Identity based Encryption: An Operative Method for Authentication in Pervasive Computing

Piyush Kumar Sharma
Department of Computer Science and Engineering
Samrat Ashok Technological Institute
Vidisha, (M.P.), India

Pranita Jain
Asst Prof.
Department of Computer Science and Engineering
Samrat Ashok Technological Institute
Vidisha, (M.P.), India

ABSTRACT
Pervasive Computing is an emerging technology which is primarily used for collaborating information. With the advent of this new technology several Challenges and Security issues comes into presence such as authentication of Users. The Existing methodology implemented for the Unceasing Verification in Pervasive Computing using Blended Identity is proposed which delivers Refuge from numerous attacks but since it involved with the implemented of RSA / DSA based algorithm computation cost and Communiqué time is high. Hence a new and efficient methodology is implemented for Pervasive Computing using Identity based Encryption which not only delivers refuge from numerous attacks but also takes less Calculation Cost and Communication time.

Keywords
Pervasive Computing, Identity based Encryption, Blended Identity, Authentication, Identity Provider, Federated Identity Management.

1. INTRODUCTION
‘‘The most thoughtful machineries are those that vanish. They texture themselves into the material of ordinary life until they are vague from it.’’ So commenced Mark Weiser’s influential 1991newspaper [1] that designated his hallucination of omnipresent calculating, now also baptized pervasive calculating. The quintessence of that hallucination was the conception of surroundings soaking with calculating and communiqué competence, yet elegantly combined with humanoid users. When uttered, this was a hallucination too far gaining of its time the hardware knowledge wanted to accomplish it basically did not happen. Not astonishingly, the employment endeavored by Weiser and his generations at Xerox PARC fell dumpy.

1.1 Distributed System:
The arena of disseminated organizations arose at the connection of individual processors and indigenous area systems. The investigation that shadowed from the mid-1970’s finished the primary 1990’s shaped a theoretical agenda and algorithmic dishonorable that has established to be of continuing assessment in all exertion connecting two or more processors linked by a system — whether movable or static, supported or wireless, scant or unescapable. This physique of information distances many expanses that are opening to unescapable figuring and is now well organized in schoolbooks [2, 3, 4]:

- Distant communiqué, counting etiquette layering, distant process call [5], the use of breathers, and the use of end-to-end influences in assignment of functionality [6].
- Responsibility broad mindedness, comprising thermonuclear communications, disseminated and nested communications, and two-phase obligate [7].
- High obtainability, counting positive and negative imitation regulator [8], reflected performance [9], and positive repossession [10].
- Inaccessible material admittance, counting hoarding, meaning transport, disseminated file organizations, and spread catalogues [11].
- Safety, counting encryption-based communal confirmation and confidentiality [12].

1.2 Mobile Computing:
Mobile calculating is motionless a very vigorous and embryonic arena of investigation; whose figure of information anticipates systematization in primers. The consequences accomplished so distant can be assembled into the subsequent comprehensive zones:

- Mobile schmoosing, counting Moveable IP [13], ad hoc procedures [14], and practices for educating TCP presentation in wireless systems [15, 16].
- Mobile evidence admittance, counting disengaged procedure [17], bandwidth adaptive sleeve admittance [18], and discriminating regulator of information steadiness [19, 20].
- Sustenance for adaptive submissions, counting transcoding by substitutions and adaptive reserve management.
- Organization equal energy exchangeable systems, such as energy conscious revision, adjustable rapidity computer preparation, and energy delicate reminiscence organization.
- Position compassion, counting position identifying and position conscious organization performance.

1.3 Structure of Smart Grid:
By adding significant new functionality, disseminated intellect, and state-of-the-art communiqué competences to the influence grid, the shrewd grid organization can be more well organized, more irrepressible, and more reasonable to accomplish and activate [21], [22]. However, it transports not only inordinate presentation benefit to the influence industry, but also tremendous risks as glowing as difficult contests in defensive the smart grid organizations from replicated sanctuary intimidations [23]. Considering the vast scale of a shrewd grid, it is sensible to imagine that the snowballing susceptibility of the shrewd grid communiqué organization strength also be massive. Virtually all gatherings decide that the significances of a clever grid replicated sanctuary opening can be massive. New meanings such as request rejoinder familiarize noteworthy new cyber attack trajectories such as a malware that freshmen an enormous synchronized and immediate droplet in request, hypothetically instigating considerable impairment to circulation, broadcast, and even cohort conveniences [24].

