Results demonstrate the dominance of our scheme as compared to counterparts in terms of computation and communication overheads along with resilience analysis. Proposed SCDSA and MPS-SCDSA schemes achieve less computational time and communication overhead during Fingerprint and verification operations along with better resilience against capturing attacks. Moreover, it is very hard to break SCDSA based on CDLP as compared to DSA which is based on DLP. In future, we shall can work on intrusion detection capabilities in conjunction with MPS-SCDSA to measure the timely attack detection and prevention and durability of our scheme, in other application scenarios [33][34]. Moreover, through the combination of some popular machine learning algorithms the computational performance of our proposed method could be further improved.

III. Problem in Existing System

Traditional DSA based on DLP and IFP having many applications in network security but not suitable for devices like wearable's, healthcare sensors and monitoring in human-centered IoT. These devices have small memory size, limited battery power, low-bandwidth and less computational capabilities. Digital Fingerprints based on DLP and IFP using larger bits size (512-1024 bits) of computation and communication that needs higher energy consumptions. Existing DSA is based on real number that produces high communication overhead using 832 bits per Message. Complexity for these devices should be as lower as possible by achieving desired security strength. Existing DSA having two different problem scenarios where former is about computation overhead and time complexity whereas later is about communication overhead during Fingerprint and verification process. Fingerprint can be modified and physical Fingerprint can easily copied by any another very easily.

IV. Proposed system

As iot involves three parties: the cloud server, the third party auditor (TPA) and users. There are two types of users in a group: the original user and a number of group users. The original user and group users are both members of the group. Group members are allowed to access and modify shared data created by the original user based on access control polices. Shared data and its verification information (i.e. Fingerprints) are both stored in the cloud server. The third party auditor is able to verify the integrity of share data in the cloud server on behalf of group members. Another important issue we should consider in the construction of Oruta is the size of storage used for ring Fingerprints. According to the generation of ring Fingerprints in HARS, a block m is an element of Zp and its ring Fingerprint contains d elements of G1, where G1 is a cyclic group with order p. It means a |p|-bit block requires a d × |p|-bit ring Fingerprint, which forces users to spend a huge amount of space on storing ring Fingerprints. It is very frustrating for users, because cloud service providers, such as Amazon, will charge users based on the storage space they used. To reduce the storage for ring Fingerprints and still allow the TPA to audit shared data efficiently, we exploit an aggregated approach from. To enable each user in the group to easily modify data and share the latest version of data with the rest of the group, Oruta should also support dynamic operations on shared data.An dynamic operation indicates an insert, delete or update operation on a single block.

V. Architecture of system

DSA based on DLP and IFP having many applications in network security but not suitable for devices like wearable's, healthcare sensors and monitoring in human-centered IoT. These devices have small memory size, limited battery power, low-bandwidth and less computational capabilities. Digital Fingerprints based on DLP and IFP using larger bits size of computation and communication that needs higher energy consumptions. Existing DSA is based on real number that produces high communication overhead using 832 bits per Message. Complexity for these devices should be as lower as possible by achieving desired security strength. Existing DSA having two different problem scenarios where former is about computation overhead and time complexity whereas later is about communication overhead during Fingerprint and verification process. Moreover, if the value of is repeated then the size of the transmitted message is doubled and security is also vulnerable to compromise.

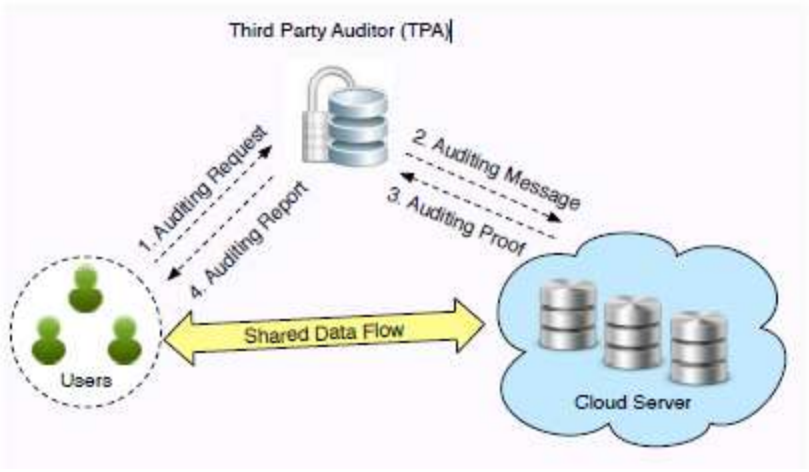

Figure 1: Architecture of IOT System

The problem of the existing DSA is high communication and computation overhead. Because size of is 512 bits and is 160 bits bits. The value of base number is in the range of 512 bits and must be greater than 1. Every message carries more than 1185 extra bits for digital Fingerprint. If we suppose to select small numbers then the DLP can be compromised and the value of private key could be easily determined by intruders. If large numbers are selected to increase security strength then it also increases computation and communication overhead per message.

