Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams

K.Gowsalya[#1],R.Hemalatha[#2],R.Jeevitha[#3] , Mrs.A.Sivasangari, MCA.,M.Phil.,Ph.D., [#4]

Pg Scholar, Associate Professor &DSCASW College

Department of MCA &Dhanalakshmi Srinivasan College of Arts and Science for Women's- Perambalur, Tamilnadu, India

[1] gowsisasi143@gmail.com,[2]hemalatha03026@gmail.com,[3]jeevitha07061997@gmail.com, [4]sankarisiva001@gmail.com

Abstract

The issues associated with the protection and privacy of consumption and commerce information gift serious challenges. In this, address the problem of providing transaction security in decentralized smart grid energy trading without reliance on trusted third parties. We have implemented a proof-of-concept for decentralized energy trading system using blockchain technology, multi-signatures, and anonymous encrypted messaging streams, enabling peers to anonymously negotiate energy prices and securely perform trading transactions. We conducted case studies to perform security analysis and performance analysis among the context of the evoked security and privacy necessities.

Keywords: smart grid systems, decentralized energy trading, blockchain technologies

INTRODUCTION

Smart grids (SGs) are expected to provide not only fine-grained consumption monitoring, but also engage increasing number of residential power generation sites into distributed energy trading (e.g., a community microgrid). As such, it is important to equip SGs with a secure energy trading infrastructure capable of executing contracts among trading agents and handling bidding, negotiation and transactions while preserving identity privacy. A majority of modern financial infrastructures are centralized and implicate involvement of a trusted third party, which handles accounts, processes payments and provides security. The centralized energy trading suffers from scalability and security concerns, e.g., 1) Single point of failure: As a key component of a centralized network, failure of a centralized middleman leads to full disturbance of authentication and payment activities, and obstruct from providing availability and reliability security goals. 2) Lack of privacy and anonymity: Following Wood's behavioral modeling of electricity consumption profiling approach, a centralized middleman may reveal patterns of an agent's energy generation and predict the agent's daily activities. These major drawbacks of the centralized infrastructure have motivated us to address the problem of providing identity privacy and transaction security in energy trading using a decentralized approach. The decentralized nature of communication relies upon the cooperation among individual nodes to carry out essential tasks of information propagation. Although public key cryptography could be applied to provide a certain level of security and integrity of information, the most important issue when dealing with public keys is ensuring their authenticity without relying on a trusted third party. A trustless or semi-trustless decentralized energy trading system could provide transaction security and identity privacy, while relying on cryptographic techniques instead of relying on a trusted third party. To verify our claim we have adapted and implemented a proof-of-concept for decentralized energy trading system where all nodes collectively act as a replacement for a trusted party, and vote on validity of transaction by traversing through history of publicly available distributed chain of transactions. The

proposedsystem, PriWatt1 is inspired and built upon decentralized digital payment Bitcoin system and decentralized peer-to-peer message authentication and delivery system Bitmessage. Bitcoin system adopts cryptographic proof-of-work along with nested chain of hashed secrets to eliminate need of trusted third party providing security and privacy when an agent trades with complete strangers. Bitmessage provides anonymity in a trustless network through propagating encrypted messages in messaging streams. While sustaining transaction security in a trustless model the PriWatt does not reveal identities of trading parties and keeps their financial profiles private. Thus, the most contribution of this work is that the integration and example implementation of blockchain technology, multi-signature approach, and anonymous encrypted message into the PriWatt system, in order thattransactions among a decentralized system are enabled with high privacy and security. We have performed performance analysis of the system, and also a qualitative analysis in terms of requirements satisfaction. In addition to helping with the reliability and privacy issues, the proposed system might be of significant help in designing and deploying SGs in challenging environments such as less developed countries, war zones, etc., some of which completely lack not just the power infrastructure, but also financial infrastructure, privacy and security-protecting laws, etc. Decentralized microgrids combined with digital currencies such as Bitcoin can lead to a faster and more robust solution to power problems in such environments and extreme conditions. Our system provides a plausible solution to enable such microgrid designs.