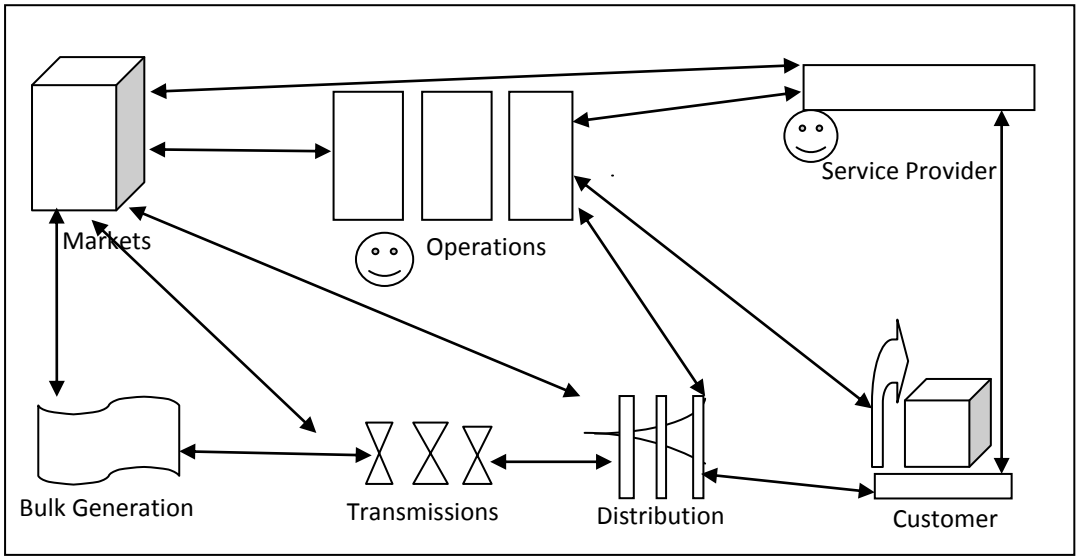

Figure 1: Smart Grid Conceptual Model.

2. PROPOSED METHODOLOGY

The perception overdue is to let a sensor independently produce a communal key on-the-fly using an uninformed string. For instance, a sensor collecting Identity readings on 22/01/2009 at 03:00 PM will first create a string str = (Identity1|22/01/2009|15). Expending this string, the instrument can originate a public key, Y_{str} to encrypt the statistics and send it to the stowage site. There is no consistent secret key shaped. In fact, the sensor cannot generate the secret key desirable to decode the communication.

When the sender wishes to release this information to a receiver, the sender can originate the conforming secret key, X_{str}, by using the similar string str = (Identity1|22/01/2009|15). This clandestine key only permits the receiver to decrypt messages encrypted by a sensor using the same string. This simplifies the key management, since the sender can produce the clandestine key on-demand without possession pathway of which keys were used to encrypt which statistics. The only obligation is that the string used to define the happening is the same.

2.1 Setup

We choice an elliptic curve with basic equation E over GF(p), where p is a big leading number. We also represent P as the Common point of E and q as the instruction of P, where q is also a big prime. A customary of n underground explanations x1, · · · ,xn∈GF(q) is selected to produce the principal underground important,

$$X = (x_1, \cdots, x_n).$$

The n communal keys are then produced to make up the principal communal important,

$$Y = (y_1, \cdots, y_n)$$

Where $y_i = x_i \cdot P$, $1 \leq i < n$. Finally, a collision resistant one-way hash function h: {0, 1}→ {0, 1}^{n} is chosen. The strictures (y, P, p, q, h(.))are unconfined as the organization public structures.

2.2 Keygen:

To derive a underground key Xstr conforming to a community key produced by a filament str, the sender implements Keygen(str) = Xstr,

$$X_{str} = \sum_{i=1}^{n} hi(str) \cdot x_i$$

Where $h_i(str)$ is the i^{th} bit of h(str).

2.3 Encrypt:

To encrypt a communication m using a communal key resulting from string str, the sensor does Encrypt(m, str) to regulate the ciphertext c. Alg. 3 demonstrations the procedure. Memorandum that Alg. 3 appearances 1 and 2 necessity only be course when to instigate the communal key Y_{str}.

Algorithm3.Encrypt(m,public_key)
1. Determine the String str using agreed upom pattern
2. Generate public key Ystr.
3. Execute ECIES_Encryption(m, Ystr) to obtain c.

2.4 Decrypt:

The receiver implements EccDecrypt(c, xstr) to attain the innovative communication m which was encoded using a clandestine important resulting from str. The procedure is shown in Alg. 4.

Algorithm4. Decrypt(U,c,r) where r is a private key
Receiver executes EciesDecrypt(U,c,r) to obtain m

3. RESULT ANALYSIS

Table 1. Examination of Numerous Refuge Events

Security Measures	**Existing Work**	**Proposed Work**
Security & Privacy	Yes	Yes
Confidentiability	Yes	Yes
Integrity	Yes	Yes

Authentication	Yes	Yes
Non-Repudiation	Yes	Yes
Accountability	Yes	Yes
Availability	Yes	Yes
Privacy	Yes	Yes
Reply Attack	Yes	Yes
Forward Secrecy	No	Yes
Escrow Problem	Yes	No
Additional Authentication	No	Yes

Table 2. Analysis of Revocation Time

	Revocation Time (s)	
No. of Blocks	**Existing Work**	**Proposed Work**
0	0	0
10	0.3	0.2
20	0.5	0.3
30	0.8	0.6
40	1.1	0.9
50	1.5	1.2

Table 3. Analysis of Communication Cost

	Communication Cost (KB)	
No. of Users	**Existing Work**	**Proposed Work**
0	0	0
1	6.8	5.5
3	5.9	5.4
5	6	5.8
7	6.3	6.1
9	7	6.7

4. CONCLUSION

Various numbers of partial identities that any user needs to manage is growing with the growing quantity of online services introduced by dissimilar package wage-earners. These identities are scattered across multiple providers making them increasingly difficult to manage. In addition, providers do not give users enough controller over their stored data. The concepts of Identity Management and different practical Identity Management Systems have been familiarized to tackle these issues.