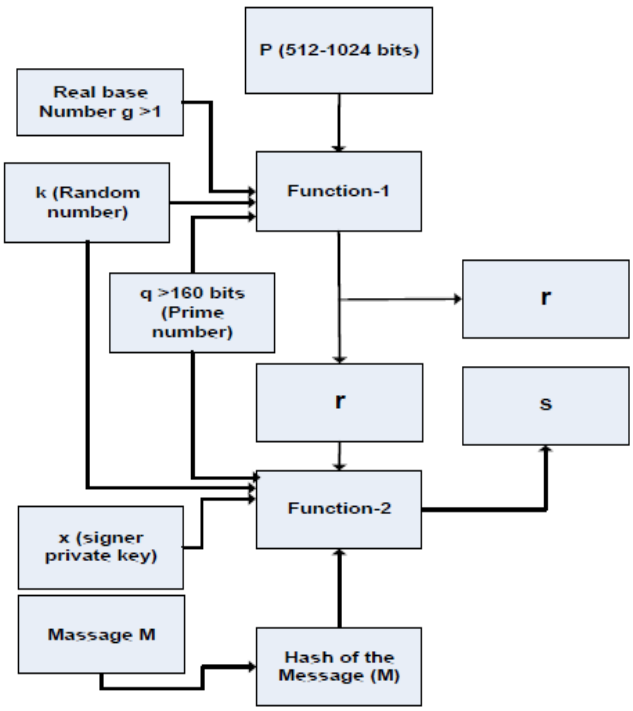

Figure 2. Digital Fingerprint process with two functions for r and s

VI. Shortened Complex Digital Fingerprint Algorithm

We have proposed **S**hortened **C**omplex **D**igital **Fingerprint** **A**lgorithm (SCDSA) that uses a novel method based on short complex numbers for Fingerprint and verification operations. Our scheme achieves better security for smaller bit sizes as compare to previous digital Fingerprint schemes based on DLP, IFP. Complex public key cryptosystem uses complex numbers which is a mathematically hard problems instead of real numbers. A complex number = + where " " part is real number and " " represents an Imaginary part. An imaginary part consist of where = √−1. The use of CDLP for designing SCDSA makes it more secure as

compared to preliminaries. We have adopted one way secure hash function SHA-1 to fix the size of to 160 bits which is first component of Digital Fingerprint. Length of the Fingerprint is equal to $|h \quad h(\ )| + |\ |$. A list of notations is provided in table 1 for SCDSA.

VII. SCDSA – Fingerprint And Verification Processes

During the Fingerprint process, initially the random number , is generated and then base number is selected from the finite field. After that the value of is computed using squaring and multiplication method. The message m is concatenated with and then SHA-1 based hash function is used to fix its length to 160 bits or 256 bits. In this way, the r part of digital Fingerprint is generated. Similarly the s part of digital Fingerprint is generated in F2 by using , , , and . The value of k is considered to be random and unique for each Fingerprint to ensure its strength. It has been calculated by involving the private key and the existing hash for strengthening randomness.

Pseudo Code I – Fingerprint Process on m
1. Random number k generate
2. $r = hash\ (\ (gk\ mod\ n) \parallel m)$
3. $s = k\ /(r + va)\ mod\ q$

Fingerprint = (r, s)
Fingerprint length: $|hash\ (.\ )| + |q|$

Pseudo Code II - Verification Process on received message
1. $gk = (\ a * gr\ )s\ mod\ n$
2. $r, = hash\ (\ k \parallel m)$
3. Check $r, = r$

Proof I - Correctness Proof
$(\ Pa * gr\ )s$
$=(\ gva * gr\ )k\ /(r + va)$
$= (\ gva+r\ )k\ /(r + va)$
$= gk(va+r)\ /(r + va)$
$= gk$

verification process. Initially, a finite field and large prime numbers up to 100 or 200 digits is chosen. Then publically define a complex number g which belongs to finite field and of order n. On the basis of parameters, Alice chooses Private Key Va and generates public key = . Private key is secret and public key is transferred to Bob. The function F1= ((kmod n) ‖ m) and its SHA-1 based hash function is calculated to get r as per step 2 in pseudocode I. Similarly, F2 = /(+ Va) mod which is equal to s according to step 3. Now Digital Fingerprint (,) is generated by as illustrated in figure 4 and then transmitted to along with public key.