RELATED WORK

S. NAKAMOTO, "BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM," 2008.

A strictly peer-to-peer version of electronic money would permit on-line payments to be sent directly from one party to a different while not researching a institution. Digital signatures give a part of the answer, however the most advantages ar lost if a trusty third party continues to be needed to stop double-spending. We propose an answer to the double-spending downside employing a peer-to-peer network. The network timestamps transactions by hashing them into Associate in Nursing current chain of hash-based proof-of-work, forming a record that can't be modified while not redoing the proof-of-work. The longest chain not solely is proof of the sequence of events witnessed, however proof that it came from the most important pool of central processing unit power. As long as a majority of central processing unit power is controlled by nodes that don't seem to be cooperating to attack the network, they will generate the longest chain and exceed attackers. The network itself requires minimal structure. Messages ar broadcast on a best effort basis, and nodes will leave and rejoin the network at can, acceptive the longest proof-of-work chain as proof of what happened whereas they were gone.

J. WARREN, "BITMESSAGE: A PEER-TO-PEER MESSAGE AUTHENTICATION AND DELIVERY SYSTEM," WHITE PAPER (27 NOVEMBER 2012), HTTPS://BITMESSAGE. ORG/BITMESSAGE. PDF, 2012.

We propose a system that enables users to firmly send and receive messages, and buy broadcast messages, employing a trustless suburbanised peer to peer protocol. Users needn't exchange any knowledge on the far side a comparatively short (around thirty six character) address to make sure security and that they needn't have any thought of public or non-public keys to use the system. It is additionally designed to mask non-content knowledge, just like the sender and receiver of messages, from those not concerned within the communication.

G. O. KARAME, E. ANDROULAKI, AND S. CAPKUN, "DOUBLESPENDING FAST PAYMENTS IN BITCOIN," IN PROCEEDINGS OF THE 2012 ACM

CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY. ACM, 2012, PP. 906–917.

Bitcoin could be a localized payment system that depends on Proof-of- Work (PoW) to verify payments. Nowadays, Bitcoin is more and more utilized in variety of quick payment eventualities, wherever the time between the exchange of currency and product is brief (in the order of few seconds). While the Bitcoin payment verification theme is intended to forestall double-spending, our results show that the system needs tens of minutes to verify a dealing and is thus inappropriate for fast payments. An example of this use of Bitcoin was recently reported in the media: Bitcoins were used as a form of fast payment in a local fast-food restaurant. Until now, the safety of quick Bitcoin payments has not been studied. In this paper, we analyze the security of using Bitcoin for fast payments. We show that, unless appropriate detection techniques are integrated in the current Bitcoin implementation, double spending attacks on fast payments succeed with overwhelming probability and can be mounted at low cost. We more show that the measures counseled by Bitcoin developers for the employment of Bitcoin in quick payments don't seem to be perpetually effective in police work double spending; we tend to show that if those recommendations ar integrated in future Bitcoin implementations, double-spending attacks on Bitcoin will still be possible. Finally, we tend to propose and implement a modification to the prevailing Bitcoin implementation that ensures the detection of double-spending attacks against quick payments.

F. MENDEL, T. PEYRIN, M. SCHL¨AFFER, L. WANG, AND S. WU, "IMPROVED CRYPTANALYSIS OF REDUCED RIPEMD-160," IN ADVANCES IN CRYPTOLOGY-ASIACRYPT 2013. SPRINGER, 2013, PP. 484–503.

In this article, we tend to propose AN improved cryptanalytics of the double-branch hash operate normal RIPEMD-160. Using a carefully designed non-linear path search tool, we study the potential di_erential paths that can be constructed from a di_erence in a single message word and show that some of these message words can lead to very good di_erential path candidates.

Leveraging the recent freedom degree utilization technique from Landelle and Peyrin to merge 2 branch instances, we eventually manage to obtain a semi-free-start collision attack for 42 steps of the RIPEMD-160 compression operate, whereas the antecedently best understand result reached thirty six steps. In addition, we also describe a 36-step semi-free-start collision attack which starts from the first step.