The Proposed methodology implemented for an efficient Authentication in Pervasive Computing using Identity based Encryption provides effective Safety from numerous occurrences and also delivers less Communication and computational cost.

5. REFERENCES

[1] Weiser, M. The Computer for the 21st Century. *Scientific American* , September, 1991.

[2] Couloris, G., Dollimore, J., Kindberg, T. *Distributed Systems Concepts and Design (Third Edition).* Addison-Wesley, 2001.

[3] Lynch, N.A. *Distributed Algorithms.* Morgan Kaufmann, 1993.

[4] Mullender, S.J. (editor). *Distributed Systems.* Addison-Wesley, 1993.

[5] Birrell, A.D., Nelson, B.J. Implementing Remote Procedure Calls. *ACM Transactions on Computer Systems* 2(1), February, 1984.

[6] Saltzer, J.H., Reed, D.P., Clark, D.D. End-to-End Arguments in System Design. *ACM Transactions on Computer Systems* 2(4), November, 1984.

[7] Gray, J., Reuter, A. *Transaction Processing: Concepts and Techniques.* Morgan Kaufman, 1993.

[8] Davidson, S.B., Garcia-Molina, H., Skeen, D. Consistency in Partitioned Networks. *ACM Computing Surveys* 17(3), September, 1985.

[9] Borg, A., Blau, W., Graetsch, W. Fault Tolerance Under Unix. *ACM Transactions on Computer Systems* 7(1), February, 1989.

[10] Strom, R.E., Yemini, S. Optimistic Recovery in Distributed Systems. *ACM Transactions on Computer Systems* 3(3), August, 1985.

[11] Satyanarayanan, M. A Survey of Distributed File Systems. In Traub, J.F., Grosz, B., Lampson, B., Nilsson, N.J. (editors), *Annual Review of Computer Science*. Annual Reviews, Inc, 1989.

[12] Needham, R.M and Schroeder, M.D. Using Encryption for Authentication in Large Networks of Computers. *Communications of the ACM* 21(12), December, 1978.

[13] Bhagwat, P., Perkins, C., Tripathi, S. Network Layer Mobility: An Architecture and Survey. *IEEE Personal Communications* 3(3), June, 1996.

[14] Royer, E.M., Toh, C.K. A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. *IEEE Personal Communications* 6(2), April, 1999.

[15] Bakre, A., Badrinath, B.R. Handoff and System Support for Indirect TCP/IP. In *Proceedings of the Second Usenix Symposium on Mobile & Location-Independent Computing*. Ann Arbor, MI, April, 1995.

[16] Brewer, E.A., Katz, R.H., Chawathe, Y., Gribble, S.D., Hodes, T., Nguyen, G., Stemm, M., Henderson, T., Amir, E., Balakrishnan, H., Fox, A., Padmanabhan, V.N., Seshan, S. A Network Architecture for Heterogeneous Mobile Computing. *IEEE Personal Communications* 5(5), October, 1998.

[17] Kistler, J.J., Satyanarayanan, M. Disconnected Operation in the Coda File System. *ACM Transactions on Computer Systems* 10(1), February, 1992.

[18] Mummert, L.B., Ebling, M.R., Satyanarayanan, M. Exploiting Weak Connectivity for Mobile File Access. In *Proceedings of the 15th ACM Symposium on Operating Systems Principles*. Copper Mountain Resort, CO, December, 1995.

[19] Tait, C.D., Duchamp, D. An Efficient Variable-Consistency Replicated File Service. In *Proceedings of*

the USENIX File Systems Workshop. Ann Arbor, MI, May, 1992.

[20] Terry, D.B., Theimer, M.M., Petersen, K., Demers, A.J., Spreitzer, M.J., Hauser, C.H. Managing Update Conflicts in a Weakly Connected Replicated Storage System. In *Proceedings of the 15th ACM Symposium on Operating Systems Principles*. Copper Mountain Resort, CO, December, 1995.

[21] Litos Strategic Communication The smart grid: An introduction," in DOE's Office of Electricity Delivery and Energy Reliability 2008.online available at: energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf.

[22] Amin, S. Massoud, and Bruce F. Wollenberg. "Toward a smart grid: power delivery for the 21st century." IEEE Power and Energy Magazine, vol. 3, no. 5 (2005): 34-41, September 2005.

[23] H. Khurana, M. Hadley, L. Ning, and D. A. Frincke, "Smart-grid security issues," IEEE Security and Privacy, vol. 8, pp. 81-85, February 2010.

[24] S. Clements, H. Kirkham, "Cyber-security considerations for the smart grid," in IEEE Power and Energy Society General Meeting 2010, pp. 1-5, July 2010.