In the verification process at receiver Bob as , the public key of sender , complex base number , modulus n and Fingerprint (r, s) are used to calculate k . Message m is concatenated with k and Hash function is applied to it to get ' . Now r is compared with ' to ensure similarity otherwise it is considered to be compromised in between transition. For example, when Bob receives the public key Pa along with r and s to verify the digital Fingerprint. Similarly Bob selects his private key "Vb" and generate public key Pb = Vb mod . For Fingerprint generation is randomly selected from finite field and keeps it secret to calculate r'. Bob uses function F3 = (Pa * r)s to calculate to calculate k as per the step I of Pseudo Code II for verification process. After that, SHA-1 based hash is calculated for the output of function F4 = k ‖ m to calculate r' as per step2. Finally, the values of ' are compared as illustrated in figure 5. If these values are same then the message is considered original as sent by Alice, otherwise, the message is being changed by some intermediary node or human being. Moreover, the correctness proof for verification of k using (Pa * r)s is presented in Proof-IGenerally, to obtain a smaller size of a ring Fingerprint than the size of a block, we choose k > d. As a trade-off, the communication cost of an auditing task will be increasing with an increase of k.

.

VIII. Basic Parameters

For exploring the example, we have considered a 10 digits value of = 1234567899 and the finite field is Fq= {0, 1, 2, 3, … , 1234567898}. The value of n is also 10 digits as = 591558727 and belong to finite field Fq with order . Moreover, the complex numbers selected from the above finite field Fq is = (11 + 12i) and Fn = {0, 1, 2, … , n-1}.

IX. Key Generation

Let Alice's private key is Va = 5 , = (11 + 12i), = 7 and = 3. Public key of Alice is Pa = Va mod which is equal to (11 + 12i)5 mod 7 = (((11 + 12i)2)2(11 + 12i)) mod 7 = (−2, −3). Value of Va is calculated by using squaring and multiplying method where Va = 5 whose binary value is 101. For first bit initialize the value of , and for bit =0, calculate square and for last bit =1 we have presented calculation below.

First Bit = 1 (Initialization)
gVa = g1 = (11+12i)
Second Bit = 0 (Squaring)
$g2$ = (11+12i)2=(121+132i+132i +144 (−1)) =(−23+164i)
$g4$ = (((11+12i)2)2=(−23+164i)2 =(529−3772i−3772i−26896 (−1)) =(−26367−7544i)
Third Bit = 1 (Squaring and Multiplying)
$g5$ = (((11+12i)2)2(11+12i))
=((−26367−7544i)(11+12i)) = (−199509 −399388i)

By using squaring and multiplying method solve the 9 where Bob's private key is Vb = 9, = 7, = (11, 12).

Public key Pb = Vbmod n = (11 + 12i)9 mod 7 is as explored below.
First Bit = 1 (Initialization)
$g\text{Va} = \text{g1} = (11+12\text{i})$
Second Bit = 0 (Squaring)
$g2 = (-23+164\text{i})$
$g4 = (-26367-7544\text{i})$
Third Bit = 0 (Squaring)
$8= (((11 + 12\text{i})2)2)2 = (-26367 - 7544\text{i})2$
$(695218689 + 198912648\text{i} + 198912648\text{i} + 56911936\ (-1))$
$= (638306753 + 397825296\text{i})$
Fourth Bit = 1 (Squaring and Multiplying)
$9= ((((11 + 12\text{i})2)2)2(11 + 12\text{i}))$
$=(638306753 + 397825296\text{i})(11 + 12\text{i})$
$=(7021374085 + 7659681036\text{i} + 4376078256$
$+4773903552\ (-1))$
$=(2247470533 + 12035759301\text{i})$

X. Fingerprint Process

In this way, a single user can generate different type of Fingerprint values that are verifiable by using the index id of Fingerprint and verification pair. In this scenario, the index value can be concatenated in the Fingerprint as well for identification at receiver. It can guard against the traffic analysis attacks where the probability of guessing the particular Fingerprint-verification pair is too complex. During signing, the value of k= 4 is randomly selected from Fn for message m and calculated the value of r as r=$hash((gk\ mod\ n)\|m)$. In this regard, we have first calculatedgk=$g4$=(−26367−7544i) by using square and multiplication method as illustrated in table 4. Public key is $g4$ mod 7=(−26367−7544i) mod 7=(5+5i) and final Fingerprint is (r, s). s= kr+va/ mod n=461+5 mod 7