EXISTING PROCESS

A majority of modern financial infrastructures are centralized and implicate involvement of a trusted third party, which handles accounts, processes payments and provides security. The centralized energy trading suffers from scalability and security concerns, e.g., 1) Single point of failure: As a key component of a centralized network, failure of a centralized middleman leads to full disturbance of authentication and payment activities, and obstruct from providing availability and reliability security goals. 2) Lack of privacy and anonymity:. Following Wood's behavioral modeling of electricity consumption profiling approach, a centralized middleman may reveal patterns of an agent's energy generation and predict the agent's daily activities.

DISADVANTAGE

- Transaction failure
- Less security
- Not user friendly
- Very slow

PROPOSED PROCESS

The work is the integration and prototype implementation of blockchain technology, multi-signature approach, and anonymous encrypted message into the PriWatt system, so that

transactions within a decentralized system are enabled with high privacy and security. We have performed performance analysis of the system, and also a qualitative analysis in terms of requirements satisfaction. In addition to helping with the reliability and privacy issues, the proposed system might be of significant help in designing and deploying SGs in challenging environments such as less developed countries, war zones, etc., some of which completely lack not just the power infrastructure, but also financial infrastructure, privacy and security-protecting laws, etc. Decentralized microgrids combined with digital currencies such as Bitcoin can lead to a faster and more robust solution to power problems in such environments and extreme conditions. Our system provides a plausible solution to enable such microgrid designs.

ADVANTAGE

- High privacy and security-protecting
- Less Financial infrastructure
- More faster
- Robust

PROCESS

- User
- Login
- Query Processing
- Key process
- Admin

USER

Before going to acquire the service, User have to register their corresponding personal details such as user name, Email id, contact no and Identity Details such as voter id, Aathar card. And the corresponding details are processed and stored in the server database. Those details are checked whenever the user has authenticate themselves.

LOGIN

After complete the basic registration process, the individual account is created to access the service for the each user. Through the account only then the user have to use the service. User has a chance to view the other users to transfer messages.

QUERY PROCESSING

Here, after the authentication process of the each user, they have to send the messages to others. Here, the message is transferred through the blockchain mechanism and also the user's information are encrypted through heuristic algorithm. It provides high security data for the user's data.

KEY PROCESS

Here, before the message is going to transfer then the user to verify themselves as a valid user through key generation process. If the key is valid then the message is transferred to the destination user through block chain mechanism else the message is not transferred.

ADMIN

Admin plays a vital role part in this process. The entire process is monitored by admin and maintain the details of the user. Admin has a chance to view the overall process of the user's message sharing mechanism and also has chance to view the intermediate of the message passing system.

SYSTEM ARCHITECTURE

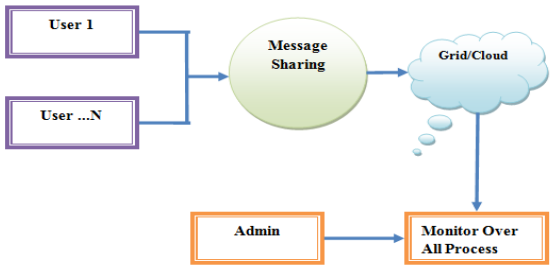

Fig 1 Architecture Diagram

Available@ www.ijrse.org Mail: info@ijrse.org ISSN: 2212-4012

CONCLUSION

The problem of providing transaction security in decentralized SG energy trading without reliance on trusted third party. We implemented a token-based private decentralized energy trading system that enables peers to anonymously negotiate energy prices and securely perform trading transactions. We used blockchain technology, multisignatures and anonymous encrypted message propagation streams to provide certain levels of privacy and security. Our system uses peer-to-peer community based data replication method where transactions are protected from failure since they are replicated among all active nodes. In addition, the proof-of-work, as in Bitcoin, allows the system to overcome Byzantine failures and to combat double-spending attacks which are critical in any electronic payment system.We sculpturesque and simulated energy commercialism case situations among peers in a very SG. We performed security and performance analysis and evaluation. We simulated network related attacks and demonstrated our claim that the system is resistant to significant known attacks; it does not reveal identities of trading parties; and it keeps financial profiles secure and private. We identified and discussed potential attacks and elicited security and privacy requirements. Overall, we found that the appropriate combination of blockchain technology, multi-signatures and anonymous encrypted message propagation streams presents a feasible and reliable direction towards decentralized SG energy trading with higher privacy and security compared to the traditional centralized trading solutions.

REFERENCE

[1] G. Wood and M. Newborough, "Dynamic energyconsumption indicators for domestic appliances: environment, behaviour and design," Energy and Buildings, vol. 35, no. 8, pp. 821–841, 2003.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[3] J. Warren, "Bitmessage: A peer-to-peer message authentication and delivery system," white paper (27 November 2012), https://bitmessage. org/bitmessage. pdf, 2012.

[4] G. O. Karame, E. Androulaki, and S. Capkun, "Doublespending fast payments in bitcoin," in Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012, pp. 906–917.

[5] K. Okupski, "Bitcoin developer reference."

[6] S. Siby, "Paying your internet, one byte at a time," 2013.

[7] N. S. Grid, "Introduction to nistir 7628 guidelines for smart grid cyber security," Guideline, Sep, 2010.

[8] A. Moise and J. Brodkin, "Ansi c12. 22, ieee 1703, and mc12. 22 transport over ip," 2011.

[9] F. Mendel, T. Peyrin, M. Schl¨affer, L. Wang, and S. Wu, "Improved cryptanalysis of reduced ripemd-160," in Advances in Cryptology-ASIACRYPT 2013. Springer, 2013, pp. 484–503.

[10] Y. Sasaki, L. Wang, and K. Aoki, "Preimage attacks on 41-step sha-256 and 46-step sha-512." IACR Cryptology ePrint Archive, vol. 2009, p. 479, 2009.

[11] B. Preneel, A. Bosselaers, and H. Dobbertin, "The cryptographic hash function ripemd-160," 1997.

[12] M. Musson, "Attacking the elliptic curve discrete logarithm problem," Ph.D. dissertation, Citeseer, 2006.

[13] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic curve cryptography in practice," in Financial Cryptography and Data Security. Springer, 2014, pp. 157–175.

[14] H. Suleiman and D. Svetinovic, "Evaluating the effectiveness of the security quality requirements engineering (square) method: a case study using smart grid advanced metering infrastructure," Requirements Engineering, vol. 18, no. 3, pp. 251–279, 2013.

[15] B. Schneier, "Attack trees," Dr. Dobbs journal, vol. 24, no. 12, pp. 21–29, 1999.

BIOGRAPHICAL NOTES

	Mrs.Sivasankari.A-Received M.C.A.,M.Phil,M.E.,Degree in computer Science. She has 11 Years of Teaching Experience. She is Guided 7 Students in M.Phil.,She had Presented 7 Papers in International Conference and also She Presented 7 Papers in National Conference.She is Currently Working has Associate Professor in Department of Computer Applications in Dhanalakshmi Srinivasan College of Arts & Science for Women(Autonomous),Perambalur,TamilNadu,India.
	Miss.Gowsalya.K,PG Scholar,[Department of Computer Applicatons],pursuing MCA in Dhanalakshmi Srinivasan College of Arts & Science for Women, (Autonomous),Perambalur-621212,TamilNadu,(India)
	Miss.Hemalatha.R,PG Scholar,[Department of Computer Applicatons],pursuing MCA in Dhanalakshmi Srinivasan College of Arts & Science for Women,Perambalur-621212,TamilNadu,(India)
	Miss.Jeevitha.R,PG Scholar,[Department of Computer Applicatons],pursuing MCA in Dhanalakshmi Srinivasan College of Arts & Science for Women,Perambalur-621212,TamilNadu,(India)