Bits for g4	Status	Operation
First Bit = 1	Initialization	$g1$ = (11+12i)
Second Bit =0	Squaring	$g2$ = (11+12i)2
Third Bit =0	Squaring	$g4$ = (((11+12i)2)2
For gk= (11 + 12)4 $g1$=(11+12) $g2$= (11 + 12)2=(−23+164i) $g4$ = (((11+12i)2)2		

Table1. Squaring and multiplication method for G4

XI. Conclusion

We have discussed about implementation, results and analysis. We have used Crypto++ library for DSA along with private-public keys for the implementation of Fingerprint-verification functions in respective classes. For the ECDSA, we have linked the borZoi library which is also based on C++. It also supports better SHA-1 (FIPS 180-1) for hash function. Moreover, we have tested the ECDsa which is an abstract base class in C# whereas ECDsaCng class is created as its child class for overriding the functions to provide functionality for ECDSA algorithm in Cryptography Next Generation (CNG). We have performed multiple executions for Fingerprint-verification operations using DSA, EDSA, our proposed SCDSA and MPS-SCDSA. Results are extracted for Fingerprint and verification execution time, impact of message length over verification time, communication for messages with Fingerprint and resilience against human operated capturing attacks or by some intelligent machines. Experimental results prove the dominance of our proposed schemes as compared to counterparts.

References

[1]. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao,"A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications", *IEEE Internet of Things Journal*, Vol. 4 No. 5, pp. 1125-1142, 2017.

[2]. X. Luo, J. Liu, D. Zhang, and X. Chang, "A large-scale web QoS prediction scheme for the industrial Internet of Things based on a kernel machine learning algorithm," *Computer Networks*, Vol. 101, pp. 81-89, 2016.

[3]. W. Zhao, R. Lun, C. Gordon, A. M. Fofana, D. D. Espy, A. Reinthal, B. Ekelman, G. D. Goodman, J. E. Niederriter, and X. Luo, "A human-centered activity tracking service: Towards a healthier workplace," *IEEE Transactions on Human-Machine Systems*, Vol. 47, No. 3, pp. 343-355, 2017.

[4]. H. Lin, T. Zong, and Y. Yeh, "A DL Based Short strong Designated Verifier Fingerprint Scheme with Low Computation" *Journal of Information Science and Engineering*, Vol. 27, pp. 451-463, 2011.

[5]. Andrew Chi-Chih Yao ; Yunlei Zhao,"Online based Fingerprints for Low-Power Devices", *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 2, pp. 283-294, 2013.

[6]. Z. Shao, "Digital Fingerprint schemes based on factoring and discrete logarithms", *Electronic Letters*, pp.1518-1519, 2002

[7]. X. Luo, D. Zhang, L. T. Yang, J. Liu, X. Chang, and H. Ning, "A kernel machine-based secure data sensing and fusion scheme in wireless sensor networks for the cyber-physical systems", *Future Generation Computer Systems*, Vol. 61, pp. 85-96, 2016

[8]. M. Mossinger, B. Petschkuhn, J. Bauer, R. C.Staudemeyer, M. Wojcik and H. C. Pohls, "Towards quantifying the cost of a secure IoT: Overhead and energy consumption of ECC Fingerprints on an ARM-based device", in *Proceedings of International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2016, pp. 1-6.

[9]. X. Luo, J. Deng, J. Liu, W. Wang, X. Ban, and J. H. Wang, "A quantized kernel least mean square scheme with entropy-guided learning for intelligent data analysis", *China Communications*, Vol. 14, No. 7, pp. 127-136, 2017

[10]. Y. Xu, X. Luo, W. Wang, and W. Zhao, "Efficient DV-HOP localization for wireless cyber-physical social sensing system: A correntropy-based neural network learning scheme", *Sensors*, Vol. 17, No. 1, Id. 135, 2017

[11]. H. C. Pohls, "JSON Sensor Fingerprints (JSS): End-to-End Integrity Protection from Constrained Device to IoT Application", in *Proceedings of International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, 2015, pp. 306-312.

[12]. X. Luo, Y. Xu, W. Wang, M. Yuan, X. Ban, Y. Zhu, and W. Zhao, "Towards enhancing stacked extreme learning machine with sparse autoencoder by correntropy", *Journal of The Franklin Institute*, Vol. 355, No. 4, pp. 1945-1966, 2018

[13]. S. Zeng, C. Yang and M. Hwang, "A new digital Fingerprint scheme based on Factoring and Discrete Logarithm", *International Journal of Computer Mathematics*, pp. 9-14, 2004.